ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2021)

XII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 27-29 октября 2021 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург
2021

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РЕГИОНОВ РОССИИ (ИБРР-2021)

XII САНКТ-ПЕТЕРБУРГСКАЯ МЕЖРЕГИОНАЛЬНАЯ КОНФЕРЕНЦИЯ

Санкт-Петербург, 27-29 октября 2021 г.

МАТЕРИАЛЫ КОНФЕРЕНЦИИ

Санкт-Петербург

2021

УДК (002:681):338.98

И 74

Информационная безопасность регионов России (ИБРР-2021).

И 74 XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 27-29 октября 2021 г.: Материалы конференции / СПОИСУ. – СПб., 2021. – 427 с.

ISBN 978_5_00182_019_2

Сборник охватывает широкий круг направлений: Государственная политика jбеспечения информационной безопасности регионов России; правовые аспекты информационной безопасности; Безопасность информационных технологий; Современные средства защиты информации; Информационная безопасность телекоммуникационных сетей; Информационно-экономическая безопасность; Информационная безопасность и импортозамещение в критических инфраструктурах; Информационная безопасность транспортных систем; Информационная безопасность объектов морской техники и морской инфраструктуры; Информационно-психологическая безопасность; Информационная безопасность в экологии; Информационная безопасность в социокомпьютинге; Информационная безопасность киберфизических систем; Информационная безопасность геоинформационных систем; Подготовка и переподготовка кадров в области обеспечения информационной безопасности, а также материалы и молодежной научной школы «Безопасные интеллектуальные информационные системы и технологии». Предназначен для широкого круга руководителей и специалистов органов государственной власти, академических учреждений, высших учебных заведений, научно-исследовательских и научно-производственных предприятий и организаций Санкт-Петербурга и других регионов, специализирующихся в области информатизации, связи и защиты информации.

УДК (002:681):338.98

Редакционная коллегия: *Б.Я. Советов, Р.М. Юсупов, В.В. Касаткин*
Компьютерная верстка: *А.С. Михайлова*
Дизайн: *Н.С. Михайлов*

Публикуется в авторской редакции

Подписано в печать 20.10.2021. Формат 60x84⅛. Бумага офсетная.
Печать – ризография. Усл. печ. л. 49,64. Тираж 400 экз. Заказ № 1678
Отпечатано в ООО «ИПЦ «Измайловский»
190005, Санкт-Петербург, Измайловский пр., 18-д

ISBN 978-5-00182-019-2

9 785001 820192 >

ISBN 978_5_00182_019_2

INFORMATION SECURITY OF RUSSIAN REGIONS (ISRR-2021)

XII ST. PETERSBURG INTERREGIONAL CONFERENCE

St. Petersburg, October 27-29, 2021

PROCEEDINGS OF THE CONFERENCE

St. Petersburg

2021

УЧРЕДИТЕЛИ КОНФЕРЕНЦИИ

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

СОУСТРОИТЕЛИ КОНФЕРЕНЦИИ

- Российский фонд фундаментальных исследований
- СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
- Государственный университет морского и речного флота имени адмирала С.О. Макарова
- Национальный исследовательский университет ИТМО
- Российский государственный гидрометеорологический университет
- Санкт-Петербургский государственный морской технический университет
- Санкт-Петербургский государственный университет аэрокосмического приборостроения
- Санкт-Петербургский государственный университет промышленных технологий и дизайна
- Санкт-Петербургский государственный экономический университет
- Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
- Санкт-Петербургский институт экономики и бизнеса
- Санкт-Петербургский научный центр Российской академии наук
- Санкт-Петербургский политехнический университет Петра Великого
- Санкт-Петербургский университет МВД России
- Группа компаний «Марвел»
- АО «Институт инфотелекоммуникаций»
- АО «Концерн «НПО «Аврора»
- АО «Научно-исследовательский институт программных средств»
- АО «Научно-производственное объединение «Импульс»
- АО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
- АО «НИИ «Масштаб»
- АО «Равенство»
- АО «Центр компьютерных разработок»
- ЗАО «Институт телекоммуникаций»
- ООО «Ассоциация специалистов безопасности»
- ООО «Геонавигатор»
- ООО «Лаборатория инфокоммуникационных сетей»
- ООО «НеоБИТ»
- ПАО «ИНТЕЛТЕХ»
- Партнерство для развития информационного общества на Северо-Западе России
- Санкт-Петербургская инженерная академия
- Санкт-Петербургское отделение Академии информатизации образования
- Санкт-Петербургское отделение Международной академии информатизации
- Санкт-Петербургское отделение Общероссийской общественной организации «Академия инженерных наук им. А.М. Прохорова»

КООРДИНАЦИОННЫЙ СОВЕТ КОНФЕРЕНЦИИ

Беглов Александр Дмитриевич	Губернатор Санкт-Петербурга
Бельский Александр Николаевич	Председатель Законодательного собрания Санкт-Петербурга
Дрозденко Александр Юрьевич	Губернатор Ленинградской области
Фальков Валерий Николаевич	Министр науки и высшего образования Российской Федерации
Шадаев Максут Игоревич	Министр цифрового развития, связи и массовых коммуникаций Российской Федерации
Аверьянов Юрий Тимофеевич	Первый заместитель Секретаря Совета Безопасности Российской Федерации
Шерстюк Владислав Петрович	Президент Национальной ассоциации международной информационной безопасности, директор Института проблем информационной безопасности Московского государственного университета им. М.В. Ломоносова, член-корреспондент Академии криптографии РФ

ПРЕЗИДИУМ КОНФЕРЕНЦИИ

Советов Борис Яковлевич	Председатель Президиума конференции, председатель Программного комитета, сопредседатель Научного совета по информатизации Санкт-Петербурга, академик Российской академии образования
Юсупов Рафаэль Мидхатович	Председатель Организационного комитета, научный руководитель Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН, член-корреспондент Российской академии наук
Белов Евгений Борисович	Заместитель председателя Совета УМО вузов России в области информационной безопасности
Ильин Николай Иванович	Заместитель начальника Управления информационных систем Службы специальной связи и информации ФСО России
Казарин Станислав Валериевич	Вице-губернатор Санкт-Петербурга
Красников Геннадий Яковлевич	Академик-секретарь Отделения нанотехнологий и информационных технологий Российской академии наук, академик Российской академии наук
Максимов Андрей Станиславович	Председатель Комитета по науке и высшей школе Санкт-Петербурга
Панкевич Виктор Николаевич	Помощник полномочного представителя Президента Российской Федерации в Северо-Западном федеральном округе
Пешехонов Владимир Григорьевич	Научный руководитель ГНЦ «Центральный научно-исследовательский институт «Электроприбор», академик Российской академии наук
Ронжин Андрей Леонидович	Директор Санкт-Петербургского Федерального исследовательского центра Российской академии наук, профессор РАН
Степура Сергей Николаевич	Руководитель Управления Федеральной службы технического и экспортного контроля по Северо-Западному федеральному округу
Смирнова Юлия Леонидовна	Председатель Комитета по информатизации и связи Санкт-Петербурга
Смирнов Анатолий Иванович	Генеральный директор Национальной ассоциации международной информационной безопасности, председатель Отделения РАЕН «Информационная глобализация»

ОРГАНИЗАЦИОННЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Председатель Организационного Комитета

Юсупов Рафаэль Мидхатович	Научный руководитель Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб НЦ РАН, член-корреспондент Российской академии наук

Заместитель председателя Организационного Комитета

Хоменок Алексей Леонидович	Начальник отдела информационно-компьютерной безопасности Управления информационной и компьютерной безопасности и технической защиты информации Комитета по информатизации и связи Санкт-Петербурга

Члены Организационного Комитета

Алексеев Анатолий Владимирович	Исполнительный директор Института автоматизации процессов борьбы за живучесть корабля, судна, профессор кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета
Антохина Юлия Анатольевна	Ректор Санкт-Петербургского государственного университета аэрокосмического приборостроения
Барышников Сергей Олегович	Ректор Государственного университета морского и речного флота имени адмирала С.О. Макарова
Басков Вячеслав Дмитриевич	Генеральный директор ООО «НеоБИТ»
Блажис Анатолий Константинович	Директор АО «Научно-технический центр биоинформатики и телемедицины «Фрактал»
Бобрович Владимир Юрьевич	Директор по стратегическому и инновационному развитию АО «Концерн «НПО «Аврора»
Богданов Владимир Николаевич	Директор АО «ЦентрИнформ», лауреат Государственной премии Российской Федерации в области науки и техники
Борисов Николай Валентинович	Заведующий кафедрой Санкт-Петербургского государственного университета
Васильев Владимир Николаевич	Ректор Национального исследовательского университета ИТМО, член-корреспондент Российской академии образования, член-корреспондент Российской академии наук
Гаценко Олег Юрьевич	Генеральный директор АО «Научно-исследовательский институт программных средств»
Гирдин Сергей Алексеевич	Президент Группы компаний «Марвел»
Григорьев Владимир Александрович	Генеральный директор ООО «Лаборатория инфокоммуникационных сетей», президент Санкт-Петербургского отделения Общероссийской общественной организации «Академия инженерных наук им. А.М. Прохорова»
Демидов Алексей Вячеславович	Ректор Санкт-Петербургского государственного университета промышленных технологий и дизайна, председатель Совета ректоров вузов Санкт-Петербурга и Ленинградской области
Жданов Сергей Николаевич	Советник генерального директора АО ВТБ Девелопмент по внешним связям
Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций», президент Санкт-Петербургского отделения Академии информатизации образования
Захаров Юрий Никитич	Первый заместитель директора СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Зегжда Петр Дмитриевич	Профессор Института кибербезопасности и защиты информации Санкт-Петербургского политехнического университета Петра Великого

Игумнов Владимир Вячеславович	Советник генерального директора АО «Научно-производственное объединение «Импульс»
Ипатов Олег Сергеевич	Заместитель проректора по научной работе Санкт-Петербургского политехнического университета Петра Великого
Касаткин Виктор Викторович	Ученый секретарь Научного совета по информатизации Санкт-Петербурга, заместитель начальника отдела аспирантуры Санкт-Петербургского Федерального исследовательского центра Российской академии наук
Кефели Игорь Федорович	Директор Центра геополитической экспертизы Северо-Западного института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации
Корниенко Анатолий Адамович	Заведующий кафедрой информатики и информационной безопасности Петербургского государственного университета путей сообщения Императора Александра I
Крупцов Сергей Владимирович	Первый заместитель генерального директора АО «Центр компьютерных разработок»
Кузичкин Александр Васильевич	Заместитель генерального директора по информационным технологиям АО «НИИ телевидения»
Кузьмин Юрий Григорьевич	Ученый секретарь Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления
Кулешов Игорь Александрович	Заместитель генерального директора по научной работе ПАО «ИНТЕЛТЕХ»
Кучерявый Михаил Михайлович	Советник генерального директора АО «Корпорация Московский институт теплотехники» Государственной корпорации «Роскосмос», Государственный советник Российской Федерации 1 класса
Максимцев Игорь Анатольевич	Ректор Санкт-Петербургского государственного экономического университета
Михайлов Николай Семенович	Заместитель генерального директора по информационным технологиям и стратегии развития АО «Равенство»
Михайлова Анна Сергеевна	Заместитель директора Санкт-Петербургского Общества информатики, вычислительной техники, систем связи и управления по связям с общественностью
Михеев Валерий Леонидович	Ректор Российского государственного гидрометеорологического университета
Молдовян Александр Андреевич	Главный научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН
Николашин Юрий Львович	Генеральный директор ПАО «ИНТЕЛТЕХ», генеральный конструктор системы управления ВМФ
Никулин Евгений Николаевич	Ректор Санкт-Петербургского института экономики и бизнеса
Ныркov Анатолий Павлович	Профессор Государственного университета морского и речного флота имени адмирала С.О. Макарова
Оводенко Анатолий Аркадьевич	Президент Санкт-Петербургского государственного университета аэрокосмического приборостроения
Жидков Денис Владимирович	Временно исполняющий обязанности директора СПб ГУП «Санкт-Петербургский информационно-аналитический центр»
Присяжнюк Сергей Прокофьевич	Генеральный директор ЗАО «Институт телекоммуникаций»
Пролетарский Андрей Викторович	Декан Московского государственного технического университета им. Н.Э. Баумана, председатель Федерального УМО по УГСН 09.00.00 «Информатика и вычислительная техника»
Пухов Геннадий Георгиевич	Директор ООО «Геонавигатор»

Силла Евгений Петрович	Ученый секретарь Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН
Смирнов Павел Игоревич	Генеральный директор АО «НИИ «Масштаб»
Солодянников Александр Владимирович	Генеральный директор ООО «Ассоциация специалистов безопасности»
Стрельцов Анатолий Александрович	профессор, ведущий научный сотрудник Института проблем информационной безопасности Московского государственного университета им. М.В. Ломоносова, действительный государственный советник Российской Федерации 3 класса
Тихомиров Сергей Григорьевич	Генеральный директор АО «Центр компьютерных разработок»
Тумарев Владимир Михайлович	Первый заместитель председателя Комитета по информатизации и связи Санкт-Петербурга
Туричин Глеб Андреевич	Ректор Санкт-Петербургского государственного морского технического университета
Устинов Игорь Анатольевич	Советник генерального директора АО «Научно-производственное объединение «Импульс»
Черешкин Дмитрий Семенович	Заведующий лабораторией Института системного анализа Федерального исследовательского центра «Информатика и управление» Российской академии наук
Чугунов Андрей Владимирович	Директор Центра технологий электронного правительства Института дизайна и урбанистики Национального исследовательского университета ИТМО
Шелудько Виктор Николаевич	Ректор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
Шерстюк Юрий Михайлович	Генеральный директор АО «Институт инфотелекоммуникаций»
Шилов Константин Юрьевич	Генеральный директор АО «Концерн «НПО «Аврора»

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Председатель Программного Комитета

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

Заместители председателя Программного Комитета

Тумарев Владимир Михайлович	Первый заместитель председателя Комитета по информатизации и связи Санкт-Петербурга, канд. техн. наук

Члены программного комитета – руководители и секретари секций

Абрамов Максим Викторович	Руководитель лаборатории теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН, канд. техн. наук
Алексеев Анатолий Владимирович	Исполнительный директор НП «Институт автоматизации процессов борьбы за живучесть корабля, судна», профессор кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета, д-р техн. наук, профессор
Беззатеев Сергей Валентинович	Заведующий кафедрой безопасности киберфизических систем Национального исследовательского университета ИТМО, д-р техн. наук, доцент

Бобрович Владимир Юрьевич	Директор по стратегическому и инновационному развитию АО «Концерн «НПО «Аврора», д-р техн. наук, профессор
Браницкий Александр Александрович	Старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН, канд. техн. наук
Бузников Анатолий Алексеевич	Засл. профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), засл. деятель науки РФ, д-р техн. наук, профессор
Верзун Наталья Аркадьевна	Доцент кафедры информационных систем и технологий Санкт-Петербургского государственного экономического университета, канд. техн. наук, доцент
Воробьев Евгений Германович	Заведующий кафедрой информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), д-р техн. наук, доцент
Горохов Владимир Леонидович	Профессор Национального исследовательского университета ИТМО, д-р техн. наук, профессор
Горяинов Виктор Сергеевич	Доцент кафедры фотоники Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук
Дронов Роман Владимирович	Заведующий кафедрой экономической безопасности Санкт-Петербургского государственного экономического университета, д-р экон. наук, канд. юрид. наук, доцент
Жигадло Валентин Эдуардович	Заместитель генерального директора ЗАО «Институт телекоммуникаций», президент Санкт-Петербургского отделения Академии информатизации образования, д-р техн. наук, доцент
Жуланова Дарья Николаевна	Старший преподаватель кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета
Заколдаев Данил Анатольевич	Декан факультета информационной безопасности и компьютерных технологий, заведующий кафедрой проектирования и безопасности компьютерных систем Национального исследовательского университета ИТМО, канд. техн. наук, доцент
Звонов Денис Валерьевич	Первый заместитель генерального директора АО «Научно-производственное объединение «Импульс», канд. техн. наук
Зикратов Игорь Алексеевич	Декан факультета информационных систем и технологий Санкт-Петербургского государственного университета телекоммуникаций им. профессор М.А. Бонч-Бруевича, д-р техн. наук, профессор
Игумнов Владимир Вячеславович	Советник генерального директора АО «Научно-производственное объединение «Импульс», канд. техн. наук
Искандеров Юрий Марсович	Заведующий лабораторией информационных технологий на транспорте Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН, д-р техн. наук, профессор
Истомин Евгений Петрович	Заведующий кафедрой прикладной информатики Российского государственного гидрометеорологического университета, д-р техн. наук, профессор
Кефели Игорь Федорович	Директор Центра геополитической экспертизы Северо-Западного института управления РАНХиГС при Президенте Российской Федерации, засл. работник высшей школы Российской Федерации, д-р филос. наук, профессор

Колбанёв Михаил Олегович	Профессор Санкт-Петербургского государственного экономического университета, д-р техн. наук, профессор
Коршунов Игорь Львович	Заведующий кафедрой информационных систем и технологий Санкт-Петербургского государственного экономического университета, канд. техн. наук, доцент
Котенко Игорь Витальевич	Заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН, д-р техн. наук, профессор
Куприянов Дмитрий Олегович	Студент факультета корабельной энергетики и автоматики Санкт-Петербургского государственного морского технического университета
Ласкин Михаил Борисович	Старший научный сотрудник лаборатории информационных технологий на транспорте Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН, канд. физ.-мат. наук, доцент
Литвинов Владислав Леонидович	Доцент кафедры информационных управляющих систем Санкт-Петербургского государственного университета телекоммуникаций им. профессор М.А. Бонч-Бруевича, канд. техн. наук, доцент
Локнов Алексей Игоревич	Майор полиции, доцент кафедры специальных информационных технологий Санкт-Петербургского университета МВД России, канд. техн. наук
Мельник Галина Сергеевна	Профессор кафедры цифровых медиакоммуникаций Высшей школы журналистики и массовых коммуникаций Санкт-Петербургского государственного университета, д-р полит. наук, профессор
Микадзе Сергей Юрьевич	Проректор Санкт-Петербургского государственного экономического университета, канд. экон. наук
Михайленко Евгений Иванович	Ведущий специалист АО «Научно-производственное объединение «Импульс»
Михайличенко Николай Валерьевич	Преподаватель Военной академии связи им. С.М. Буденного, канд. техн. наук
Молдовян Николай Андреевич	Главный научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН, д-р техн. наук, профессор, засл. изобретатель РФ
Мороз Николай Васильевич	Заместитель директора ООО «Геонавигатор»
Мусатенко Роман Иванович	Руководитель Центра ранговой партнерской сертификации НП «Институт автоматизации процессов борьбы за живучесть корабля, судна», старший научный сотрудник ВУНЦ ВМФ «ВМА»
Новикова Евгения Сергеевна	Доцент кафедры информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ», канд. техн. наук, доцент
Ныркov Анатолий Павлович	Профессор кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, д-р техн. наук, профессор
Паращук Игорь Борисович	Профессор кафедры автоматизированных систем специального назначения Военной академии связи им. С.М. Буденного, д-р техн. наук, профессор, засл. изобретатель РФ
Петренко Сергей Анатольевич	Профессор кафедры информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), д-р техн. наук, профессор

Плебанек Ольга Васильевна	Заведующая кафедрой социально-гуманитарных дисциплин Университета при МПА ЕврАзЭС, д-р филос. наук, доцент
Попов Николай Николаевич	Доцент кафедры информационных технологий и систем безопасности Института информационных систем и геотехнологий Российского государственного гидрометеорологического университета, канд. техн. наук, доцент
Примакин Алексей Иванович	Полковник полиции, начальник кафедры специальных информационных технологий Санкт-Петербургского университета МВД России, д-р техн. наук, профессор
Пухов Геннадий Георгиевич	Директор ООО «Геонавигатор», канд. техн. наук, профессор
Саенко Игорь Борисович	Ведущий научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН, д-р техн. наук, профессор
Свешникова Наталья Олеговна	Доцент кафедры политической психологии факультета психологии Санкт-Петербургского государственного университета, канд. психол. наук, доцент
Созинова Екатерина Николаевна	Доцент кафедры проектирования безопасных компьютерных систем Национального исследовательского университета ИТМО, канд. техн. наук
Соколов Борис Владимирович	Руководитель лаборатории информационных технологий в системном анализе и моделировании Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН, засл. деятель науки России, д-р техн. наук, профессор
Соколов Сергей Сергеевич	Проректор по образовательной деятельности, заведующий кафедрой комплексного обеспечения компьютерной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, д-р техн. наук, доцент
Соколов Сергей Сергеевич	Проректор по учебной работе Государственного университета морского и речного флота имени адмирала С.О. Макарова, д-р техн. наук, доцент
Татарникова Татьяна Михайловна	Директор Института информационных систем и геотехнологий, заведующая кафедрой информационных технологий и систем безопасности Российского государственного гидрометеорологического университета, д-р техн. наук, профессор
Тулупьев Александр Львович	Советник проректора по научной работе, профессор Санкт-Петербургского государственного университета, главный научный сотрудник лаборатории теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН, д-р физ.-мат. наук, доцент
Тюрин Иван Сергеевич	Аспирант Санкт-Петербургского государственного морского технического университета
Устинов Игорь Анатольевич	Советник генерального директора АО «НПО «Импульс», канд. техн. наук
Цехановский Владислав Владимирович	Заведующий кафедрой информационных систем, профессор Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина), канд. техн. наук, доц.
Чугунов Андрей Владимирович	Директор Центра технологий электронного правительства Института дизайна и урбанистики Национального исследовательского университета ИТМО, канд. полит. наук, доц.
Шакин Дмитрий Николаевич	Заместитель руководителя Управления ФСТЭК России по Северо-Западному федеральному округу, канд. воен. наук, доцент

Юсупов Рафаэль Мидхатович	Научный руководитель Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН, член-корреспондент Российской академии наук, засл. деятель науки и техники РФ, д-р техн. наук, профессор
Яковлева Наталья Александровна	Полковник полиции, начальник кафедры математики и информатики Санкт-Петербургского университета МВД России, канд. психол. наук

Ученый секретарь Конференции

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

ПЛЕНАРНЫЕ ДОКЛАДЫ

1. КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ САНКТ-ПЕТЕРБУРГА

Казарин Станислав Валериевич — Вице-губернатор Санкт-Петербурга,

Советов Борис Яковлевич — Сопредседатель Научного совета по информатизации Санкт-Петербурга, академик Российской академии образования

2. АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАЗВИТИЯ СИСТЕМЫ РАСПРЕДЕЛЁННЫХ СИТУАЦИОННЫХ ЦЕНТРОВ В СОВРЕМЕННЫХ УСЛОВИЯХ

Ильин Николай Иванович — Заместитель начальника Управления информационных систем Службы специальной связи и информации ФСО России,

Пухов Геннадий Георгиевич — Директор ООО «Геонавигатор»

3. ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА И МЕНТАЛЬНЫХ ВОЙН

Юсупов Рафаэль Мидхатович — Научный руководитель Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН, член-корреспондент Российской академии наук

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

4. РАЗВИТИЕ ЭКОСИСТЕМЫ БЕЗОПАСНЫХ ЦИФРОВЫХ СЕРВИСОВ САНКТ-ПЕТЕРБУРГА

Поляков Сергей Сергеевич — Заместитель председателя Комитета по информатизации и связи Санкт-Петербурга

5. КИБЕРБЕЗОПАСНОСТЬ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА (МОЖЕТ ЛИ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ОШИБАТЬСЯ?)

Зегжда Петр Дмитриевич — Профессор Института кибербезопасности и защиты информации Санкт-Петербургского политехнического университета Петра Великого

6. ИНТЕЛЛЕКТУАЛЬНЫЕ МЕТОДЫ КОРРЕЛЯЦИИ СОБЫТИЙ КИБЕРБЕЗОПАСНОСТИ: АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ ФУНДАМЕНТАЛЬНЫХ И ПРИКЛАДНЫХ ИССЛЕДОВАНИЙ

Котенко Игорь Витальевич — Руководитель лаборатории проблем компьютерной безопасности, главный научный сотрудник Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН

7. АКТУАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ НЕЙРОСЕТЕВЫХ АЛГОРИТМОВ В СИСТЕМАХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Ложников Павел Сергеевич — Заведующий кафедрой комплексной защиты информации Омского государственного технического университета

8. НОВОЕ ПРАВО XXI ВЕКА И ЦИФРОВАЯ ТРАНСФРМАЦИЯ

Наумов Виктор Борисович — Главный научный сотрудник Санкт-Петербургского Федерального исследовательского центра Российской академии наук

9. МЕНТАЛЬНЫЕ ВОЙНЫ И ИНФОРМАЦИОННО-КОГНИТИВНАЯ БЕЗОПАСНОСТЬ

Кефели Игорь Федорович — Директор Центра геополитической экспертизы Северо-Западного института управления – филиала Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации

10. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Лившиц Илья Иосифович	Профессор Национального исследовательского университета ИТМО
Молдовян Александр Андреевич	Главный научный сотрудник лаборатории кибербезопасности и постквантовых криптосистем Санкт-Петербургского института информатики и автоматизации Российской академии наук СПб ФИЦ РАН

11. ОПЫТ СПБГЭТУ «ЛЭТИ» В РЕАЛИЗАЦИИ ПРОЕКТА СЕЙФНЕТ НАЦИОНАЛЬНОЙ ТЕХНОЛОГИЧЕСКОЙ ИНИЦИАТИВЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Воробьев Евгений Германович	Заведующий кафедрой информационной безопасности Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)

ГОСУДАРСТВЕННАЯ ПОЛИТИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕГИОНОВ РОССИИ

УДК 004.056

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ САНКТ-ПЕТЕРБУРГА

Казарин Станислав Валерьевич[1], Советов Борис Яковлевич[2]
[1]Правительство Санкт-Петербурга
[2] Смольный, Санкт-Петербург, 191060, Россия
[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: bysovetov@mail.ru

Аннотация. Рассматривается идеология построения концепции информационной безопасности Санкт-Петербурга, базирующейся на многолетнем опыте обсуждения ключевых проблем информационной безопасности регионов России, развития научно-педагогических школ, разработки концептуальных документов, обобщения результатов фундаментальных и прикладных исследований и разработок в области информационной безопасности. Обсуждаются цели, принципы, а также методы и средства обеспечения информационной безопасности, рассматривается нормативно-правовая база, понятийный аппарат и научные аспекты стратегии информационной безопасности, сформулированы предложения по развитию приоритетных направлений и решению ключевых проблем в области обеспечения информационной безопасности, опережающей подготовки и переподготовки кадров.

Ключевые слова: информационная безопасность; вызовы угрозы в сфере информационной безопасности; информационный суверенитет; информационно-психологическая и когнитивная безопасность; научное и кадровое обеспечение информационной безопасности; подготовка специалистов в области информационной безопасности; реализация концепции информационной безопасности.

THE CONCEPT OF REGIONAL INFORMATION SECURITY

Kazarin Stanislav[1], Sovetov Boris[2]
[1] Government of St. Petersburg
[2]Smolny, St. Petersburg, 191060, Russia
[2] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: bysovetov@mail.ru

Abstract. The ideology of constructing the concept of information security of St. Petersburg is considered, based on many years of experience in discussing key problems of information security in the regions of Russia, the development of scientific and pedagogical schools, the development of conceptual documents, the synthesis of the results of fundamental and applied research and development in the field of information security. The objectives, principles, as well as methods and means of ensuring information security are discussed, the regulatory framework, conceptual apparatus and scientific aspects of the information security strategy are considered, proposals are formulated to develop priority areas and solve key problems in the field of ensuring information security, advanced training and retraining of personnel.

Keywords: information security; threats to information security; information sovereignty; information, psychological and cognitive security; scientific and personnel information security; training in information security; implementation of the information security concept.

Широкомасштабная цифровая трансформация экономики, государственного управления и социальной сферы в условиях завершения построения информационного общества в России и в мире в целом и перехода к обществу знаний, сопровождающаяся новыми внешними вызовами и угрозами в информационной сфере, обуславливает необходимость совершенствования государственной политики в области региональной, национальной и международной информационной безопасности [1, 2].

В Санкт-Петербурге накоплен значительный опыт в этом направлении [3, 4]: в результате многолетнего обсуждения ключевых проблем информационной безопасности регионов России сформированы и получили развитие научно-педагогические школы, выработан единый терминологический аппарат, разработаны концептуальные документы, проводятся фундаментальные и прикладные исследования и разработки в области информационной безопасности. В настоящее время можно считать сформированной идеологию

информационной безопасности, которую можно рассматривать как основу построения концепции информационной безопасности города, региона, страны и как важную составляющую подхода к формированию политики информационной безопасности.

Для разработки Концепции по инициативе Комитета по информатизации и связи Правительств Санкт-Петербурга была создана рабочая группа, научно-методическое руководство которой было возложено на Научный совет по информатизации Санкт-Петербурга, действующий в структуре Правительства города.

Современная концепция информационной безопасности такого мегаполиса как Санкт-Петербург учитывает особенности второго по величине города страны, крупного промышленного, научного и культурного центра, находящегося на пересечении международных транспортных коридоров, сконцентрировавшего мощный научно-технологический потенциал и занимающий важное геополитическое положение. В структуре концепции информационной безопасности Санкт-Петербурга в качестве основных выделены следующие разделы: современные вызовы и основные угрозы в информационной сфере; состояние информационной безопасности Санкт-Петербурга; цели, задачи и принципы обеспечения информационной безопасности; нормативно-правовые основы обеспечения информационной безопасности; методы и средства обеспечения информационной безопасности Санкт-Петербурга; организационные основы обеспечения информационной безопасности Санкт-Петербурга; научное и кадровое обеспечение информационной безопасности; сотрудничество в сфере информационной безопасности; реализация Концепции информационной безопасности Санкт-Петербурга.

Нормативно-правовой базой для разработки концепции служат: Конституция РФ; Федеральный закон «О безопасности»; Доктрина информационной безопасности Российской Федерации (от 05.12.2016 № 646); Стратегия национальной безопасности Российской Федерации; Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы» (утв. Указом Президента РФ от 09.05.2017 № 203); Стратегия противодействия экстремизму в Российской Федерации до 2025 года (утв. Указом Президента РФ от 29.05.2020 № 344); Устав Санкт-Петербурга; Стратегия экономического и социального развития Санкт-Петербурга на период до 2030 года, а также ряд других важных документов [1, 2].

Особое внимание разработчиками концепции уделено определению элементов понятийного аппарата, в том числе таких объектов информационной безопасности как: государственные и частные информационные ресурсы, информационные системы, базы данных, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, информационная инфраструктура (центры обработки и анализа информации, каналы информационного обмена и телекоммуникации, системы управления телекоммуникационных систем и сетей, технические средства защиты информации) и др.

К числу отличительных особенностей документа следует отнести проблемы, затронутые в концепции информационной безопасности, отражающие научные аспекты стратегии информационной безопасности; базовой модели угроз, модели взаимодействия участников информационной системы; прорывных технологических подходов к решению задач информационной безопасности: обработки нечетких знаний; интеллектуального анализа данных; обработки больших данных; теории и практики построения цифровых двойников и др.

Разработанная концепция существенно отличается от региональных вариантов концепций тем, что, по мнению разработчиков, она носит научно-обоснованный характер, отражает системный подход и охватывает такие составляющие как: информационно-психологическая и когнитивная безопасность, расширенное понимание информационной безопасности, информационного суверенитета, информационного потенциала, информационного иммунитета, ориентирована на опережающее кадровое обеспечение и поддержку развития научно-педагогических школ в области информационной безопасности и др.

Особо следует подчеркнуть необходимость дальнейшей проработки составляющих информационной безопасности с учетом отличительных особенностей обсуждаемого документа, а именно: концепция отражает меры по обеспечению защиты информации и меры по обеспечению защиты от информации. Содержание и актуальность второй составляющей в современных условиях приобретает самостоятельное значение: ее развитие в направлении обеспечения информационно-психологической и когнитивной безопасности открывает возможность решения важной социальной задачи обеспечения информационного суверенитета страны, воспитания подрастающего поколения в духе патриотизма, противодействия внешним угрозам, защиты граждан и, в первую очередь, молодежи от деструктивного информационного воздействия, в том числе враждебной зарубежной идеологии.

Для этого необходимо решение ряда ключевых проблем в области информационной безопасности:

– развитие научно-прикладных основ информационной безопасности, соответствующих сложившимся геополитической ситуации и условиям социально-экономического развития Санкт-Петербурга;

– формирование нормативно-правовой базы обеспечения информационной безопасности, совершенствование механизмов реализации прав граждан на информацию;

– комплексное решение задач выявления новых видов угроз, включая угрозы деструктивного информационного воздействия на жителей города;

– разработка и внедрение перспективных методов и технических средств, обеспечивающих комплексное решение задач информационной безопасности;

– формирование единой системы обеспечения информационной безопасности Санкт-Петербурга, обеспечивающей комплексное решение задач информационной безопасности;

– разработка критериев и методов оценки эффективности систем и средств информационной безопасности и их сертификации;

– исследование и разработка новых форм и способов защиты жителей города от деструктивного информационного воздействия и обеспечения информационно-психологической безопасности населения города;

– разработка и реализация перспективных направлений непрерывной системы опережающей подготовки и переподготовки кадров в области информационной безопасности.

Предложенная идеология информационной безопасности неоднократно апробировалась [5], совершенствовалась и получила одобрение в процессе многократных обсуждений на общественных слушаниях различного уровня с участием представителей органов государственной власти, средств массовой информации, профессиональных научных формирований и научной общественности Санкт-Петербурга.

В Концепции сформулированы основные стратегические цели в области информационной безопасности Санкт-Петербурга, задачи (работы), этапы по реализации Концепции и плана мероприятий по разработке программы создания СОИБ города.

Реализация Концепции позволит:

– оценить реальное состояние информационной безопасности в Санкт-Петербурге;

– наиболее полно выявить источники внутренних и внешних угроз информационной безопасности города;

– выработать и реализовать стратегию и политику обеспечения информационной безопасности в Санкт-Петербурге;

– разработать комплекс нормативно-правовых и организационно-методических документов в области информационной безопасности города;

– стимулировать создание действенной системы обеспечения информационной безопасности мегаполиса.

Стратегической целью Санкт-Петербурга, обладающего высоким научно-технологическим, информационным, образовательным и кадровым потенциалом, является стремление к достижению передовых позиций для обеспечения возможности эффективного использования своих усилий, ресурсов и потенциала (с учетом географического положения и экономических особенностей) в интересах укрепления национальной безопасности России, защиты ее национальных интересов, информационного суверенитета и обеспечения информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 02.07.2021 № 400) // URL: http://publication.pravo.gov.ru/Document/View/0001202107030001?index=1&rangeSize=1 (дата обращения: 31.08.2021).
2. Основы государственной политики Российской Федерации в области международной информационной безопасности (утв. Указом Президента РФ от 12.04.2021 № 213) // URL: http://publication.pravo.gov.ru/Document/View/0001202104120050?index=1&rangeSize=1 (дата обращения: 31.08.2021).
3. Материалы Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2011 –ИБРР-2019)». Под ред. Б.Я. Советова, Р.М. Юсупова, В.В. Касаткина / СПОИСУ. – СПб // URL: http://www.spoisu.ru/conf/ibrr2021 (дата обращения: 31.08.2021).
4. Региональная информатика и информационная безопасность. Сборник трудов. Выпуски 1-9. Под ред. Б.Я. Советова, Р.М. Юсупова, В.В. Касаткина / СПОИСУ. – СПб / СПОИСУ. – СПб // URL: http://www.spoisu.ru/riib (дата обращения: 31.08.2021).
5. Б.Я. Советов, В.В. Касаткин. Идеология построения концепции региональной информационной безопасности // Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет; науч. ред. : Б.В. Соколов. – Севастополь: СевГУ, 2021. – 211с. С. 46-50.

УДК 004.9:351.9

ОЦЕНКА ВОСТРЕБОВАННОСТИ ИНСТРУМЕНТОВ ЭЛЕКТРОННОГО УЧАСТИЯ В САНКТ-ПЕТЕРБУРГЕ: ПО РЕЗУЛЬТАТАМ ОПРОСА СОТРУДНИКОВ ИОГВ

Видясова Людмила Александровна
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: bershadskaya.lyudmila@gmail.com

Аннотация. В докладе представлены основные результаты социологического опроса 354 сотрудников исполнительных органов государственной власти Санкт-Петербурга. Опрос был проведен с целью оценки востребованности инструментов электронного участия, а также их влияния на городское управление. По данным исследования, большинство опрошенных отметили позитивное влияние инструментов электронного участия, реализованных на данный момент, как в контексте взаимодействия с гражданами, так и с точки зрения межведомственного взаимодействия. По результатам опроса была определена приоритетность электронных каналов G2C коммуникации по мнению представителей ИОГВ Санкт-Петербурга.

Ключевые слова: электронное участие; опрос; сотрудники органов власти; каналы коммуникации.

E-PARTICIPATION PORTALS DEVELOPMENT AT THE REGIONAL AND MUNICIPAL LEVEL IN RUSSIA: 2019 MONITORING RESULTS

Vidiasova Lyudmila
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mail: bershadskaya.lyudmila@gmail.com

Abstract. The report presents the main results of a sociological survey of 354 employees of the executive bodies of state power in St. Petersburg. The survey was conducted to assess the relevance of e-participation tools, as well as their impact on urban governance. According to the study, most of the respondents noted the positive impact of the e-participation tools implemented so far, both in the context of interaction with citizens and in terms of interdepartmental interaction. According to the results of the survey, the priority of the electronic channels of G2C communication was determined in the opinion of representatives of the authorities in St. Petersburg.

Keywords: e-participation; survey; government officials; communication channels.

Работа представляет результаты социологического опроса сотрудников исполнительных органов государственных власти Санкт-Петербурга (ИОГВ). Опрос представителей исполнительных органов государственной власти Санкт-Петербурге (полевой этап был организован через Комитет по информатизации и связи - уполномоченный орган, курирующий программы информатизации и построения «умного города» в Санкт-Петербурге) проводился с целью сбора мнений чиновников о влиянии инструментов электронного гражданского участия на городское развитие. Исследование является продолжением направления изучения доверия информационным технологиям в области электронного участия [1, 2].

В опросе приняли участие 354 сотрудника ИОГВ. Объем выборки является пропорциональным по отношению к представленности комитетов в общей численности сотрудников ИОГВ. Были опрошены представители 43 управлений, комитетов, инспекций и служб Санкт-Петербурга. Выборка воспроизводит структуру генеральной совокупности по соотношению руководителей высшего звена и их заместителей, начальников управлений, отделов и секторов ИОГВ к сотрудникам, не занимающих руководящие должности. Первых опрошено 25%, вторых -75%. По полу и возрасту получено случайное распределение. Среди опрошенных - 64% женщин и 36% мужчин. Возрастная структура опрошенных была следующей: 18-25 лет - 7%, 26-35 лет - 34%, 36-45 лет - 30%, 46-55 лет - 19%, 56-64 лет - 9%, 65 и старше лет - 1%.

Респонденты самостоятельно заполняли электронную анкету. После завершения опроса была проведена проверка соблюдений позиций выборки, затем получен текстовый отчет и база данных в формате MS Excel. С помощью Excel проведены простые распределения и проведена визуализация данных, более сложные вычисления (анализ таблиц сопряженности) осуществлялись с помощью программы SPSS. При анкетировании сотрудников ИОГВ Санкт-Петербурга был собран срез мнений о влиянии инструментов электронного гражданского участия на городское развитие.

Большинство опрошенных отметили позитивное влияние инструментов электронного участия, реализованных на данный момент, как в контексте взаимодействия с гражданами, так и с точки зрения внутриведомственного взаимодействия. 82% респондентов отметили, что благодаря инструментам ЭУ улучшилось информирование граждан о деятельности органов власти, 74% отметили рост эффективность взаимодействия ведомств, а 64% отметили позитивные эффекты благодаря более грамотному и четкому распределению ответственности между ведомствами (распределение зон ответственности).

По результатам опроса были определены наиболее и наименее предпочтительные каналы взаимодействия власти и граждан. Порталы сообщений о городских проблемах, открытого бюджета, электронных голосований и опросов были определены как наиболее предпочтительные. Мнение сотрудников ИОГВ по приоритетности использования социальных сетей разделились, а среди наименее предпочтительных инструментов были названы порталы инициативного бюджетирования и краудсорсинга.

По результатам применения всех исследовательских методов были сделаны обобщения, сформулированы результаты динамики политического процесса и принятия государственных решений (public policy) в условиях реализации региональной программы «умного города».

Исследование выполнено за счет гранта Российского фонда фундаментальных исследований (проект №19-311-90031 «Электронное участие граждан в городском управлении на примере Санкт-Петербурга»).

СПИСОК ЛИТЕРАТУРЫ

1. Видясов Е., Видясова Л. Цифровизация в управлении городом: исследование коммуникационных каналов приема и обработки обращений граждан в Петербурге // Журнал исследований социальной политики. 2021. Т. 19. № 1. С. 115-128
2. Видясов Е.Ю., Тенсина Я.Д., Видясова Л.А. Оценка уровней вовлечения граждан в развитие городской среды в Петербурге: результаты экспертного опроса // Информационные ресурсы России. 2021. № 3(181). С. 8-10.

УДК 004

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ УЧАСТИЯ ГРАЖДАН В ЭЛЕКТРОННОМ ИНИЦИАТИВНОМ БЮДЖЕТИРОВАНИИ НА УРОВНЕ МЕСТНОГО САМОУПРАВЛЕНИЯ

Голубева Анастасия Алексеевна, Бакалец Дарья Андреевна, Гиленко Евгений Валерьевич
Санкт-Петербургский государственный университет, Высшая школа менеджмента
Волховский пер., 3, Санкт-Петербург, 199004, Россия
e-mails: golubeva@gsom.spbu.ru, d-bakalets@mail.ru, e.gilenko@gsom.spbu.ru

Аннотация. В центре внимания пилотного исследования находится изучение факторов, влияющих на намерение граждан участвовать в инициативном бюджетировании через электронные каналы участия. На базе классификации факторов участия, выявленных в предыдущих исследованиях, построена концептуальная модель факторов участия граждан в электронном инициативном бюджетировании, включающая в себя три блока факторов: отношение граждан к электронным каналам вз аимодействия с органами государственной власти и местного самоуправления, социальный капитал граждан на территории муниципального образования, и мотивация граждан участвовать в электронном инициативном бюджетировании. Для проверки взаимосвязи и влиянии различных факторов на намерение граждан участвовать в инициативном бюджетировании проведено эмпирическое исследование. Для этого была разработана анкета и организован опрос населения Южно-Приморского муниципального округа в Санкт-Петербурге. Далее, на базе проведенного опроса 259 человек, предложенная модель факторов была оценена при помощи метода структурного моделирования уравнений PLS-SEM.

Ключевые слова: электронное участие; инициативное бюджетирование; местное самоуправление; моделирование структурными уравнениями.

PROBLEMS AND PERSPECTIVES OF CITIZENS' PARTICIPATION IN ELECTRONIC PARTICIPATORY BUDGETING ON MUNICIPAL LEVEL

Golubeva Anastasia, Bakalets Daria, Gilenko Evgenii
Saint Petersburg State University, Graduate School of Management
3 Volkhovskiy per., St. Petersburg, 199004, Russia
e-mails: golubeva@gsom.spbu.ru, d-bakalets@mail.ru, e.gilenko@gsom.spbu.ru

Abstract. This pilot study focuses on the factors influencing the intention of citizens to be involved in participatory budgeting (PB) on the municipal level via different electronic communication channels. Having classified such factors based on a literature review, we construct a comprehensive model of citizens' participation in electronic PB (e-PB) which comprises the following three blocks of factors: (1) citizens' attitude towards various electronic communication channels with public authorities; (2) citizens' social capital (as related to their municipality); (3) citizens' motivation to participate in e-PB. To empirically verify interconnections and influence of different factors on citizens' involvement in e-PB, we conducted a survey. To this end, we developed a questionnaire to poll the inhabitants of the Yuzhno-Primorskiy municipality of St. Petersburg. Using the collected information on 259 respondents, the developed model was estimated using the partial least squares structural equation modeling approach (PLS-SEM).

Keywords: electronic participation; participatory budgeting; local government; structural equation modeling.

В рамках данной работы была предложена концептуальная модель участия граждан в инициативном бюджетировании (далее – ИБ) через электронные каналы участия. В качестве главной зависимой переменной в Модели факторов выступает намерение гражданина участвовать в электронном ИБ, переменные, влияющие на намерение, в свою очередь, разделены на три теоретических блока: социальный капитал, мотивация к участию в ИБ и отношение к электронным каналам взаимодействия с органами государственной власти и местного самоуправления. Остальные переменные представлены в Модели факторов в качестве контрольных.

Группа факторов социального капитала

Три ключевых аспекта социального капитала широко обсуждаются в литературе [1-3]: доверие, социальные связи и нормы. Именно они легли в основу подхода, на основе которого в Модели измеряется социальный капитал, заданный как латентная переменная (соответствующие измеряемые переменные – доверие органам местного самоуправления, доверие людям в местном сообществе, взаимодействие с людьми из местного сообщества, идентификация с местным сообществом, приверженность местному сообществу, коллективная эффективность членов местного сообщества).

Группа факторов мотивации к участию в ИБ

Данный блок факторов представляет собой пирамиду, отражающую степень «мотивации» граждан к участию в ИБ. Таким способом, факторы мотивации участия граждан в ИБ, выделяемые в литературе [4-8], были расположены иерархически – от базовой осведомленности до мотиваторов участия в ИБ самого высокого порядка, таких как гражданский долг, желание влиять и желание внести вклад в общее благо.

Группа факторов отношения к электронным каналам

К данной группе факторов были отнесены ожидаемая эффективность, ожидаемые усилия, отношение к использованию электронных каналов, содействующие условия (такие как, например, удобство интерфейса), воспринимаемая надежность [1,3,9].

Для оценки модели было использовано программное обеспечение semPLS. Полученные результаты позволили сделать ряд выводов о выявленных закономерностях. Как можно увидеть, самым существенным блоком факторов в определении намерения граждан участвовать в э-ИБ будет мотивация к данному участию. Путевой коэффициент между мотивацией и намерением является самым высоким по значению (+0,62), чем было доказано первостепенное влияние мотивационной составляющей на намерение. Следующий по значению путевой коэффициент (+0,47) характеризует статистически значимое положительное влияние социального капитала на мотивацию к участию в э-ИБ, которая, в свою очередь, и определяет намерение участвовать. Далее по значению следует коэффициент, определяющий статистически значимое положительное влияние отношения к электронным каналам на мотивацию к участию в э-ИБ (+0,35).

В работе продемонстрировано, что мотивация граждан оказывает приоритетное статистически значимое влияние на намерение граждан участвовать в инициативном бюджетировании. Наличие выявленных при проверке модели эффектов медиации подтвердило влияние социального капитала и отношения к электронным каналам на мотивацию граждан к участию в электронном ИБ. На основе полученных результатов оценки модели факторов были разработаны рекомендации для органов местного самоуправления Южно-Приморского муниципального округа. Ожидается, что с помощью предоставленных рекомендаций по организации и продвижению практики ИБ среди местного населения Администрация округа сможет повысить привлекательность данной практики для граждан и их вовлеченность в процесс участия.

Общие статистические результаты, полученные в ходе проведенного исследования, а также рекомендации, разработанные на их основе, безусловно ограничены спецификой выборки и используемым инструментарием. Однако даже они проливают свет на логику формирования мотивации граждан к участию в ИБ и задают направления следующих исследований в этой области, среди которых кластеризация потребителей, работа с каналами коммуникации и продвижения практики ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Naranjo-Zolotov M. et al. Examining social capital and individual motivators to explain the adoption of online citizen participation // Future Generation Computer Systems. 2019a. Vol. 92. P. 302–311.
2. Naranjo-Zolotov M., Oliveira T., Casteleyn S., Irani Z. Continuous usage of e-participation: The role of the sense of virtual community // Government Information Quarterly. 2019. Vol. 36 (3). P. 536–545.
3. Choi J-C., Song C. Factors explaining why some citizens engage in E-participation, while others do not // Government Information Quarterly. 2020. Vol. 37 (4). Article 101524.
4. Zepic R., Dapp M., Krcmar H. Participatory Budgeting without Participants: Identifying Barriers on Accessibility and Usage of German Participatory Budgeting, 2017 // Conference for E-Democracy and Open Government (CeDEM), Krems, 2017. P. 26-35.
5. Švaljek S., Rašić Bakarić I., Sumpor M. Citizens and the city: the case for participatory budgeting in the City of Zagreb // Public Sector Economics. 2019. № 43, br. 1. P. 21-48.
6. Schneider S.H. Bürgerhaushalte in Deutschland. Individuelle und kontextuelle Einflussfaktoren der Beteiligung. Springer, 2018. VS. 341, S. 54, 99.
7. Porten-Cheé P., Frieß D. What Do Participants Take Away from Local eParticipation?: Analyzing the Success of Local eParticipation Initiatives from a Democratic Citizens' Perspective // Analyse & Kritik. 2018. Vol. 40 (1). P. 1-30.
8. Montambeault F. Participatory citizenship in the making? The multiple citizenship trajectories of participatory budgeting participants in Brazil // Journal of Civil Society. 2016. Vol. 12 (3). P. 282-298.
9. Naranjo-Zolotov M., Oliveira T., Casteleyn S. Citizens' intention to use and recommend e-participation: Drawing upon UTAUT and citizen empowerment // Information Technology & People. 2019. Vol. 32 (2). P. 364-386.

УДК 378.14

ЗАДАЧИ И ФУНКЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА И «МЕНТАЛЬНЫХ» ВОЙН

Жигадло Валентин Эдуардович
ЗАО «Институт телекоммуникаций»
Кантемировская ул., 5М, Санкт-Петербург, 194100, Россия
e-mail: zve@mail.ru

Аннотация. В тезисах доклада рассматриваются основы методологии информационной безопасности, новые задачи и функции информационной безопасности в условиях информационного противоборства и «ментальных» войн, обосновывается значимость и задачи информационно-психологической и когнитивной безопасности. Проводится анализ стратегии национальной безопасности Российской Федерации в части вопросов информационной безопасности. Особое внимание уделяется вопросам существенного изменения подходов к подготовке кадров, учету в процессе обучения непрерывного характера образования и его междисциплинарного характера, а также вопросам воспитания детей в духе традиционных русских ценностей и патриотизма, повышения цифровой грамотности, реализации методов цифровой гигиены, как в среде педагогического состава школы и ВУЗа, так и в среде школьников и студентов.

Ключевые слова: цифровые технологии; информационные технологии; информационная безопасность; защита информации; защита от информации; цифровая гигиена.

TASKS AND FUNCTIONS OF INFORMATION SECURITY IN THE CONDITIONS OF INFORMATION CONFRONTATION AND "MENTAL" WARS

Zhigadlo Valentin
JSC "Institute of Telecommunications"
5M Kantemirovskaya St, St. Petersburg, 194100, Russia
e-mail: zve@mail.ru

Abstract. The theses of the report consider the basics of the methodology of information security, new tasks and functions of information security in the conditions of information confrontation and "mental" wars, substantiate the importance and tasks of information-psychological and cognitive security. The analysis of the national security strategy of the Russian Federation in terms of information security issues is carried out. Special attention is paid to the issues of significant changes in approaches to personnel training, taking into account the continuous nature of education and its interdisciplinary nature in the learning process, as well as issues of raising children in the spirit of traditional Russian values and patriotism, improving digital literacy, implementing digital hygiene methods, both among the teaching staff of schools and universities, and among schoolchildren and students.

Keywords: digital technologies; information technologies; information security; information protection; information protection; digital hygiene.

В настоящее время, в условиях усиливающегося информационного противоборства против России развернута и ведется необъявленная информационная война, направленная на уничтожение самосознания, изменение ментальной (цивилизационной) основы нашего государства, в крайне агрессивной форме ее проявления – когнитивной (ментальной) войны, направленной на деструкцию (изменение) мироощущения, миропонимания и целостного мировоззрения жителей [1]. Под воздействием когнитивных операций осуществляется манипуляция сознанием и навязывание ложных убеждений. Результатом когнитивных операций является инверсия убеждений, мировоззрения и идеологических ориентиров. Если в классических войнах целью является уничтожение живой силы противника, а в современных кибервойнах - уничтожение инфраструктуры противника, то целью новой когнитивной (ментальной) войны является манипуляция сознанием, уничтожение самосознания, изменение ментальной (цивилизационной) основы общества, разрушение мировоззрения. И если живую силу и инфраструктуру можно восстановить, то «ход эволюции сознания повернуть вспять невозможно, тем более что последствия этой "ментальной" войны проявляются не сразу, а только как минимум через поколение, когда сделать уже что-либо будет просто невозможно" [1].

Поэтому несомненным приоритетом и значимостью обладает задача разработки концепции информационной безопасности, определяющей принципы построения и структуру региональной системы ИБ, официальные взгляды на цели, задачи, принципы и основные направления которой изложены в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646 [2]. Существенно возрастает роль и значение информационной безопасности, в частности, для задач защиты всего населения и, в первую очередь, молодежи от деструктивного информационного воздействия. Данным вопросам особое внимание уделено так же в Стратегии национальной безопасности Российской Федерации [3], где информационной безопасности посвящен целый раздел и определено, что целью обеспечения информационной безопасности является укрепление суверенитета Российской Федерации в информационном пространстве.

В докладе подробно рассматриваются новые свойства ИБ, определяющие двойственный характера воздействия информации на человека и социальную среду, и, соответственно, новые задачи защиты от деструктивного, разрушительного воздействия информации. Отмечается важность развития и формирования в недрах теории информационной безопасности новой ее междисциплинарной составляющей – информационно-психологической и когнитивной безопасности (ИПКБ). Сформулированы цели, задачи и методы информационно-психологической и когнитивной безопасности, направленные на формирование устойчивого иммунитета к существующим и вновь возникающим угрозам деструктивного информационного воздействия на население страны и, как следствие, обеспечение государственного суверенитета в информационном пространстве страны.

Подробно анализируются механизмы реализации функций ИБ, обеспечивающие формирование государственного суверенитета в информационном пространстве на региональном уровне. Рассматривается структура потенциалов страны, развитие которых обеспечит формирование устойчивого иммунитета против деструктивного информационного воздействия и, как следствие, укрепление государственного суверенитета в региональном информационном пространстве.

Показано, что методология ИБ получила дальнейшее развитие, в состав которой, помимо задач защиты информации и обнаружения угроз и уязвимостей объекта защиты, впервые включена задача обеспечения информационно-психологической и когнитивной безопасности населения и, в первую очередь, молодежи от деструктивного информационного воздействия.

В докладе проводится детальный анализ основных положений Стратегии национальной безопасности Российской Федерации и, в частности, раздела, посвященного информационной безопасности. Обращается внимание на крайне актуальную задачу - развитие на практике тех изменений, что приняты в Стратегии национальной безопасности Российской Федерации. Отмечается, что базовым предположением о характере

процессов в сфере национальной безопасности страны отныне подразумевается принципиальная неразделимость внутренних и внешних вызовов — ментальных прежде всего. Сбережение российского народа как особой цивилизации, защита наших духовно-нравственных ценностей — в фокусе Стратегии. Поэтому подходы к обеспечению национальной безопасности должны учитывать цивилизационный масштаб вызовов и угроз, нарастающую сложность разделения военно-силовых и невоенных рисков [4]. Базовым принципом обновленной Стратегии становится опережающий характер противодействия, основанный на единой системе прогнозирования и предупреждения угроз нашей цивилизации во всех сферах: образовании, культуре, экологии экономике, науке и обороне [4]. По этой причине обращается внимание на крайне актуальную задачу - развитие и доктринальное закрепление концепции ментальной войны и обновленных методологических основ информационной безопасности, включающих в свой состав ИПКБ.

Одной из ключевых задач информационно-психологической и когнитивной безопасности и обеспечения суверенитета страны в информационном пространстве выделяется задача подготовки кадров в области информационно-психологической и когнитивной безопасности и повышения общего образовательного уровня населения в области информационной безопасности.

В докладе подробно анализируется методология образования в области информационной безопасности. Внимание обращается на необходимость обеспечения организации непрерывного образовательного процесса при изучении вопросов информационно-психологической и когнитивной безопасности, начиная с младших классов начальной школы и заканчивая пост вузовской подготовкой, и на его междисциплинарный характер. Отмечается особая важность и актуальность в современных условиях вопросов возвращения в учебный процесс функции воспитания во всех его аспектах (воспитания подрастающего поколения в духе традиционных русских ценностей и патриотизма), повышения цифровой грамотности и реализации методов цифровой гигиены, повышения уровня культуры в целом, как в среде педагогического состава образовательных учреждений, так и в среде обучаемых.

СПИСОК ЛИТЕРАТУРЫ

1. А. М. Ильницкий. Безопасность страны как фундамент развития. М.: «Арсенал Отечества», № 1 (51), 2021
2. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 [2].
3. Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400
4. А. М. Ильницкий. Ментальная война России. М.: «Военная мысль», № 8, 2021
5. Р. М. Юсупов, В. Э. Жигадло. О проблемах защиты от разрушительного воздействия информации. //Перспективные направления развития отечественных информационных технологий. Материалы конференции, Ч. 1., Севастополь, 22-26 сентября 2020 г. /Севастопольский государственный университет, науч. ред. Б.В. Соколов. – Севастополь: 2020. 305с., С.35-37.

УДК 004.056

ПРОТИВОДЕЙСТВИЕ КИБЕРУГРОЗАМ НА ОСНОВЕ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УСЛОВИЯХ ПАНДЕМИИ

Касаткин Виктор Викторович[1], Советов Борис Яковлевич[2]
[1] Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
14 линия, 39, Санкт-Петербург, Россия
[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
Профессора Попова ул., 5, Санкт-Петербург, Россия
e-mails: v.v.kasatkin@iias.spb.su, bysovetov@mail.ru

Аннотация. Анализируются причины роста киберпреступности, связанные с массовым переходом работников предприятий на удаленный режим работы в условиях пандемии. Рассматриваются задачи выявления киберугроз и типы систем искусственного интеллекта, применяемых в сфере обеспечения информационной безопасности предприятий. Обсуждаются примеры и результаты использования технологий искусственного интеллекта в системах обнаружения кибератак на корпоративные информационные системы и предложения по разработке профильных программ повышения квалификации руководителей и специалистов предприятий.

Ключевые слова: информационная безопасность; киберпреступления; корпоративные информационные системы; искусственный интеллект; подготовка и переподготовка разработчиков интеллектуальных систем и технологий.

COUNTERING CYBER THREATS THROUGH THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN PANDEMIC CONDITIONS

Kasatkin Viktor[1], Sovetov Boris[2]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences
39 14th Line Str., St. Petersburg, Russia
[2] The St. Petersburg State Electrotechnical University «LETI»
5 Professor Popov str., Str. Petersburg, Russia
e-mails: v.v.kasatkin@iias.spb.su, bysovetov@mail.ru

Abstract. The reasons for the growth of cybercrime associated with the mass transition of enterprise workers to a remote mode of work in pandemic conditions are analyzed. The tasks of identifying cyber threats and types of artificial

intelligence systems used in the field of ensuring the information security of enterprises are considered. There are discussed examples and results of using artificial intelligence technologies in systems for detecting cyberattacks on corporate information systems and proposals for developing specialized training programs for managers and specialists of enterprises.

Keywords: information security; cybercrime; corporate information systems; artificial intelligence; training and retraining of intelligent systems and technology developers.

Массовый переход работников предприятий и организаций на удаленный режим работы в условиях пандемии привел к расширению круга общения исполнителей и негативным последствиям, связанным с появлением новых вызовов и угроз информационной безопасности [1]. Это привело к необходимости оперативного реагирования на киберинциденты, а также оперативного анализа аномальных ситуаций на основе обработки больших объемов данных и машинного обучения. При этом сохранились основные признаки, позволяющие относить возникающие угрозы с традиционным типам: угрозам конфиденциальности, целостности, доступности, угрозам естественным и искусственным, внешним и внутренним и др.

Рост киберпреступности на фоне пандемии обусловлен целым рядом причин, связанных с резким увеличением числа удаленных рабочих мест вне защищенного периметра предприятия, возрастанием трафика информационного обмена и электронного документооборота, расширением многообразия видов и путей внедрения вредоносного программного обеспечения в инфраструктуру предприятий, наличием уязвимостей в используемых средствах организации видеоконференций, активным использованием злоумышленниками методов социальной инженерии, неудовлетворительным состоянием организационного обеспечения удаленного режима работы с учетом специфики предприятия и т.д. Следует отметить, что использование ИКТ в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества рассматривается не только как угроза безопасности граждан, общества и государства в рамках Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 02.07.2021 № 400, но и официально отнесено к числу основных угроз международной кибербезопасности [2].

В настоящее время при обеспечении информационной безопасности предприятий к числу наиболее востребованных могут быть отнесены задачи:

– поиска информации о возможных угрозах извне, что требует выявления признаков потенциальных угроз со сторон злоумышленников;

– выявления информации о возможных угрозах изнутри на основе изучения поведения сотрудников и в случаях необходимости блокировки их необъяснимых действий;

– контроля за сетевыми подключениями и информационным взаимодействием сотрудников между собой и с внешними лицами через локальные сети или с использованием интернета;

– организации защищенного доступа сотрудников, работающих в удаленном режиме, к корпоративным ресурсам предприятия.

Опыт использования систем искусственного интеллекта в целях обеспечения информационной безопасности показал: 64 % предприятий с оборотом $1 млрд. утверждают, что внедрение технологий искусственного интеллекта значительно повышает эффективность обнаружения атак; 75 % предприятий отмечают сокращение времени реагирования на выявленные угрозы. К настоящему времени сформировались следующие типы систем искусственного интеллекта, эффективно функционирующих в сфере информационной безопасности:

– системы обнаружения атак на рабочих станциях;
– системы обнаружения атак на сетевом уровне;
– системы анализа поведения пользователей и сущностей информационных систем;
– системы выявления угроз на ранних стадиях на основе обработки больших данных;
– системы мониторинга сетевой структуры информационных систем;
– самообучающиеся системы автоматического выявления угроз информационной безопасности.

Опыт внедрения подобных систем показал значительное повышение показателей, характеризующих эффективность обеспечения информационной безопасности на основе применения технологий искусственного интеллекта. По разным оценкам, скорость анализа и выявления угроз повышается на 17-60 %. Кроме этого наблюдается сокращение расходов на содержание управленческого аппарата. Одновременно системы искусственного интеллекта подобного назначения оказываются менее подверженными атакам по причине сложности и дороговизны оборудования, необходимого для инициирования подобных атак.

В то же время ряд кампаний, например, Google призывают к определенной осторожности при использовании подобных систем искусственного интеллекта по причине недостаточной изученности последствий их применения и проблемы, в целом. На современном этапе сформировано правило: если можно не использовать, то не используйте искусственный интеллект в системах борьбы с угрозами. Его суть заключается в том, что системы искусственного интеллекта, используемые для обеспечения информационной безопасности, достаточно сложны и сами могут преднамеренно или случайно явиться источником угроз, выявление которых на основе применения традиционных методов и средств может быть существенно затруднено.

Результаты научных исследований и прикладных разработок, базирующихся на применении искусственного интеллекта в сфере противодействия киберугрозам, в том числе в задачах моделирования

кибератак, управления рисками с использованием методов машинного обучения, внедрения методов киберразведки на основе активного выявления и превентивного предотвращения угроз, недостаточно широко освещаются в литературе, в том числе в силу специфики отдельных областей специального применения таких систем.

В целом, развитие технологий искусственного интеллекта и их широкое внедрение в инфраструктуру информационной безопасности предприятий следует считать неизбежным и весьма перспективным, в первую очередь при решении задач противодействия различным формам киберпреступности, включая кибертерроризм; создания и внедрения превентивных методов и средств выявления вредоносных программ; обеспечения информационной безопасности информационных систем различного назначения, а также компонентов инфраструктур, в том числе критически важных объектов и систем; защиты интеллектуальной собственности и др. Можно утверждать, что вынужденный переход работников предприятий и организаций на удаленный режим работы в условиях пандемии в определенной мере мотивировал работодателей на целенаправленное принятие мер, направленных на минимизацию рисков возникновения новых угроз безопасности информации, защиты информационных ресурсов и совершенствования систем информационной безопасности предприятий, в том числе на основе внедрения передовых методов и технологий.

В докладе обсуждаются примеры и результаты использования технологий искусственного интеллекта в системах обнаружения кибератак на корпоративные информационные системы и ресурсы, в том числе в системах проактивного поиска и обнаружения угроз, интерес к которым возрастает в связи с неопределенностью прогнозов развития пандемии и ростом числа киберпреступлений. Рассматриваются предложения по разработке содержания профилей основных [3, 4] и ряда дополнительных образовательных программ подготовки разработчиков интеллектуальных систем и технологий с включением указанных результатов в соответствующие разделы программ повышения квалификации руководителей и специалистов предприятий.

СПИСОК ЛИТЕРАТУРЫ

1. Удаленный режим работы в условиях пандемии COVID-19: руководство для работодателей // URL: https://www.garant.ru/products/ipo/prime/doc/74483214/ (дата обращения: 31.08.2021).
2. Указ Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // URL: https://www.garant.ru/products/ipo/prime/doc/400473497/ (дата обращения: 31.08.2021).
3. Советов Б.Я., Касаткин В.В. Цифровой инженер как путь профессионализации подготовки специалистов по разработке информационных систем и технологий и обеспечению информационной безопасности // Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2019 г.: Материалы конференции. / СПОИСУ. – СПб, 2019. – 596 с. С. 525-526.
4. Б.Я. Советов, В.В. Касаткин. Перспективные направления подготовки кадров в области искусственного интеллекта // Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет; науч. ред. : Б.В. Соколов. – Севастополь: СевГУ, 2021. – 211с. С. 102-106.

УДК 004.9

РЕШЕНИЕ ГОРОДСКИХ ЗАДАЧ ЧЕРЕЗ ВОВЛЕЧЕННОСТЬ ГРАЖДАН: ОПЫТ ПРОЕКТИРОВАНИЯ ЦИФРОВОЙ КРАУДСОРСИНГ-ПЛАТФОРМЫ

Локтев Егор Михайлович
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: loktev@lok-tech.com

Аннотация. Анализируются подходы к решению городских задач с помощью методологии краудсорсинга с помощью цифровых платформ. Определяются функциональные и структурные требования к краудсорсинг-платформе.

Ключевые слова: краудсорсинг; общественное участие; проектирование информационных систем.

URBAN SOLUTIONS WITH CIVIC ENGAGEMENT: CROWDSOURCING DIGITAL PLATFORM DESIGN

Loktev Egor
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mail: loktev@lok-tech.com

Abstract. Crowdsourcing methodology is considered support of urban issues solutions. Functional requirements are listed and system design is described.

Keywords: crowdsourcing; civic engagement; system design.

Краудсорсинг как технология привлечения широкого круга лиц к решению задач может быть эффективно использован при работе с проблемами развития городских пространств. Пользователями городской среды являются жители, поэтому для удовлетворения их запросов может быть применен анализ спроса с помощью цифровой платформы, агрегирующей запросы горожан, связанные с развитием и содержанием городских территорий. Вознаграждением для участников становится развитие среды в соответствии с реальным запросом,

что является более значимой наградой, нежели материальные стимулы, для граждан с активной жизненной позицией. Тем самым краудсорсинг выступает социальным механизмом включения граждан в развитие общества и территорий [1]. Из российских регионов эту технологию активно использует Москва [2] и имеется опыт применения в других городах.

Краудсорсинг реализует четыре базовых метода: создание объектов, поиск решений, обработка объектов, оценка объектов. В результате создания объектов, участники создают проекты в соответствии с поставленной задачей, при этом дальнейший отбор лучшего решения может осуществлять всем сообществом, экспертной комиссией или использоваться каждый созданный проект. Поиск решений подразумевает изыскания по проблеме, результатом является лучшее решение поставленной задачи. При этом важно задачей является формулирование критериев выбора лучшего решения.

К задачам, которые могут быть решены с использованием краудсорсинг-платформы относятся:

- сбор идей по развитию и обсуждение проектов модернизации городских пространств;
- общественная экспертиза городских проектов;
- агрегация проблем городских пространств с возможным поиском путей их решения;
- многоцелевой сбор данных и их последующая обработка;
- другие задачи, актуальные для развития города, или решения неких проблем.

Для обозначенных задач наиболее подходят такие методы как создание объектов, поиск решений и обработка объектов.

Для успешного внедрения краудсорсинг-платформы необходимо обеспечить ее доступность для широкого круга лиц, следовательно, взаимодействие с ней должно осуществляться посредством браузера без необходимости установки дополнительного программного обеспечения с настольных и/или мобильных устройств. С нашей точки зрения, краудсорсинг-платформа должна быть реализована в модульной архитектуре для обеспечения возможности расширения функционала, в том числе, создания мобильных приложений.

В процессе проектирования платформы определены структурные требования к системе. Основным компонентом является виртуальный проектный офис, обеспечивающий функциональность управления краудсорсинг-проектами. Компонент реализует возможности создания проектов, управления проектами, обеспечения их жизненного цикла. Требования к компоненту следуют из структуры сущности проекта. Основной структурной единицей проекта является этап. Проект может состоять из следующих этапов: сбор предложений (участники размещают свои предложения и комментируют чужие), оценка объектов (в том числе результатов этапа сбор предложений), создание решения (организатором определяются подробные критерии решения задачи (значительно более узкие, нежели чем на этапе «сбор предложений», например, может включать требование представления технико-экономического обоснования), участники размещают собственные решения и не могут просматривать решения других участников). Жизненный цикл проекта состоит из одного или нескольких этапов в зависимости от решаемых в рамках проекта задач, а также служебного обязательного этапа - определение победителей. Компонент обеспечивает возможность составления проекта из необходимых этапов, установки условий для участников, временных рамок и прочих требований, а также возможность генерации контента участниками проекта, комментирования и оценки контента. Дополнительно компонент обеспечивает возможность разграничения доступа пользователей к проекту в целом и к отдельным этапам.

Для обеспечения релевантности генерируемого пользователями контента требуется реализация компонента модерации и фасилитации. Компонент состоит из автоматических функций обработки контента: анализа тональности, исключение обсценной лексики и некорректного поведения пользователей, и функций ручной фасилитации и модерации. Ручная обработка заключается в отправке пользовательского контента на проверку модератором платформы и фасилитаторам проекта в случае срабатывания функций предотвращения нежелательного поведения пользователей. Также компонент обеспечивает возможности фасилитации дискуссий в цифровом формате: выделение приоритетных направлений изысканий участников, повышение продуктивности коммуникаций с помощью служебных комментариев.

Помимо вышеобозначенных элементов проектируемой платформы, необходима реализация компонента управления пользователями и их личных кабинетов. Компонент обеспечивает возможность авторизации и регистрации на платформе. Для городских задач особенно важно подтверждение отношения пользователя к конкретному месту проживания или регистрации, задача может быть решена путем интеграции платформы с Единой системой авторизации и аутентификации. Дополнительно компонент обеспечивает возможность управления ролями пользователей, корректирования информации о пользователях, а также временной или постоянной блокировки пользователей.

В рамках определения направлений перспективного развития проектируемой краудсорсинг-платформы можно обозначить интеграцию с государственными информационными системами для исключения дублирования информации и функций (например, портал “Наш Санкт-Петербург”, “Единый портал обращений граждан”).

Таким образом, минимально необходимая структура краудсорсинг-платформы включает три основных компонента: проектный офис, компонент модерации и фасилитации, компонент управления пользователями. На наш взгляд, технологии краудсорсинга могут быть эффективно использованы для решения городских задач, путем создания цифровой коммуникационной платформы, реализующей отдельные методы краудсорсинга. Предполагается, что платформа будет обеспечивать перечисленные функциональные возможности и архитектурные подходы для эффективного достижения цели.

Работа выполняется в рамках магистерской работы в рамках образовательной программы Университета ИТМО «Цифровые технологии умного города».

СПИСОК ЛИТЕРАТУРЫ

1. Абагеро Д.Д. Социальные механизмы включения индивида в коммуникативное пространство города // Социодинамика. 2020. № 2. С. 35-45. DOI: 10.25136/2409-7144.2020.2.32264 URL: https:// nbpublish.com/library_read_article.php?id=32264.
2. Казакова Н. Д., Денисова Ж. А. Технология краудсорсинга в государственном региональном управлении (на примере краудсорсинг-проектов правительства города Москвы) // Власть. 2016. №4. С. 21-28.

УДК 351/354 (470)

НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОССИИ: ДИНАМИКА ПРИОРИТЕТОВ

Казанцев Виктор Прокопьевич[1], Поправко Елена Александровна[2]
[1] Университет «РЕАВИЗ»
Калинина ул., 8/2А, Санкт-Петербург, 199098, Россия
[2] Военная академия материально-технического обеспечения имени генерала армии А. В. Хрулёва
Макарова наб., 8, Санкт-Петербург, 199034, Россия
e-mails: smunspb@rambler.ru, elena_popravko@mail.ru

Аннотация. В статье исследуется динамика представлений о национальной безопасности в Российской Федерации, отраженная в Концепции 1997 г. и Стратегиях 2009, 2015, 2021 гг. Авторы уделяют внимание внешним и внутренним факторам, повлиявшим на изменения в определении как самого понятия, так и практического определения приоритетов национальной безопасности в 1990-е – 2021 гг.

Ключевые слова: национальная безопасность; концепция; стратегия; угроза; национальные приоритеты; Российская Федерация.

NATIONAL SECURITY OF RUSSIA: DYNAMICS OF PRIORITIES

Kazantsev Viktor[1], Popravko Elena[2]
[1] University «REAVIZ»
8/2A Kalinina St, St. Petersburg, 199098, Russia
[2] Army General A.V. Khrulev Military Academy of Logistics
8 Makarova Emb, St. Petersburg, 199034, Russia
e-mails: smunspb@rambler.ru, elena_popravko@mail.ru

Abstract. In the article was researched the dynamics of ideas about national security in the Russian Federation from National Security Conception of 1997 to the National Security Strategies of 2009, 2015, 2021. The authors paid attention to external and internal factors that changed of the definition «national security» and practice of identification of priorities in national security at the 1990s-2021**.**

Keywords: national security; conception; strategy; threat; national priorities; Russian Federation.

В 1991 г. после распада СССР для России начался новый этап развития, характеризующийся необходимостью решения ряда проблем социального, экономического и политического развития. Одной из таких проблем стала потребность в комплексном обеспечении безопасности личности, общества и государства в новых исторических условиях.

Распад СССР и реформирование всей системы общественных отношений в Российской Федерации распространился на все внутренние и внешние отношения страны, вызвав крупномасштабные последствия как положительного, так и отрицательного характера. Президент Российской Федерации В. В. Путин в 2008 г. так характеризовал этот период: «У нас, по сути, не было единой страны, у нас даже гимна своего не было на постоянной основе. У нас в каждом субъекте Федерации была своя конституция, отличающаяся от Конституции Российской Федерации, у нас не было единой страны.» [1].

Второй аспект, влияющий на мультидисциплинарность проблемы национальной безопасности связан с тем, что само понятие «национальная безопасность» находится в постоянной динамике. Термин «национальная безопасность», как и практика представлять Стратегию в этой области появились в США [6]. США с 1986 г. обновляли Стратегию 18 раз [6].

В Российской империи и СССР не было практики регулярного обращения главы государства (или в советский период – партии) к законодательным органам.

В 1997 г. в Российской Федерации впервые была принята Концепция национальной безопасности. В 2000 г., вступив в должность Президента РФ, В. В. Путин утвердил новую редакцию данного документа. В 2009 г. была принята Стратегия национальной безопасности Российской Федерации до 2020 г., но реально документ действовал до 2015 г. В 2015 и 2021 гг. Россия обновила свою Стратегию национальной безопасности.

Таким образом, практика представления Стратегий национальной безопасности в России включает 4 документа [2–5]: 1997, 2009, 2015 и 2021 гг. (для сравнения: США с 1997 по 2021 г. обновляли аналогичный документ 10 раз [6]). Особого внимания заслуживает, несомненно, расстановка ключевых составляющих национальной безопасности в разделе IV. Отдельным параграфом в этом разделе Стратегии 2021 г. впервые выделена информационная безопасность. В Стратегии 2021 г. этот аспект национальной безопасности с точки

зрения реальных угроз личности («снижение до минимально возможного уровня количества утечек информации ограниченного доступа и персональных данных, а также уменьшение количества нарушений установленных российским законодательством требований по защите такой информации и персональных данных», «обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий»); обществу («обеспечение приоритетного использования в информационной инфраструктуре Российской Федерации российских информационных технологий и оборудования, отвечающих требованиям информационной безопасности», «развитие взаимодействия органов публичной власти, институтов гражданского общества и организаций при осуществлении деятельности в области обеспечения информационной безопасности Российской Федерации», «противодействие использованию информационной инфраструктуры Российской Федерации экстремистскими и террористическими организациями, специальными службами и пропагандистскими структурами иностранных государств для осуществления деструктивного информационного воздействия на граждан и общество»), государству и его отдельным институтам («предотвращение и (или) минимизация ущерба …, связанного с осуществлением иностранными государствами технической разведки»; «укрепление информационной безопасности Вооруженных Сил, других войск, воинских формирований и органов, а также разработчиков и изготовителей вооружения, военной и специальной техники») [4].

Заимствовав традицию создания и публичного представления Стратегий национальной безопасности из практики США, российские Президенты сумели сделать этот документ одним из ключевых в Российской политике. В нем не только декларируются, но действительно находят отражения изменения в представлении государства (как одного из социальных институтов) и общества в целом о приоритетных направлениях развития, о характере и источниках внутренних и внешних угроз, а также о способах поддержания стабильности российского социума.

СПИСОК ЛИТЕРАТУРЫ

1. Путин В. В. Я получил подарок от народа и от Господа – работать главой России // Комсомольская правда. 2008. 15 февраля. – Доступно из URL: https://www.kp.ru/daily/24049/102749/ (Дата обращения: 20. 07. 2021).
2. Указ Президента РФ от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года». – Доступно из URL: https://docs.cntd.ru/document/902156214?marker=6540IN (Дата обращения: 20. 07. 2021).
3. Указ Президента РФ от 17 декабря 1997 г. № 1300 «Об утверждении Концепции национальной безопасности Российской Федерации» (в ред. от 10 января 2000 г.). – Доступно из URL: https://docs.cntd.ru/document/901751578 (Дата обращения: 20. 07. 2021).
4. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации». – Доступно из URL: http://www.consultant.ru/document/cons_doc_LAW_389271/ (Дата обращения: 20. 07. 2021).
5. Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации». – Доступно из URL: http://www.consultant.ru/document/cons_doc_LAW_191669/ (Дата обращения: 20. 07. 2021).
6. National Security Strategy Archive. – Доступно из URL: https://nssarchive.us/ (Дата обращения: 20. 07. 2021).

УДК 004.9:351.9

АНАЛИЗ ДЕЯТЕЛЬНОСТИ УПРАВЛЯЮЩИХ ОРГАНИЗАЦИЙ НА ПРИМЕРЕ Г.НЕВИННОМЫССКА СТАВРПООЛЬСКОГО КРАЯ

Корохова Инна Валерьевна[1 2], Шаталова Ольга Ивановна[1], Баланов Сергей Сергеевич[2]
[1] Северо-Кавказский социальный институт
Голенева ул., 59А, Ставрополь, 355012, Россия
[2] ООО «Ростелеком информационные технологии» (Москва)
километр Киевское шоссе 22-й (п Московский), домовладение 6/1, Москва, 108811, Россия
e-mail: InnaKV-24@yandex.ru

Аннотация. В статье рассматривается процесс формирования оценки деятельности руководителя управляющей организации. С использованием методологии комплексного анализа был проведен анализ деятельности управляющей организации, в рамках которого выделен ряд проблем. Одной из главных проблем – это является экономически необоснованное соотношение качества и стоимости услуг по содержанию общего имущества многоквартирных домов. В качестве решения авторами предложен инструмент решения.

Ключевые слова: управляющая организация; ЖКХ; бизнес-процесс; менеджмент; деятельность руководителя; собственники помещений; стоимость услуг; проектно-процессный подход; стейкхолдеры; информатизация; умный город.

FORMATING THE ASSESSMENT OF THE MANAGER'S PERFORMANCE AS A DIGITAL TOOL FOR INCREASING THE EFFICIENCY OF THE MANAGING COMPANY

Korokhova Inna[1 2], Shatalova Olga[1], Balanov Sergey[2]
[1] The North Caucasian Social Institute
59A, Goleneva St, Stavropol, 355012, Russia
[2] Rostelekom Information Technologies, LLC (Moscow)
Household 6/1, 22nd km Kievskoe Highway, Moscow, 108811, Russia
e-mail: InnaKV-24@yandex.ru

Abstract. In the research, the issue of the formation an assessment of the activities of a managing company's head. It has allowed making the conclusion papers about the assessment of the activities of the managing company's head. The present issue is considered to scientists from a general point of view. An analysis of the managing company's activities was carried out with using complex analysis's method. The problems were chosen, one of the main ones being the economically unjustified ratio of the quality and cost of services for the maintenance of the common property of apartment buildings. As a solution, the authors proposed a solution tool.

Keywords: managing company; sphere of housing and utilities; business process; company's activities; management decision; owner's apartment buildings; the cost services; design-process approach; stakeholders; informatization; smart city.

В качестве важного направления Программы «Цифровая экономика» выступает создание и развитие «умных городов», включающего задачи по повышению эффективности ЖКХ, с применением современных информационных технологий. Основными задачами данного направления являются: повышение качества жизни граждан, предоставление гражданам качественных услуг без переплаты за них, а также обеспечение прозрачности и эффективности деятельности системы ЖКХ. В данной работе представлены результаты анализа деятельности организаций сферы ЖКХ по выполнению поставленных задач.

Деятельность организаций сферы ЖКХ отражается на индикаторах оценки эффективности деятельности органов самоуправления муниципальных округов. В работе рассмотрены два индикатора, которые являются одними из определяющих в сфере ЖКХ, так как включают основной перечень ресурсов потребления собственниками МКД 1:

– удельная величина потребления энергетических ресурсов (энергетическая и тепловая энергия, вода, природный газ) в МКД;

– удовлетворенность населения деятельностью органов местного самоуправления городского округа (муниципального района).

Анализ динамики данных показателей, базирующийся на отчетности главы города Невинномысска Ставропольского края, сформированного по результатам оценки деятельности органов местного самоуправления, позволил установить, что за последние два года (2019-2020) исследуемые показатели не достигнуты 2. Такая ситуация обусловлена проблематичностью взаимодействия между городским управлением ЖКХ, управляющими организациями, собственниками МКД и подрядными организациям по вопросам:

– несоответствия качества оказываемых услуг и стоимости;

– набора сотрудников с невысокой квалификацией;

– частого перехода собственников МКД из одной организации в другую.

Для подтверждения актуальности исследуемого вопроса несоответствия качества и стоимости оказываемых услуг, были проанализированы обращения граждан в администрацию города. Рост количества обращений отмечен после преобразования муниципальных унитарных предприятий в общества с ограниченной ответственностью. Как следствие, произошло резкое увлечение стоимости услуг по содержанию ОИ МКД.

Для рассмотрения проблемных вопросов был проведен анализ функционирования существующих бизнес-процессов 2 управляющих организаций различной формы собственности, где эмпирическую базу исследования составляют данные, аккамулированные в результате применения следующих методов:

– опрос собственников помещений МКД об удовлетворении оказываемых услуг управляющей организации в 2020 г. (N=120), выборка репрезентативности по возрастному составу: от 18 до 35, от 36 до 55, от 56 до 75 лет.

– сравнительный анализ деятельности двух управляющих организаций разной формы собственности (муниципальное унитарное предприятие, общество с ограниченной ответственностью);

– экспертный опрос сотрудников министерства экономического развития Ставропольского края, министерства жилищно-коммунального хозяйства Ставропольского, управления жилищно-коммунального хозяйства администрации города Невинномысска Ставропольского края, управляющих организаций, подрядных организаций (N=45). Опрос был проведен в 2021 г. в формате очного анкетирования;

– опрос подрядных организаций об удовлетворенности взаимодействия с управляющими организациями и собственниками МКД, и возможности открытого предоставления расчетов по проведению работ в 2021 г. (N=17), выборка репрезентативности по видам работ: кровля, оконное остекление, стены, водоотведение.

Результаты исследования позволили сделать вывод, что расчет стоимости услуг по содержанию ОИ МКД производится на основании полученных результатов работы за предыдущий период, при этом находясь в одних климатических условиях с одинаковыми техническими характеристиками различна. Значительная доля расходов управляющих организаций приходится на заработную плату сотрудников. Таким образом, возникает вопрос необходимость создания цифрового инструмента для проведения оценки эффективной деятельности руководители управляющей организации на основании разработанных 15 критериях, что позволит3, 4:

– улучшить показатели удельной величины потребления энергетических ресурсов в МКД;

– улучшить показатели удовлетворенности населения деятельностью органов местного самоуправления городского округа (муниципального района) (процент от числа опрошенных).

На следующем этапе авторы исследуют вопрос формирования оценки деятельности руководителя управляющей организации.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 28 апреля 2008 №607 (ред. от 11.06.2021) «Об оценке эффективности деятельности органов местного самоуправления муниципальных, городских округов и муниципальных районов».
2. Указ Президента Российской Федерации от 07 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // Собрание законодательства РФ – 2018. – № 20. – ст. 2817.
3. Друкер П. В. Эффективный руководитель / П. Ф. Друкер. – М. : Издательство «Манн, Иванов И Фербер», 2018. – 240 с.
4. Ляндау Ю.В. Бизнес-архитектор: проектирование систем управления. Часть 1 / Ю.В Ляндау. – М. : Издательство «Русайнс», 2015. – 112 с.

УДК 004.9:351.9

РАЗВИТИЕ СЕРВИСОВ ЭЛЕКТРОННОГО УЧАСТИЯ НА УРОВНЕ МЕСТНОГО САМОУПРАВЛЕНИЯ: МЕДИАЭКОЛОГИЧЕСКИЙ ПОДХОД

Мисников Юрий Георгиевич[1], Филатова Ольга Георгиевна [2]
[1] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
[2] Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mails: yuri.misnikov@gmail.com, o.filatova@spbu.ru

Аннотация. В докладе представлены основные результаты исследования сервисов электронного участия на уровне муниципальных образований внутри Санкт-Петербурга в зависимости от той медийной среды, в которой эти сервисы реализованы. Чтобы связать сервисы электронного участия со средой мультимедиа, которая обеспечивает функциональность, удобство использования и содержание таких сервисов, используется экосистемный подход, применяемый для теоретического обоснования экологии средств массовой информации и систем обсуждения. Основываясь на реальных эмпирических данных, собранных с помощью тематических исследований на уровне местных муниципалитетов в Санкт-Петербурге, построена модель экосистемы электронного участия, объединяющая три технически различных типа коммуникационных сред - сайты, социальные сети и службы обмена сообщениями. Продемонстрировано, что власти муниципальных образований заинтересованы прежде всего в информировании жителей, не уделяя должного внимания развертыванию сервисов сотрудничества и участия граждан в принятии решений.

Ключевые слова: электронное участие; электронный сервис; местное самоуправление; сайт; медиаэкология; экосистема; социальная сеть.

DEVELOPMENT OF ELECTRONIC PARTICIPATION SERVICES AT THE LEVEL OF LOCAL GOVERNMENT: A MEDIA-ECOLOGICAL APPROACH

Misnikov Yuri[1], Filatova Olga[2]
[1] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
[2] Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mails: yuri.misnikov@gmail.com, o.filatova@spbu.ru

Abstract. The report presents the main results of a study of e-participation services at the level of municipalities within St. Petersburg, depending on the media environment in which these services are implemented. To link e-participation services to a multimedia environment that provides functionality, usability and content for such services, an ecosystem approach is used to theoretically underpin the ecology of media and discussion systems. Based on real empirical data collected through case studies at the level of local municipalities in St. Petersburg, an e-participation ecosystem model has been built that combines three technically different types of communication media - sites, social networks and messaging services. It has been demonstrated that the authorities of municipalities are primarily interested in informing residents, not paying due attention to the deployment of cooperation services and citizen participation in decision-making.

Keywords: e-participation; e-service; local government; website; media ecology; ecosystem; social network.

В представляемом исследовании проанализированы все существующие сервисы электронного участия, используемые на уровне местного самоуправления в Санкт-Петербурге и выявлены различия между основными медийными средами: средой веб-сайтов, средой соцсетей и средой мобильных платформ. Эти три среды рассматриваются как основные элементы экосистемы электронного участия, реализуемые через соответствующие сервисы – сервисы информирования, сотрудничества и участия в принятии решений. Выбор этих сервисов был основан на признанных международных исследованиях и практике электронного участия.

Термин «медийная среда», который используется в данном исследовании в качестве основного, является частью дискурса в области медиаэкологии. Понятие «медиаэкологии», введенное Маршаллом Маклюэном в 1960-х годах, означает сегодня сложные и часто гибридные системы коммуникации, определяемые как видимые и невидимые среды, в которых технологии взаимодействуют с культурами, ценностями, мнениями, языками, поведением. В последнее время наблюдается возобновление интереса к изучению медиаэкологий как систем [1-

4]. Использование термина «медийная среда» позволяет выделить ее структурные элементы - веб-сайты, социальные сети, службы обмена сообщениями (мессенджеры). Термин «система» также предусматривает наличие взаимосвязанных структурных элементов, без которых система не может функционировать.

Наша основная гипотеза состояла в том, что, применяя принципы медиаэкологии и информационной экологии к электронному участию, можно разработать целостную модель экосистемы, чтобы выявить взаимосвязь между процессами взаимодействия власти с гражданами и соответствующими средами на низовом уровне. Вопросы нашего исследования касались возможности эмпирического моделирования экосистемы электронного участия на местном уровне в отличие от доминирующего в настоящее время внимания к разным платформам и инструментам.

Учитывая экспериментальный характер исследования, в качестве исследовательского объекта было выявлено десять муниципальных образований (МО) внутри Санкт-Петербурга. Особое внимание уделялось изучению разделов меню веб-сайтов МО как важнейшего средства коммуникации и взаимодействия с гражданами. Соответственно, каждый раздел и подраздел меню сайта рассматривался как конкретный сервис информирования, сотрудничества или принятия решений. Страницы в социальных сетях также рассматривались как отдельный сервис, классифицируемый как информирование. В случае имеющихся других разделов, созданных для организации дискуссий или проведения голосования, страница оценивалась как сервис сотрудничества или принятия решений соответственно, аналогичным образом оценивались и сервисы в мобильной среде.

В итоге зафиксировано 690 сервисов всех трех типов, или 69 в среднем по МО, в том числе - 61 сервис информирования, 72 сервиса сотрудничества и 7 сервисов принятия решений. Эти данные свидетельствуют о том, что функции информирования явно превалируют над другими. Причем полученные данные показали отсутствие значимой связи между численностью населения муниципального образования и типом сервисов.

Исследование показало, что власти муниципальных образований Санкт-Петербурга не уделяют должного внимания развертыванию сервисов сотрудничества и участия граждан в принятии решений, предпочитая использовать сервисы одностороннего информирования (даже в избыточном количестве, которое порой затрудняет поиск необходимой информации). Выводом исследования является и очень слабое использование официальных страниц муниципальных образований в социальных сетях для целей сотрудничества, где также доминирует функция информирования, несмотря на то что соцсети оказываются более предпочтительной средой для сервисов сотрудничества в силу своих особых интерактивных свойств. Отсутствие сервисов принятия решений связано как с их малым количеством вообще, так и необходимостью более сложных технических решений, которые сложнее осуществить в среде соцсетей, включая аспекты кибербезопасности. Исследование также показало, что роль среды мобильных приложений является минимальной в отношении всех сервисов участия. Можно предположить, что дальнейшее распространение мобильных каналов, чатов, сообществ, чат-ботов может привести к более значимым различиям между сервисами и медийной средой. Ведь большая часть новейшей среды — это мобильные службы обмена сообщениями на базе смартфонов - платформы и приложения. Это меняет сетевой ландшафт, поскольку «мобильные приложения для обмена сообщениями и агрегаторы новостей становятся все более важными для людей» [5]. Происходит переход к распределенной медиасреде, которая меняет конфигурацию каналов связи для поиска информации и открывает новые способы политического участия из-за быстрого роста популярности групп в приложениях для обмена сообщениями [6].

Более подробно выводы проведенного исследования представлены в публикации авторов [7], которая позволяет осторожно подтвердить исследовательскую гипотезу о возможности построения модели экосистемы электронного участия, основанной на концепции медиаэкологии, выдвигающей медийную среду на первый план.

Для лучшего понимания того, в какой степени жители муниципальных образований могут быть заинтересованы в местных сервисах электронного участия, необходимы дополнительные исследования. Одним из направлений будущих исследований также может стать изучение не только официальных, но и частных и общественных сервисов и инструментов как элементов экосистемы. Следует также протестировать другие методы исследования, чтобы продемонстрировать преимущества и недостатки медиаэкологического подхода. Эксперименты с различными схемами и критериями помогут сформировать более обоснованные представления о том, как участие общественности работает в различных онлайн-средах как целостных экосистемах.

СПИСОК ЛИТЕРАТУРЫ

1. Cali D. Mapping Media Ecology: Introduction to the Field. New York, Bern, Frankfurt, Berlin, Brussels, Vienna, Oxford, Warsaw: Peter Lang, 2017.
2. Santos L.G.M.: Toward the Open Government Ecosystem: Connecting e-Participation Models and Open Government to Analyze Public Policies. Springer Nature Switzerland AG (2019).
3. Scolari C. Media Ecology: Exploring the Metaphor to Expand the Theory, Communication Theory, Vol. 22, Issue 2, pp. 204-225, 2012.
4. Strate L. A Media Ecology Review, Communications Research Review, Vol. 23, No. 2, P. 3 – 48, 2004.
5. Rainie L., Smith A., Schlozman K., Brady H., Verba S.: Social media and political engagement. Pew Research: Internet Project, 2012.
6. Marquart F., Ohme J., Möller J.: Following Politicians on Social Media: Ef-fects for Political Information, Peer Communication, and Youth Engagement. In: Media and Communication, 8, 2, 197-207, Youth Digital Participation: Opportunities, Challenges, Contexts, and What's at Stake; PRT, 2020.
7. Misnikov Y., Filatova O., Trutnev, D., 2021, Social Computing and Social Media: Experience Design and Social Network Analysis - 13th International Conference, SCSM 2021, Held as Part of the 23rd HCI International Conference, HCII 2021, Proceedings. Meiselwitz, G. (ed.). Springer Nature, p. 87-104.

УДК 332.142.6

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ КОРЕННОГО НАСЕЛЕНИЯ АРКТИЧЕСКОЙ ЗОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Митько Арсений Валерьевич[1], Сидоров Владимир Константинович[2]

[1] Всероссийский научно-исследовательской институт метрологии имени Д.И. Менделеева
Московский пр., 19, Санкт-Петербург, 190005, Россия

[2] Санкт-Петербургский университет государственной противопожарной службы МЧС России
Московский пр., 149, Санкт-Петербург, 196105, Россия
e-mails: arseny73@yandex.ru, hamradio-spb@yandex.ru

Аннотация. В статье рассматриваются экологические проблемы развития Арктического региона. В настоящее время наблюдается активизация деятельности всех без исключения государств, граничащих с Арктикой. Безусловно, во главе угла экономический потенциал Арктического шельфа, его освоение и защита национальных интересов. Однако все социально-экономические мероприятия, проводимые в Арктике, должны учитывать и соблюдать экологические требования. С этой целью разрабатывается единый национальный экологический стандарт, процесс реализации которого не скоротечный и имеет много «подводных камней».

Ключевые слова: экология; Арктика; Северный морской путь; экологический стандарт; социально-экономическое развитие; национальные интересы.

ENSURING LIVING SAFETY OF THE INDIGENOUS POPULATION OF THE ARCTIC ZONE OF THE RUSSIAN FEDERATION

Mitko Arseny[1], Sidorov Vladimir[2]

[1] D. I. Mendeleev All-Russian research institute of metrology
19 Moskovskij Av, St. Petersburg, 190005, Russia

[2] Saint-Petersburg University of State Fire Service of EMERCOM of Russia
149 Moskovskiy Av, St. Petersburg, 196105, Russia
e-mails: arseny73@yandex.ru, hamradio-spb@yandex.ru

Abstract. The article examines the environmental problems of the development of the Arctic region. Currently, there is an intensification of the activities of all states bordering the Arctic without exception. Of course, the economic potential of the Arctic shelf, its development and protection of national interests are at the forefront. However, all socio-economic activities carried out in the Arctic must take into account and comply with environmental requirements. For this purpose, a unified national environmental standard is being developed, the implementation process of which is not short-lived and has many pitfalls.

Keywords: ecology; Arctic; Northern Sea Route; environmental standard; socio-economic development; national interests.

Экологические проблемы, являющиеся частью глобальных проблем современного мира, впервые официально были обозначены во второй половине двадцатого века и на сегодняшний момент сохраняют свою актуальность. Мир живой природы разнообразен, а взаимодействие живых организмов с окружающей средой настолько специфично и уникально, что однозначно утверждать какие факторы и в какой степени воздействуют в тех или иных природных условиях для неспециалиста достаточно сложно. Здесь нет унификации, понятной простому человеку, а есть биологические закономерности функционирования живой природы.

На сегодняшний день при научном и общественном сопровождении Арктической общественной академии наук, представлен проект Национального общественного стандарта «Экологической безопасности Арктики», процесс реализации которого не скоротечный и имеет много «подводных камней». Необходимо представить реализованные в документе положения в соответствующие международные специализированные рабочие группы Арктического экономического совета и государственную комиссию по Арктике для получения соответствующей поддержки. Работа предприятий изменится только с введением законодательных актов, соответствующих этим нормативам, и они будут более эффективными, если будут носить международный характер при соответствующем государственном контроле.

Основные идеи, положенные в основу Стандарта:

– правила экологичного поведения хозяйствующих субъектов на территории российской Арктики и система индикаторов экологичного поведения, задающая ориентиры для действующих и новых предприятий на территории российской Арктики;

– единый свод лучших практик и инициатив научных, общественных и коммерческих организаций, отечественных и международных правил и требований в области охраны окружающей среды Арктической зоны РФ;

– формирование нового «института» добровольного принятия правил экологического поведения для действующих и новых предприятий на территории российской Арктики.

Россия, как «Арктическое государство», обладающее одной из самых больших площадей Арктических территорий в мире, должна иметь основополагающий документ национального характера, который бы определял стандарты экологически безопасной деятельности в Арктике, поскольку вне экологической безопасности не

может существовать экономической деятельности, являющейся основой социального развития страны. Основной причиной необходимости настоящего стандарта является то, что существующая нормативная база не отражает и принципиально не может отразить все аспекты природопользования в Арктической зоне РФ. Происходит это не потому, что нормативная база несовершенна, а потому, что огромное количество аспектов не может быть встроено в закон, не всегда есть необходимость жестко регулировать деятельность, зачастую достаточно руководствоваться определенными принципами в ее организации для снижения рисков экологических катастроф.

Кроме того, при росте интенсивности использования Арктической зоны будут возникать новые принципы хозяйствования и новые риски, нормативная база не может оперативно реагировать на такие изменения, в этом случае Стандарт, включающий в себя базовые принципы природопользования и обеспечения экологической безопасности вполне может если не заменить закон в полной мере, то хотя бы обеспечить общественно приемлемые форматы деятельности в Арктических регионах. Для осуществления процесса стандартизации деятельности в Арктической зоне требуется доработать и формализовать на национальном уровне принципы рационального и эффективного использования природных ресурсов Арктики, исключающие прямой перенос «южных» технологий без прохождения процесса региональной адаптации и апробации. Кроме того, следует заменить изживший себя на настоящем этапе развития отраслевой подход освоения природных ресурсов Арктики, поскольку при современном уровне разделения труда невозможно в рамках одной отрасли, а тем более в рамках одного предприятия решить все проблемы обеспечения экологической безопасности производства. В первую очередь стандартизация должна касаться существующей нормативной базы, которая не соответствует документу «Основы государственной политики Российской Федерации в Арктике на период до 2035 года» [1]. Таким образом, в процессе стандартизации должны быть решены следующие проблемы нормативной базы:

– множественность и ведомственность нормативно-правовых актов, стандартов, регулирующих экологические вопросы по разным направлениям, в том числе распространяющаяся на Арктическую зону РФ, но не учитывающие ее природные особенности;

– отсутствие учета во многих отраслевых актах инициатив Международных организаций в области защиты окружающей среды;

– отсутствие механизма получения новых знаний о структурно-функциональной организации Арктических экосистем, механизмах устойчивости и их включения в существующие правовые акты, носящие регулирующий характер для отдельных видов деятельности;

– отсутствие требований по региональной адаптации и апробации технологий добычи и переработки природных ресурсов Арктики;

– отсутствие механизма учета значительных различий территорий российского сектора Арктики, чрезвычайно высокого разнообразия ландшафтов и климатических условий;

– отсутствие базовых документов национального характера, как основы для формирования узкоспециализированных, отраслевых нормативных актов, имеющих территориальную привязку для отраслей промышленности, причастных к использованию природных ресурсов, формирующих свою нормативную базу;

– не разработаны подходы к определению допустимого антропогенного воздействия и нагрузок на арктические экосистемы;

– экологическая экспертиза и оценка воздействия на окружающую среду не распространяется на все проекты намечаемой хозяйственной деятельности в Арктической зоне РФ;

– не предусмотрен учет особых природно-климатических условий в технических регламентах для продукции, которая может производиться или потребляться в Арктической зоне РФ.

Исходя из вышеизложенного, Национальный общественный стандарт экологической безопасности в Арктике:

– должен исключать ведомственный или отраслевой подход;

– должен являться базовым документом для формирования территориальных актов;

– объектом стандартизации является отдельное предприятие.

Национальный характер стандарта выражается в том, что он разработан для применения на суверенных территориях Российской Арктической зоны с учетом российского законодательства для работы в российском правовом поле. Стандарт является функциональным продолжением документов «Основы государственной политики Российской Федерации в Арктике на период до 2035 года», «Экологической доктрины Российской Федерации», «Морской доктрины Российской Федерации» [2]. Национальный характер стандарта не исключает присоединение к стандарту иностранных организаций, работающих на территории Российской арктической зоны.

Общественный характер стандарта выражается, прежде всего, в принципе добровольности, то есть, стандарт не является обязательным к исполнению, однако, организации, принимающие стандарт, берут на себя обязательства по выполнению его критериев добровольно, осознавая важность сохранения целостности окружающей среды, соблюдения норм безопасности и ответственности за качество жизни перед будущими поколениями. Проверить свое соответствие принципам стандарта и заявить о принятии норм стандарта организация может самостоятельно, используя материалы 4 радела. Однако, функционирование стандарта как системы, подразумевает создание экспертного совета, который возьмет на себя функции проверки соответствия деятельности сертифицируемой организации нормам стандарта. Экспертный совет должен быть выборным органом и состоять из представителей организаций, уже присоединившихся к стандарту, научных работников и представителей власти. Состав и численность экспертного совета, а также его полномочия определяются на его первом заседании представителей организаций готовых принять стандарт. Грядущие вызовы по освоению

природных ресурсов Арктики и обеспечения ее экологической безопасности определяются задачами, формализованными в документе «Основы государственной политики Российской Федерации в Арктике на период до 2035 года».

Эти задачи включают в себя:

– реализация конкурентных преимуществ России по добыче и транспортировке энергетических ресурсов;

– решение задач структурной перестройки экономики в Арктической зоне Российской Федерации на основе освоения минерально-сырьевой базы и водных биологических ресурсов региона;

– повышение экономической эффективности освоения минерально-сырьевой базы и водных биологических ресурсов арктического региона за счет использования комплексного подхода и их природных особенностей;

– создание и развитие инфраструктуры и системы управления коммуникациями Северного морского пути для решения задач обеспечения евразийского транзита;

– завершение создания единого информационного пространства Арктической зоны Российской Федерации;

– превращение Арктической зоны Российской Федерации в ведущую стратегическую ресурсную базу Российской Федерации;

– глобальные изменения окружающей среды и климата [3].

Национальный общественный стандарт «Экологическая безопасность Арктики» разработан Общественной комиссией по направлению «Экология» Межрегиональной общественной организации «Ассоциация полярников» (АСПОЛ) при содействии сотрудников Института проблем промышленной экологии Севера Российской академии наук.

СПИСОК ЛИТЕРАТУРЫ

1. «Основы государственной политики Российской Федерации в Арктике на период до 2035 года» http://www.kremlin.ru/acts/bank/45255
2. Митько А.В. Основные направления формирования Арктической доктрины России/Научный вестник Ямало-Ненецкого автономного округа №4(105): 2019.-с.25-29.
3. Митько А.В., Болотов И.Н. Проблемы обеспечения экологической безопасности и устойчивое развитие Арктических территорий. Сборник материалов Всероссийской конференции с международным участием II Юдахинские чтения, Архангельск: ФИЦКИА, -2019.- с. 323-327.

УДК 004

ОБРАБОТКА ВИЗУАЛЬНЫХ ДАННЫХ ДЛЯ ВЫЯВЛЕНИЯ СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ

Низомутдинов Борис Абдуллохонович[1], Углова Анна Борисовна[2], Беген Петр Николаевич[1], Низомутдинова Валентина Дмитриевна

[1] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
[2] Российский государственный педагогический университет им. А.И. Герцена
р. Мойки наб., 48, Санкт-Петербург, 191086, Россия
e-mails: boris@itmo.ru, anna.uglova@list.ru, petyabegen@mail.ru

Аннотация. В докладе представлены основные результаты исследования Центра технологий электронного правительства Института дизайна и урбанистики Университета ИТМО совместно с Российским государственным педагогическим университетом им. А. И. Герцена, посвященного обработке визуальных данных для выявления социально-психологических характеристик пользователей. Методика позволяет проводить анализ, полученных изображений из социальных сетей, для выявления социально-психологических характеристик пользователей, с использованием машинного обучения. В апреле 2021 года было проведено анкетирование 202 жителей Санкт-Петербурга, по итогу каждый участник ответил на ряд вопросов и дал согласие на обработку профиля в социальной сети Вконтакте. Для обработки изображений, был разработан сервис, позволяющий распознать лицо (лица) на изображении и вернуть список атрибутов (Accessories; Age; Blur; Emotion; Exposure; FacialHair; Gender; Glasses; Hair; HeadPose; Makeup; Mask; Noise; Occlusion; Smile). На последнем этапе был проведен поиск взаимосвязей ответов пользователей и выявленных атрибутов, были выявлены достоверно значимые взаимосвязи различных атрибутов, выделенных на фотографиях и социально-психологических характеристик пользователей.

Ключевые слова: обработка изображений; распознавание лиц; распознавание эмоций; Microsoft Azure.

PROCESSING OF VISUAL DATA TO IDENTIFY THE SOCIO-PSYCHOLOGICAL CHARACTERISTICS OF USERS OF SOCIAL NETWORKS

Nizomutdinov Boris[1], Uglova Anna[2], Begen Petr[1], Nizomutdinova Valentina

[1] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
[2] Herzen state pedagogical university of Russia
48 Moika Emb, St. Petersburg, 191086, Russia
e-mails: boris-wels@yandex.ru, anna.uglova@list.ru, petyabegen@mail.ru

Abstract. The report presents the main results of a study by the Center for E-Government Technologies of the Institute of Design and Urban Studies of ITMO University together with the A. I. Herzen Russian State Pedagogical University, dedicated to the processing of visual data to identify the socio-psychological characteristics of users. The technique allows analyzing the images obtained from social networks to identify the socio-psychological characteristics of users using machine learning. In May 2021, a survey of 202 residents of St. Petersburg was conducted, as a result, each participant answered a number of questions and agreed to the processing of a profile in the Vkontakte social network. For image processing, a service was developed that allows you to recognize the face (s) in the image and return a list of attributes (Accessories; Age; Blur; Emotion; Exposure; FacialHair; Gender; Glasses; Hair; HeadPose; Makeup; Mask; Noise; Occlusion; Smile). At the last stage, a search was carried out for the interrelationships of users ' responses and the identified attributes, reliably significant interrelations of various attributes highlighted in photos and socio-psychological characteristics of users were revealed.

Keywords: image preprocessing; face detection; emotion detection; Microsoft Azure.

Визуальная самопрезентация в социальных сетях в настоящее время является одним из самых простых и доступных способов наладить успешную коммуникацию с другими пользователями и презентовать себя [2, 5]. В рамках социально-психологических исследований визуальная продукция в социальной сети является наиболее доступным источником информации о пользователе [3, 4]. Однако ручная обработка изображений требует больших трудовых и временных ресурсов, поэтому наиболее оптимальным решением является автоматизированный сбор и обработка изображений с помощью прикладных инструментов [6].

Работа представляет результаты разработки сервиса обработки визуальных данных для выявления социально-психологических характеристик пользователей. На первом шаге было проведено анкетирование жителей Санкт-Петербурга, каждый участник оставил ссылку на профиль в социальной сети Вконтакте, ссылка на профиль необходима для выгрузки фотографии.

Одним из наиболее востребованных сервисов является инструмент Azure от Microsoft, в котором реализовано множество API-сервисов для компьютерного зрения, машинного обучения, параллельных вычислений и обработок и др.

Облачный сервис Azure позволяет использовать свои вычислительные мощности для различных задач, в том числе и для машинного анализа изображений и текста. Решение располагает собственным семейством сервисов API, которые помогают пользователям непосредственно отправлять запросы на сервера Microsoft и получать необходимую информацию за достаточно быстрое время. В рамках текущей задачи для распознавания эмоций пользователей социальных сетей был выбран API сервис «Распознавание лиц» (Face Detection). Данный сервис позволяет распознать лицо (лица) на изображении и вернуть список атрибутов. Всего в сервисе доступно 15 атрибутов: Accessories; Age; Blur; Emotion; Exposure; FacialHair; Gender; Glasses; Hair; HeadPose; Makeup; Mask; Noise; Occlusion; Smile. Некоторые атрибуты являются комплексными и содержат в себе список податрибутов и типов. Всего сервис «Распознавание лиц» содержит 35 доступных атрибутов лица.

Разработка собственного инструментария велась на языке Python 3.6 с использованием фреймворка Flask для работы в веб-интерфейсе; для подключения к API-сервисам Azure были использованы официальные библиотеки от Microsoft [1]. Для доступа к API предварительно был получен ключ и идентификаторы ресурса, для доступа была применена специальная подписка для обучающихся.

Для анализа эмоций аватаров была сформирована выборка из 202 пользователей с помощью стороннего парсера vk.barkov.net, также были получены ссылки на первое изображение аватара со страницы профиля. В результате был сформирован итоговый файл по 35 атрибутам лица в формате EXCEL. В соответствии с первыми полученными результатами было распознано 112 лиц с атрибутами. В ходе анализа выяснилось, что большинство полученных изображений аватаров либо действительно не содержали лиц или человека, либо оказались в недостаточном качестве и разрешении (шум, высокое размытие, пересветы, большая удаленность человека на фотографии и т.д.). Это побудило на создание списка условий и ограничений для предварительного отбора таких изображений.

На втором этапе для проверки качества анализа фотографий и возможности использования подобной обработки визуальных данных в практике реальных исследований нами был проведен анализ взаимосвязей выделенных атрибутов и социально-психологических характеристик пользователей. Нами был проведен социально-психологический опрос пользователей, с целью выявления базовых ценностных ориентаций (ценностный опросник Шварца К.) и основных диспозиционных личностных черт (краткий опросник Большой Пятерки, Корнилова Т. В., Чумакова М. А.), которые опосредуют взаимодействие в сети и эмоциональный опыт пользователя, отраженный в визуальной самопрезентации. С помощью корреляционного анализа (коэффициент корреляции Спирмена) были выявлены достоверно значимые взаимосвязи различных атрибутов, выделенных на фотографиях и социально-психологических характеристик пользователей:

Высокий уровень шума и размытости фотографий отрицательно взаимосвязан с экстраверсией ($r=-0,19$, $p\leq0,05$), отзывчивостью ($r=-0,24$, $p\leq0,05$), ценностью вежливости ($r=-0,21$, $p\leq0,05$) и уважения традиций ($r=-0,26$, $p\leq0,05$). Как упоминалось ранее, при анализе аватаров было выявлено большое количество фотографий в недостаточном качестве и разрешении. что само по себе является важной информацией и может быть использовано для анализа.

Выявлен ряд взаимосвязей с эмоциями, выявленными на аватарах пользователей. Эмоция гнева положительно взаимосвязана с нейротизмом, эмоциональной неустойчивостью, тревожностью ($r=0,19$, $p\leq0,05$);

эмоция отвращения отрицательно взаимосвязана с ценностью новых впечатлений (r=-0,22, p≤0,05); чувство счастья на аватаре положительно взаимосвязаны с ценностью равенства в общении (r=0,21, p≤0,05), ценностью безопасности (r=0,20, p≤0,05), открытостью (r=0,21, p≤0,05), ценностью универсализма (терпимость и защита благополучия) (r=0,22, p≤0,05); нейтральные эмоции, выявленные на аватаре отрицательно взаимосвязаны с ценностью универсализма (r=-0,23, p≤0,05) и положительно взаимосвязаны с ощущением себя творческим человеком (r=0,20, p≤0,05); эмоция удивления отрицательно взаимосвязана с открытостью новому опыту (r=-0,21, p≤0,05), смелостью (r=-0,20, p≤0,05), ценностью послушания (r=-0,19, p≤0,05), ценностью гедонизма (r=-0,19, p≤0,05).

Проведенный анализ показывает, что через анализ экспрессии, выраженной на аватарах пользователей, можно оценить не только эмоциональный фон фотографий, но и сделать ряд выводов об особенностях ценностно-смысловой и коммуникативной сферы пользователей, что может быть использовано для составления социально-психологического профиля пользователя. С практической точки зрения, данная методика может использоваться для систем Безопасного города и проектов Smart City в крупных мегаполисах. В дальнейшем команда исследователей планирует продолжение поиска взаимосвязей для прикладных задач.

СПИСОК ЛИТЕРАТУРЫ

1. API-интерфейс для распознавания лиц. URL: https://azure.microsoft.com/ru-ru/services/cognitive-services/face/.
2. Вирясова М.А. Визуальная самопрезентация как аспект коммуникации в социальных сетях (на примере Instagram) // Социология. материалы 58-й Международной научной студенческой конференции. Новосибирский государственный университет. Новосибирск, 2020. С. 49-50.
3. Горных А. Визуальная антропология: видеть себя другим / А. Горных // Антропологический форум. 2007. № 7. С. 32–52.
4. Сергеева, О. В., & Орех, Е. А. (2015). Визуальная самопрезентация личности в сети интернет (о некоторых гипотезах в развитие темы) // Визуальная коммуникация в социокультурной динамике. 2014. С. 250-259.
5. Steffan D. (2020) Visual Self-Presentation Strategies of Political Candidates on Social Media Platforms: A Comparative Study. International Journal of Communication. Vol.14. p. 3096–3118.
6. Zhao C., Jiang G. (2011) Cultural Differences on Visual Self-Presentation through Social Networking Site Profile Images. Proceedings of the International Conference on Human Factors in Computing Systems, doi: 10.1145/1978942.1979110.

УДК 004.9:351.9

АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВИТИЯ ЭЛЕКТРОННОГО ВЗАИМОДЕЙСТВИЯ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В СФЕРЕ ЗДРАВООХРАНЕНИЯ ФЕДЕРАЛЬНОГО И РЕГИОНАЛЬНОГО УРОВНЕЙ

Орлов Геннадий Михайлович
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: g.orlov@itmo.ru

Аннотация. В статье представлен обзор нормативных документов и рекомендаций, представляющих общий методологический подход к организации сквозного электронного взаимодействия информационных систем на уровне медицинской организации, субъекта Российской Федерации и федерального уровня и оценки цифровой трансформации процессов по наиболее приоритетным профилям для совершенствования управления оказанием медицинской помощи в России. В заключении приведены перспективные направления дальнейшей цифровой трансформации таких процессов.

Ключевые слова: цифровое здравоохранение; медицинская информационная система; оценка цифровой зрелости; единый цифровой контур здравоохранения; ВИМИС; ЕГИСЗ; цифровые сервисы для пациентов.

TOPICAL ISSUES OF THE DEVELOPMENT OF ELECTRONIC INTERACTION OF STATE INFORMATION SYSTEMS IN THE FIELD OF HEALTHCARE AT THE FEDERAL AND REGIONAL LEVELS

Orlov Gennadii
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mail: g.orlov@itmo.ru

Abstract. The article presents an overview of regulatory documents and recommendations that represent a general methodological approach to organizing end-to-end electronic interaction of information systems at the level of a medical organization, a subject of the Russian Federation and the federal level and evaluating the digital transformation of processes in the most priority profiles for improving the management of medical care in Russia. In conclusion, promising directions for further digital transformation of such processes are presented.

Keywords: digital healthcare; medical information system; digital maturity assessment; unified digital healthcare circuit; VIMIS, EGISZ; digital services for patients.

Работа посвящена обзору методологического подхода к организации электронного взаимодействия подсистем государственной информационной системы в сфере здравоохранения субъектов Российской Федерации (ГИСЗ) с вертикально-интегрированными медицинскими информационными системами (ВИМИС)

«Акушерство и гинекология», «Неонаталогия», «Сердечно-сосудистые заболевания» и «Онкология», а также к оценке уровня зрелости цифровой трансформации соответствующих процессов оказания медицинской помощи и процессов взаимодействия с пациентом. Разработка методических рекомендаций к функциональным возможностям ГИСЗ осуществлялась автором в Центре компетенций цифровой трансформации сферы здравоохранения Минздрава России с привлечением ряда экспертов РОО «Экспертное сообщество э2мед.ру» в 2020-2021 гг.

Эффективное принятие управленческих решений и контроль качества в рамках наиболее приоритетных профилей для совершенствования управления оказанием медицинской помощи возможно только при наличии максимально полного спектра данных о каждом пациенте, о каждой медицинской организации по профилю и каждом медицинском работнике. То есть с применением принципов управления на основе данных.

Выполнение данной задачи стало возможным в 2021 году на новом этапе развития ЕГИСЗ в связи с созданием специализированных информационных систем ВИМИС, обеспечивающих оперативное поступление первичной информации о медицинской диагностике и лечении пациента от врача медицинской организации на уровень субъекта РФ и далее на уровень Федерации для проведения анализа процессов оказания медицинской помощи со стороны федеральных национальных медицинских исследовательских центров, специализирующихся на конкретном профиле лечения.

Выстраивание вертикали взаимодействия требует комплексного подхода к определению требований на всех уровнях:

– на уровне медицинских организаций - к Медицинским информационным системам в рамках соответствующих требований Минздрава России [1];

– на уровне субъекта РФ - к обработке информации в ГИСЗ, изложенным в методических рекомендациях [2-4];

– на уровне взаимодействия ГИСЗ и ВИМИС - к протоколам передачи информации на федеральный уровень [5] в рамках федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)» [6];

– на уровне профильного федерального национального медицинского исследовательского центра (НМИЦ) – к эксплуатируемой им системе ВИМИС по соответствующему профилю медицинской помощи, изложенным, например, в Концепции [7] и проектных документах системы.

Для управления процессами цифровой трансформации на всех рассматриваемых уровнях, а особенно после принятия Указа Президента Российской Федерации «О национальных целях развития Российской Федерации на период до 2030 года» [8], стала крайне актуальной задача оценки уровня цифровой зрелости трансформации процессов медицинской организации и субъекта Федерации. Указ Президента Российской Федерации определил «цифровую трансформацию» как одну из пяти национальных целей развития России. Целевыми показателями этой цели установлены: «достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, государственного управления.

Методика подобной оценки была разработана в 2021 году, включена в методические рекомендации [2-4] и описана в статье [9]. Методика устанавливает показатели, вычисляемые на основе первичных данных информационной системы, для учреждений, оказывающих медицинскую помощь по профилю, и определяет общие интегральные индексы, характеризующие как достигнутый функциональный уровень зрелости цифровой трансформации, так и объемные показатели внедрения цифровых технологий. Методика позволяет организовать непрерывное измерение текущего уровня цифровой трансформации системы оказания медицинской помощи по профилю медицинской помощи, мониторировать и прогнозировать его изменение, формировать рейтинги медицинских организаций. Она может применяться на федеральном уровне в целом по Российской Федерации, для рейтингования субъектов Российской Федерации или на региональном уровне для рейтингования медицинских организаций. Разработанный методологический подход после практической апробации на региональном и федеральном уровне потребует постоянной актуализации по мере развития цифровой трансформации.

В методике, примененной в [2-4], также устанавливается ряд показателей оценки цифровой трансформации системы оказания медицинской помощи для граждан, определяется соответствующий интегральный индекс и так называемый «социальный рейтинг цифровой трансформации» процессов оказания медицинской помощи по профилю. В связи с активным развитием и ростом популярности цифровых сервисов для пациентов [10] это направление исследований, по мнению автора, также является перспективным.

В связи со сложностью проведения оценки уровня зрелости медицинских информационных систем в медицинских организациях на основе Приказа Минздрава России [1], требуется разработка и принятие новой редакции приказа, с включением в его состав методики оценки. Методика должна обеспечивать широкое применение при проведении самооценки медицинской организацией с возможностью аудита оценки на уровне субъекта Российской Федерации или федеральном уровне. Она должна обеспечить медицинской организации возможность планирования этапов цифровой трансформации и должна быть гармонизирована с международными подходами (например, методикой EMRAM HIMSS).

СПИСОК ЛИТЕРАТУРЫ

1. Приказ Министерства здравоохранения Российской Федерации от 24 декабря 2018 г. №911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций».

2. Методические рекомендации по обеспечению функциональных возможностей централизованной системы (подсистемы) «Организация оказания медицинской помощи по профилям «акушерство и гинекология» и «неонатология» государственной информационной системы в сфере здравоохранения субъекта Российской Федерации // Минздрав России. URL: https://portal.egisz.rosminzdrav.ru/materials/3803 (дата обращения: 14.02.2021).
3. Методические рекомендации по обеспечению функциональных возможностей централизованной системы (подсистемы) «Организация оказания медицинской помощи больным сердечно-сосудистыми заболеваниями» государственной информационной системы в сфере здравоохранения субъекта Российской Федерации// Минздрав России. URL: https://portal.egisz.rosminzdrav.ru/materials/3805 (дата обращения: 14.02.2021).
4. Методические рекомендации по обеспечению функциональных возможностей централизованной системы (подсистемы) «Организация оказания медицинской помощи больным онкологическими заболеваниями» государственной информационной системы в сфере здравоохранения субъекта Российской Федерации // Минздрав России. URL: https://portal.egisz.rosminzdrav.ru/materials/3801 (дата обращения: 14.02.2021).
5. Протокол информационного взаимодействия ВИМИС «Онкология» с внешними информационными системами https://portal.egisz.rosminzdrav.ru/materials/3595 (дата обращения: 01.09.2021).
6. Паспорт федерального проекта «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)» URL: https://static-3.rosminzdrav.ru/system/attachments/attaches/000/046/712/original/FP_Cifrovoj_kontur_zdravooxraneniya.pdf?1565344851 (дата обращения: 01.09.2021).
7. Концепция создания Федеральной системы «Онкология» (вертикально-интегрированной медицинской информационной системы по профилю «Онкология») - https://portal.egisz.rosminzdrav.ru/materials/3593 (дата обращения: 01.09.2021).
8. Указ Президента от 21 июля 2020 года № 474 «О национальных целях развития Российской Федерации на период до 2030 года»
9. Орлов Г.М., Левин М.Б. Методологические подходы к разработке эталонных моделей подсистем государственных информационных систем в сфере здравоохранения субъектов Российской Федерации // Информационные ресурсы России. 2021. № 2. С. 20-27. DOI 10.46920/0204-3653_2021_02180_20.
10. Долгова Н.А. Цифровое здравоохранение: как развиваются пациентоориентированные сервисы в России. интернет-журнал «Популярная механика», 2021, URL: https://www.popmech.ru/gadgets/748403-cifrovoe-zdravoohranenie-kak-razvivayutsya-pacientoorientirovannye-servisy-v-rossii/ (дата обращения: 17.09.2021).

УДК 004.9:351.9

МОНИТОРИНГ ЭЛЕКТРОННОГО УЧАСТИЯ В РОССИИ 2021: РЕЗУЛЬТАТЫ ВТОРОГО ЭТАПА ИССЛЕДОВАНИЯ И НОВЫЕ ВЫЗОВЫ

Панфилов Георгий Олегович, Чугунов Андрей Владимирович
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: panfilovgeorg@mail.ru, chugunov@itmo.ru

Аннотация. В докладе представлены результаты второго этапа исследования процессов электронного участия в России, проведенного Центром технологий электронного правительства Университета ИТМО в январе-феврале 2021 года. Так же, как и на первом этапе был произведен мониторинг каналов электронного участия в России шести основных типов, созданных органами власти субъектов РФ и органами местного самоуправления городов, являющихся административными центрами субъектов РФ. Исследование проводилось по методике, позволяющей оценить такие критерии ресурсов как «открытость», «доступность», «принятие решений», «обратная связь» и «специфические требования». Общее количество региональных ресурсов увеличилось с 198 до 207 по отношению к 2020 г., а муниципальных – напротив, сократилось с 155 до 148. Канал «сообщения о проблемах» значительно улучшил свои позиции, увеличив число ресурсов и набранные баллы. Канал «инициативное бюджетирование» - наоборот, ухудшил свои позиции – количество ресурсов данного типа значительно сократилось. Каналы «открытый бюджет», «электронные инициативы», «электронные голосования» и «краудсорсинг» в целом сохранили свое развитие на том же уровне.

Ключевые слова: электронное участие; интернет-ресурсы; мониторинг; Платформа обратной связи.

MONITORING E-PARTICIPATION IN RUSSIA 2021: RESULTS OF THE SECOND STAGE OF RESEARCH AND NEW CHALLENGES

Panfilov Georgiy, Chugunov Andrei
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: panfilovgeorg@mail.ru, chugunov@itmo.ru

Abstract. The report presents the results of the second stage of the study of e-participation processes in Russia, conducted by the Center for e-Government Technologies of ITMO University in January-February 2021. The second stage of monitoring of six main types of electronic participation channels in Russia was carried out, created by the authorities of the constituent entities of the Russian Federation and local governments of cities that are the administrative centers of the constituent entities of the Russian Federation. The study was carried out according to a methodology that allows evaluating such criteria of resources as "openness", "availability", "decision making", "feedback" and "specific requirements". The total number of regional resources increased from 198 to 207 in relation to 2020, while municipal resources, on the contrary, decreased from 155 to 148. The channel "reporting problems" has significantly improved its position, increasing the number of resources and the points scored. On the contrary, the channel “initiative budgeting” has worsened its position - the amount of resources of this type has significantly

decreased. The channels “open budget”, “e-initiatives”, “e-voting” and “crowdsourcing” have generally maintained their development at the same level.

Keywords: e-participation; internet resources; monitoring; feedback platform.

Мониторинг интернет-ресурсов, обеспечивающих функционирование каналов электронного участия, осуществленный в январе-феврале 2021 г. является логическим продолжением исследования, проведенного в декабре 2019 – январе 2020 г. [1]. Методика и инструментарий исследования не претерпели существенных изменений, что позволяет сопоставлять результаты в динамике. Так же, как и в исследовании 2020 г. были выявлены и оценены каналы электронного участия, созданные органами власти субъектов РФ и органами местного самоуправления городов, являющихся столицами субъектов РФ. Ресурсы, не обновляемые модераторами более одного года, не учитывались в исследовании и были исключены из анализа.

Общее количество выявленных региональных каналов электронного участия увеличилось с 198 в 2020 г. до 207 в 2021 г. На муниципальном уровне количество каналов, наоборот, сократилось с 155 до 148. Средний балл по-прежнему являлся более высоким у ресурсов регионального уровня (12 баллов), чем муниципального (10). В наибольшей степени эта разница была ощутима в каналах о бюджете и сообщениях о проблемах.

Каналом электронного участия с наибольшим охватом регионов (100%) по-прежнему остались системы информирования о бюджетном процессе типа «Открытый бюджет». Этот канал функционирует в каждом из 85 регионов России как минимум на одном уровне. Средний балл на региональном уровне увеличился на 1 балл, на муниципальном - остался без изменений.

Второе место по охвату регионов занял канал сообщений о проблемах, обогнав инициативное бюджетирование, занявшее второе место в 2020 году. Количество каналов этого типа на уровне регионов увеличилось с 30 до 37, а в городах-столицах сократилось с 20 до 19. Таким образом, общий охват составил 47 регионов (55%). Средний набранный балл увеличился на 2, на региональном и муниципальном уровне.

На третьем месте, уменьшив свой охват на 17 регионов (20%), оказались каналы инициативного бюджетирования. Количество каналов этого типа уменьшилось с 51 до 38 на уровне регионов и с 25 до 16 - на уровне городов. Средний балл увеличился на 3 на региональном уровне (прежде всего, за счет ликвидации части ресурсов низкого качества), на муниципальном - остался без изменений.

Последние три места так же, как и в исследовании прошлого года заняли электронные голосования, электронные инициативы и краудсорсинг соответственно. Возможность проголосовать за проекты благоустройства и другие инициативы власти сегодня имеют жители 24 регионов (увеличилось на 11) и 17 административных центров регионов (сократилось на 3). Возможность отправить на рассмотрение в органы власти собственный проект реализована в 12 регионах и 10 городах-столицах. Канал краудсорсинга сегодня реализован всего в 12 субъектах и 6 городах-столицах.

Параллельно с изменениями региональных и муниципальных каналов, описанными выше, существенные изменения претерпела институциональная структура процедур осуществления органами власти обратной связи с гражданами. Изменения были стимулированы подписанием Президентом РФ перечня поручений по итогам заседания Совета по развитию местного самоуправления, который состоялся 30 января 2020 г. [2] Поручения предполагали создание единой Платформы обратной связи (ПОС) на базе Единого портала государственных и муниципальных услуг, на которой должно осуществляться взаимодействие по таким каналам электронного участия, как сообщения о проблемах, опросы, голосования и общественные обсуждения. На сентябрь 2021 г. все субъекты РФ являются подключенными к Платформе обратной связи и используют ее каналы для взаимодействия с гражданами. В результате данной централизации многие регионы, имеющие свои каналы электронного участия с выстроенной логистикой обработки обращений граждан, столкнулись с необходимостью обеспечения информационного взаимодействия региональных систем с ЕПГУ, либо отказа от региональных систем в пользу федеральной.

Ввиду обозначенных выше изменений, авторы исследования столкнулись с необходимостью доработки методики исследования и учета в исследовании особенностей электронного участия «фактора ПОС». Для этого была разработана новая институциональная модель, иллюстрирующая основных участников, процессы и инструменты (каналы) электронного участия на местном и региональном уровнях с учетом появления ПОС, системы «Инцидент-менеджмент» и Центров управления регионами, сотрудники которых осуществляют администрирование данных ресурсов. Доработка методики оценивания будет осуществлена перед следующим этапом мониторинга, который планируется провести в начале 2022 г.

СПИСОК ЛИТЕРАТУРЫ

1. Панфилов Г.О., Чугунов А.В., Кабанов Ю.А. Развитие порталов электронного участия на региональном и муниципальном уровне в России: результаты мониторинга 2019 года//Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020 г.: Материалы конференции. Часть 1. - 2020. - С. 33-35
2. Перечень поручений по итогам заседания Совета по развитию местного самоуправления // Официальный сайт Президента РФ. Документы. 1 марта 2020. URL: http://kremlin.ru/acts/assignments/orders/62919 (дата обращения: 30.05.2021)

УДК 004.056

УГРОЗЫ ЧЕЛОВЕЧЕСТВУ В УСЛОВИЯХ ПЕРЕХОДА К ОБЩЕСТВУ ЗНАНИЙ

Советов Борис Яковлевич[1], Касаткин Виктор Викторович[2]

[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия

[2] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: bysovetov@mail.ru, v.v.kasatkin@iias.spb.su

Аннотация. Рассматриваются особенности современного этапа общественного развития, связанного с переходом в общество знаний, основой которого становится искусственный интеллект. Обсуждаются угрозы, возникающие как следствие перехода в общество знаний. Обсуждаются возможные подходы к решению задач предотвращения угроз потери контроля над системами искусственного интеллекта на основе классической теории управления и методов информационно-психологической и когнитивной безопасности. Подчеркивается значение опережающей подготовки и переподготовки кадров в области информационной безопасности.

Ключевые слова: информационное общество; общество знаний; искусственный интеллект; информационная безопасность; угрозы в сфере информационной безопасности; информационно-психологическая и когнитивная безопасность; подготовка специалистов в области информационной безопасности.

THREATS TO HUMANITY IN THE TRANSITION TO A KNOWLEDGE SOCIETY

Sovetov Boris[1], Kasatkin Viktor[2]

[1] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia

[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: bysovetov@mail.ru, v.v.kasatkin@iias.spb.su

Abstract. The features of the modern stage of social development connected with the transition to a knowledge society, the basis of which becomes artificial intelligence, are considered. Threats arising from the transition to a knowledge society are discussed. Possible approaches to solving the problems of preventing threats of loss of control over artificial intelligence systems based on the classical theory of control and methods of information-psychological and cognitive security are discussed. The importance of advanced training and retraining of personnel in the field of information security is emphasized.

Keywords: information society; the knowledge society; artificial intelligence; information security; threats to information security; information, psychological and cognitive security; Training of information security professionals.

Завершение формирования информационного общества заставляет задуматься о будущем человечества. С большой долей вероятности можно предположить, что очередной этап общественного развития будет связан с переходом в общество знаний [1], в котором преобладающее значение для граждан, экономики и государства приобретают получение, сохранение, производство и распространение знаний в целях развития человеческого потенциала, наращивания интеллектуального капитала, обеспечения безопасности и повышения эффективности труда и качества жизни граждан с учетом стратегических национальных приоритетов. Важнейшими чертами общества знаний является стимулирование развития существующих и новых технологических достижений и, в первую очередь, технологий искусственного интеллекта [2].

Развитие прогресса в области искусственного интеллекта предполагает целый ряд позитивных изменений в жизни людей, таких, как: уход от тяжелых, рутинных видов деятельности; реализация когнитивных функций человека, включая самообучение, обобщение и поиск решений конкретных задач, сопоставимых или превосходящих по эффективности результаты интеллектуальной деятельности человека; замена человека более быстродействующими и точными интеллектуальными роботами и т.д. Уже в настоящее время такие области деятельности человека, как финансовая, рекламная, страховая, правоохранительная, сфера здравоохранения и др. неразрывно связаны с необходимостью анализа большого объема данных, выявления скрытых закономерностей и явлений, где естественные возможности человека оказываются недостаточными. Особенно привлекательно использование систем искусственного интеллекта для решения нестандартных и математически трудно формализуемых задач, где перспективные подходы связывают с моделированием на основе искусственного интеллекта мыслительных процессов человека.

В связи с этим возникает проблема ответственности за действия и последствия использования систем искусственного интеллекта, особенно в тех областях, где их применение необходимо, либо более эффективно по сравнению с результатами деятельности человека. Уже сейчас просматриваются угрозы, возникающие как следствие перехода в общество знаний, среди которых можно выделить: вытеснение рабочей силы искусственным интеллектом, исчезновение ряда профессий, смена технологий в производстве, науке и образовании, непрерывное усложнение и как следствие – рост числа потенциальных уязвимостей систем

искусственного интеллекта, а также вероятность замены человека полностью системами искусственного интеллекта, лишенными духовно-нравственного начала, с захватом ими функций управления.

Выполнен целый ряд теоретических и экспериментальных исследований по проблеме выявления отличий деятельности системы искусственного интеллекта от человека, которые показывают, что на основе анализа результатов функционирования в целом ряде случаев выявить различия не удается. Отсюда возникает главный вопрос: останется ли система искусственного интеллекта контролируемой сознанием человека либо самовольно выйдет из-под контроля.

Ответ на этот вопрос можно попытаться получить на основе классической теории управления, в которой четко выделяются большие системы, отличительным признаком которых является большое число элементов, и сложные системы, для которых характерным является наличие множества подсистем, в результате взаимодействия которых сложная система приобретает новые свойства, а также неизученность связей между ними и как следствие – «необъяснимость» их взаимодействия. Можно утверждать, что перспективным является подход к разработке и изучению системы искусственного интеллекта, основанный на рассмотрении ее одновременно как большой и сложной системы управления. С развитием искусственного интеллекта для таких систем характерно увеличение энтропии их поведения, что является залогом саморазвития большой и сложной системы. А отсюда возникает угроза, что в перспективе системы искусственного интеллекта могут выйти из-под контроля человека. Целенаправленные ограничения энтропии проектируемой системы искусственного интеллекта лишают ее возможности самообучения и развития, отказ от таких ограничений увеличивает вероятность ее неуправляемого развития. В связи с этим при разработке и внедрении таких систем в условиях перехода в общество знаний особую актуальность приобретает применение и развитие методов информационно-психологической и когнитивной безопасности, что особенно важно для сложных систем искусственного интеллекта, в контуре обратной связи которых присутствует человек.

В докладе рассматриваются модели угроз и обсуждаются предложения по совершенствованию непрерывной системы подготовки и переподготовки кадров в области информационной безопасности [3], в том числе нацеленные на предотвращение угроз, характерных для этапа перехода к обществу знаний, и формирование у выпускников профессиональных компетенций, носящих опережающий характер.

СПИСОК ЛИТЕРАТУРЫ

1. Советов, Б.Я., Касаткин, В.В Современное состояние информационного общества и перспективы перехода в общество знаний // Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет; науч. ред. : Б.В. Соколов. – Севастополь: СевГУ, 2021. – 211с. С. 5-9.
2. Советов, Б.Я., Касаткин, В.В Информационное общество и искусственный интеллект // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 8 / СПОИСУ. – СПб., 2020. – 474 с. С. 117-120
3. Советов, Б.Я., Касаткин, В.В. Перспективные направления подготовки кадров в области искусственного интеллекта // Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет; науч. ред. : Б.В. Соколов. – Севастополь: СевГУ, 2021. – 211с. С. 102-106.

УДК 681.3.004.8

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СТРАТЕГИЧЕСКИХ СИСТЕМАХ УПРАВЛЕНИЯ СОЦИАЛЬНЫМ И ЭКОНОМИЧЕСКИМ РАЗВИТИЕМ СУБЪЕКТОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Соколенко Виктор Николаевич
Северо-Западный институт управления РАНХиГС
Средний пр., В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: sokolenko-vn@ranepa.ru

Аннотация. В статье рассматривается обеспечение информационной безопасности в создаваемых стратегических системах управления социальным и экономическим развитием субъектов Российской Федерации на основе комплексного подхода с использованием методов искусственного интеллекта по прогнозированию состояния информационной безопасности.

Ключевые слова: информационная безопасность; искусственный интеллект; система стратегического управления; экономическое и социальное развитие; субъекты Российской Федерации.

ENSURING INFORMATION SECURITY IN STRATEGIC SYSTEMS FOR THE MANAGEMENT OF SOCIAL AND ECONOMIC DEVELOPMENT OF ENTITIES OF THE RUSSIAN FEDERATION

Sokolenko Viktor
The North-West Institute of Management of RANEPA
57/43 Sredny Av, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: sokolenko-vn@ranepa.ru

Abstract. The article considers ensuring information security in the created strategic systems for managing the social and economic development of the constituent entities of the Russian Federation on the basis of an integrated approach using artificial intelligence methods to predict the state of information security.

Keywords: information security; artificial intelligence; strategic management system; economic and social development; subjects of the Russian Federation.

Введение. Главная особенность современного этапа стратегического развития Российской Федерации (РФ) заключается в признании особой роли, которую начала играть цифровая трансформация государственного управления (ГУ) и бизнеса. Переход страны, в целом, и субъектов РФ, в частности, к цифровой трансформации ГУ и бизнеса, связывается, несмотря на множество возможностей, главным образом с экономическим ростом, который должен обеспечиваться инновационным развитием во всех областях. И все возрастающую роль при стратегическом управлении социальным и экономическим развитием (СЭР) территорий субъектов РФ, как хозяйствующих субъектов, начинает играть создание стратегических систем управления (ССУ), которые относятся к классу больших информационных систем (БИС), представляющим определенную категорию сложных систем. К основным свойствам этих систем можно отнести следующие [1]:

– обеспечение функционирования пространственно – распределенных объектов, расположенных на определенном удалении друг от друга;
– наличие разнородных элементов в системе, находящихся в сложной взаимосвязи;
– динамический характер функционирования такой сложной системы;
– иерархичность структуры и многоцелевые решаемые задачи управления;
– наличие сотрудников, на которых возложены обязанности по обслуживанию системы в интересах управления;
– стохастический характер внешних информационных воздействий (ВИВ) на систему;
– большое время создания и значительный жизненный цикл, и модернизации системы.

Стратегические системы управления СЭР субъектов РФ создаются для обеспечения реализации полномочий органов государственной власти и местного самоуправления в соответствии с целями, установленных федеральными законами, в первую очередь, федеральным законом № 172 от 28 июня 2014 года «О стратегическом планировании». А также на них возлагается информационный обмен между соответствующими уровнями управления. Владение информацией необходимого качества в нужное время и в нужном месте, несомненно, является залогом успеха в любом виде деятельности, особенно, в хозяйственной деятельности. Но можно утверждать, что в создаваемых ССУ СЭР субъектов РФ необходимо, в первую очередь, обеспечить информационную безопасность (ИБ) при их функционировании. Под ИБ, в широком смысле, понимается состояние защищенности важнейших интересов государства, общества и личности в информационной среде. И поэтому проблема обеспечения ИБ становится особенно актуальной при создании ССУ СЭР субъектов РФ с целью поддержания должного уровня качества управления, которая не снимается и сегодня с повестки дня. Предложения по основам проектирования и создания ССУ СЭР субъектов РФ сформулированы с участием автора в [2]. Но в связи с развитием процессов цифровизации ГУ в настоящее время имеются актуальные и нерешенные информационные проблемы, рассмотренные с участием автора в [3]. Так как современное информационное пространство настолько доступно и открыто, что возможности злоупотребления им фактически не ограничены. Наличие таких проблем свидетельствует о том, что в постиндустриальном обществе информация с точки зрения государственной и экономической безопасности выступает в двух категориях: как основа формирования угроз во всех сферах общественной деятельности и как один из основных экономических продуктов и товаров, обеспечивающих развитие важнейшей составляющей постиндустриального общества – информационной. Для решения указанных проблем в интересах повышения эффективности ГУ, достижения устойчивого развития и обеспечения ИБ при создании ССУ СЭР субъектов РФ можно отметить, что используемые в настоящее время СЗИ имеют ряд существенных недостатков, которые не позволяют эффективно решать вопросы по обеспечению заданного уровня защищенности информации в течение всего жизненного цикла и модернизации таких аналогичных систем. Это объясняется сложившимися требованиями к архитектуре больших автоматизированных систем управления (АСУ). Существующие методы и средства защиты информации АСУ регионального значения, в основном, обеспечивают защиту информации лишь от известных угроз. Это определяет низкую эффективность применения имеющихся средств и СЗИ в настоящее время с учетом стохастического и практически постоянного появления новых угроз и увеличением их числа реализаций. Для повышения эффективности защищенности информации в создаваемых ССУ СЭР субъектов РФ необходимо при их проектировании закладывать упреждающие способы защиты информации, способные адаптироваться к любым изменениям ВИВ. Поэтому для эффективной защиты информации в таких системах необходимо использовать особые подходы, учитывающие особенности влияния условий ВИВ на информационные подсистемы в создаваемых ССУ СЭР субъектов РФ. На основе анализа информации в [4-6], можно выделить следующие особенности влияния условий ВИВ на БИС:

– проведение негативных воздействий на ограниченное число элементов БИС определенного уровня, как правило, нижнего. Это объясняется тем, что применение ВИВ на элементы всех уровней БИС требует привлечения большого объема ресурсов;
– большая степень неопределенности ВИВ в целом на БИС. Это связано с разнообразием её элементов, широким спектром хаотических воздействий и сложностью в их согласовании как по времени, так и по пространству, при масштабном применении;

– проведение ВИВ с учетом потенциальной возможности оперативного оповещения о нем на один из элементов БИС всех других её элементов и актуализации базы описаний ВИВ в каждом элементе системы, что связано с наличием разветвленных связей между элементами БИС;

– различная важность элементов БИС и разные подходы к обеспечению их ИБ, что предполагает выявление наиболее уязвимых элементов и сосредоточение ВИВ на них.

С учетом вышеизложенных особенностей для обеспечения ИБ при создании ССУ СЭР субъектов РФ необходимо разработать следующие методические положения:

– по выбору оптимальной стратегии реагирования ССУ СЭР субъектов РФ на ВИВ;

– по изменению свойств и параметров подсистемы защиты информации в ССУ СЭР субъектов РФ;

– по количественной оценке, уровня защищенности элементов ССУ СЭР субъектов РФ. При разработке этих методических положений целесообразно ориентироваться на их максимально возможную формализацию с целью создания на их основе алгоритмов системы поддержки принятия решений по управлению защитой информации в этой ССУ. В целом, разработка указанных методических положений необходима для создания способа построения и управления подсистемой защиты информации в ССУ СЭР субъектов РФ на основе теории искусственного интеллекта с распознаванием ВИВ и прогнозированием информационной среды, а также самоадаптацией и обоснованием автоматического приспособления к непредвиденным изменениям параметров ССУ СЭР субъектов РФ и внешней среды, который должен послужить основой для программно – аппаратной реализации. Одним из вариантов, который может быть положен в основу такого способа, целесообразно рассмотреть методические положения, изложенные в [7], существо которых состоит в следующем. Повышение вероятности защищенности информационно – вычислительной сети (ИВС) может достигаться за счет определения угроз вторжений и состояния ИБ с помощью математических алгоритмов, разработанных на основе древовидного классификатора и карт Кохонена. И тогда алгоритм управления должен включать: наблюдение и выделение признаков цифровых потоков с протоколами передачи данных, поступающих в ИВС и в используемый сервер, распознавание вторжения, выбор и реализация способа защиты. Предложенное в [8], в отличие от известных, должно позволить в создаваемых в ССУ СЭР субъектов РФ:

– учесть динамику и стохастическую неопределенность основных процессов защиты информации в этих системах;

– проводить мониторинг, распознавание вторжений и прогнозировать состояния при интеллектуальных процессах защиты;

– обеспечивать возможность обоснованного принятия решения на проведение мероприятий по предотвращению реализации угроз безопасности ССУ СЭР субъектов РФ за счет прогнозирования состояния ИБ.

Заключение. Предлагаемый подход обеспечения ИБ в создаваемых в ССУ СЭР субъектов РФ позволит осуществить оперативное перестроение структуры СЗИ элемента, подвергнувшегося ВИВ, а также произвести подготовку решения о возможном изменении структуры СЗИ остальных элементов ССУ, в случае необходимости отражения ВИВ. Кроме того, это должно сопутствовать повышению качества управления при функционировании ССУ СЭР в субъектах РФ, имея в виду перспективу полного перехода управленческих структур на платформу стратегического видения будущего и его конструирования в интересах повышения качества жизни населения в субъектах РФ.

СПИСОК ЛИТЕРАТУРЫ

1. Лисенкова А.А, Левкин И.М. Обеспечение информационной безопасности государственных информационных систем - Труды Всероссийского Форума, Санкт - Петербург, 25-27 октября 2017 г. «Система распределенных ситуационных центров как основа цифровой трансформации государственного управления «СРСЦ–2017». /Научный совет по информатизации Санкт - Петербурга. - СПб.: ООО «Политехника Сервис». 2018. с.179 - 181
2. Баранец С.Н., Соколенко В.Н. Основы проектирования и создания стратегической системы управления экономическим и социальным развитием субъекта Российской Федерации – Материалы Всероссийской научно-практической конференции «Современное управление: векторы развития» – Калининград: ЗФ РАНХиГС, 2021. С. 239 – 245.
3. Баранец С.Н., Соколенко В.Н. Проблемы создания стратегической системы управления экономическим и социальным развитием субъекта Российской Федерации – Материалы XV Международной научно-практической конференции «Цифровые трансформации в развитии экономики и общества» 21 апреля 2021 г. – Воронеж: НАУКА-ЮНИПРЕСС, 2021. С. 339 - 346.
4. Володина А.А., Левкин И.М. Оценка эффективности процесса отражения информационных угроз в больших информационных системах// Приборостроение, № 5, 2016, с. 335-341.
5. Рахимов Е.А. Модели и методы поддержки принятия решений в интеллектуальной системе защиты информации: дис. Канд.техн.наук: 05.13.19. Уфа, 2006, с.237. РГБ ОД, 61:07-5/726.
6. Создание систем защиты информации государственных информационных систем [Электронный ресурс]. URL: http:// www.dialognauka.ru/solutions/ security_ gosinfosystem/(дата обращения 12.07.2020 г.).
7. Липатников В.А., Литвинов А.А., Сахаров Д.В. Управление информационно – вычислительной сетью с распознаванием вторжений и прогнозированием состояния информационной безопасностью - Труды Всероссийского Форума, Санкт - Петербург, 25-27 октября 2017г. «Система распределенных ситуационных центров как основа цифровой трансформации государственного управления «СРСЦ–2017». /Научный совет по информатизации Санкт - Петербурга. - СПб.: ООО «Политехника Сервис». 2018. с.176 – 179.

УДК 378

ПРИНЦИПЫ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ УПРАВЛЕНИЯ ПРОЕКТАМИ УМНОГО ГОРОДА

Соколова Екатерина Владимировна
Санкт-Петербургский государственный университет
Волховский пер., 1-3, Санкт-Петербург, 199004, Россия
e-mail: sokolova@gsom.spbu.ru

Аннотация. Внедрение концепции умного города в практику развития городов становится основным направлением работы урбанистов. Однако подобная практика во многом носит рамочный характер в связи с отсутствием единого общепринятого подхода к определению того, что следует считать умным городом. Тем не менее, в условиях высоких темпов цифровизации экономики и процессов управления оправданно растет спрос на специалистов в данной сфере.

Ключевые слова: управление проектами; умный город; подготовка специалистов.

PRINCIPLES OF TRAINING SPECIALISTS IN THE FIELD OF SMART CITY PROJECT MANAGEMENT

Sokolova Ekaterina
Saint Petersburg State University
1-3 Volkhovskiy Ln, St. Petersburg, 199004, Russia
e-mail: sokolova@gsom.spbu.ru

Abstract. The introduction of the concept of a smart city into the practice of urban development is becoming the main focus of urbanists' work. However, this practice is largely of a framework nature due to the lack of a unified generally accepted approach to determining what should be considered a smart city. Nevertheless, in the conditions of high rates of digitalization of the economy and management processes, the demand for specialists in this area is justifiably growing.

Keywords: project management; smart city; training of specialists.

Можно выделить два основных подхода к определению умного города [1-3], которые находят свое применение в практике городского управления.

Наиболее привычный, но более узкий подход определяет умный город, как город, в котором находят повсеместное применение информационно-коммуникационные технологии, используемые для повышения эффективности реализации различных градообразующих функций и сервисов. Этот подход представляет собой определение умного города в рамках технологической парадигмы.

Подготовка специалистов в сфере технологической парадигмы умного города может и должна проводиться в рамках широко спектра инженерно-технических специальностей.

Второй, реже упоминающийся, но более широкий, системный подход к определению умного города сформировался в рамках управленческой парадигмы. В данном случае под умным городом понимается совокупность трех уровней организации инфраструктуры города: традиционная инфраструктура, смарт-технологии и Data Science, и люди, использующие данные технологии для удовлетворения собственных потребностей. И в этом случае подготовка специалистов в области умного города – задача управленческих специальностей.

Основная особенность подготовки специалистов в данном случае – это формирование у выпускников не только системного видения особенностей развития города и городских проблем, но и навыков общения со специалистами в области инженерно-технических специальностей с использованием единого языка.

Магистерская программа «Управление умным городом - Master in Smart City Management, MSC» сформирована таким образом, чтобы подготовить аналитиков, способных формировать тактические требования к проектам умного города на основании анализа стратегических целей городского развития и общего понимания особенностей функционирования города как сложной открытой системы.

Для реализации поставленных задач учебный план программы включает несколько сквозных образовательных треков, которые позволяют сформировать у выпускников широкий спектр компетенций, направленных на умение разрабатывать и воплощать в жизнь проекты умного города в тесном сотрудничестве с инженерно-техническими специалистами.

СПИСОК ЛИТЕРАТУРЫ

1. Thompson E. M. What makes a city “smart”? International Journal of Architectural Computing, 2016, pp.: 358-371.
2. Technopedia. Smart city definition. 2019. [Электронный ресурс]. URL: https://www.technopedia.com/definition/31494/smart-city (дата обращения: 21.03.2021).
3. Smart Cities Council. Definition of smart cities. 2019. [Электронный ресурс]. URL: https://smartcitiescouncil.com (дата обращения: 18.04.2021).

УДК 004.9:351.9

СЕРВИСЫ ЦИФРОВОГО ЗДРАВООХРАНЕНИЯ В САНКТ-ПЕТЕРБУРГЕ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Фокин Сергей Андреевич
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: Sfokin@spbmiac.ru

Аннотация. В докладе представлены сведения о применении основных сервисов и подсистем государственной информационной системы Санкт-Петербурга в сфере здравоохранения (ГИС РЕГИЗ), применяемых и активно развивающихся в период сложной эпидемической ситуации и оказывающих значительное влияние на качество и своевременность оказания медицинской помощи жителям города в период пандемии COVID-19. Также в докладе отражены преимущества и возможности для органов управления здравоохранением и ИОГВ Санкт-Петербурга в части подготовки аналитической информации и информационных панелей для руководителей разных уровней. Определены слабые стороны цифровизации в здравоохранения и обозначены планы по развитию отрасли.

Ключевые слова: информационные ресурсы; здравоохранение; цифровизация; covid-19; аналитика; мониторинг; рейтингование.

DIGITAL HEALTH SERVICES IN ST. PETERSBURG TO ENSURE LIFE SAFETY

Fokin Sergei
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mail: Sfokin@spbmiac.ru

Abstract. The report presents information on the use of the main services and subsystems of the state information system of St. Petersburg in the field of health care (GIS REGIZ), used and actively developing during a difficult epidemic situation and having a significant impact on the quality and timeliness of medical care for city residents during the pandemic. COVID-19 The report also reflects the advantages and opportunities for health authorities of St. Petersburg in the preparation of analytical information and information panels for managers at different levels. Weaknesses of digitalization in healthcare were identified and plans for the development of the industry were outlined.

Keywords: information resources; healthcare; digitalization; covid-19; analytics; monitoring; rating.

В настоящее время Минздравом в рамках национального проекта «Здравоохранение» реализуется федеральный проект «Создания единого цифрового контура здравоохранения на основе ЕГИСЗ» [1] (далее – «Цифровой контур»). Проект направлен на создание механизмов взаимодействия медицинских организаций на основе ЕГИСЗ, что должно обеспечить цифровое преобразование и повышение эффективности функционирования отрасли здравоохранения на всех уровнях и создать условия для использования гражданами электронных услуг и сервисов в сфере здравоохранения. Внедрение региональных сегментов ЕГИСЗ и электронной медицинской карты становится ключевым элементом управления в здравоохранении на ближайшие годы. На федеральном уровне в последнее время принят ряд документов по электронному документообороту. А в Санкт-Петербурге в феврале 2018 года Комитет по здравоохранению издал распоряжение о создании и ведении электронной медицинской карты петербуржца [2], которое опирается на постановление о региональном фрагменте ЕГИСЗ.

Вместе с развитием медицинских информационных систем в медицинских организациях идет создание инфраструктуры, позволяющей пациентам управлять своими данными, добавлять данные о своем состоянии здоровья и принимаемых медикаментах, а также получать доступ к своей электронной медицинской карте и предоставлять доступ другим врачам по своему желанию. Практика показывает, что внутри организации необходимо сохранить доступ врачей ко всей медицинской информации, возможно, закрыв лишь очень узкий перечень документов. Но наибольшие сложности возникают при попытке получить доступ к данным из других организаций. Так, например, участковому терапевту при планировании визита к пациенту с подозрением на COVID-19 важно знать историю предыдущей госпитализации пациента в стационар, какие были проведены оперативные вмешательства и какие рекомендации дал лечащий врач при выписке пациента, какие сопутствующие заболевания есть у пациента, необходимо ли взять пациента на диспансерное наблюдение. Эта информация позволяет повысить качество и решить задачи преемственности оказания медицинской помощи.

Эту задачу в Санкт-Петербурге решает Государственная информационная система «Региональный фрагмент единой государственной информационной системы в сфере здравоохранения» (ГИС РЕГИЗ). Цели, стоящие перед информационной системой: обеспечение эффективной информационной поддержки процесса управления системой медицинской помощи, а также процесса оказания медицинской помощи, обеспечение преемственности медицинской помощи, повышение качества оказания медицинской помощи на основе совершенствования информационно-технологического обеспечения деятельности медицинских и фармацевтических организаций, повышение информированности населения по вопросам ведения здорового образа жизни, профилактики заболеваний, получения медицинской помощи, качества обслуживания в

медицинских организациях, а также осуществления деятельности в сфере здравоохранения на основе обеспечения возможностей электронного взаимодействия с соответствующими уполномоченными организациями.

Федеральные информационные ресурсы также обеспечивают процессы поддержания высокого уровня безопасности жизни и информирования пациентов о результатах его состояния здоровья. Сюда входят и процессы управления вакцинацией взрослого населения в том числе с использованием единого портала государственных услуг и функций, организация сбора хранения и использования информации об результатах лабораторных исследований на определение особо опасных видов заболеваний, создание и ведение специализированных регистров пациентов в рамках региона и всей страны. Данные информационные ресурсы требуют создания поддержки на региональном уровне новых бизнес-процессов по работе с данными пациента и определяют новые возможности межведомственного взаимодействия.

Наиболее важной составляющей является возможность построения аналитических информационных панелей, решающих задачи мониторинга и контроля распространения опасных заболеваний. Обеспечение интеграционного взаимодействия между собой аналитических систем комитета по здравоохранению, Администраций районов, ситуационного центра при аппарате губернатора Санкт-Петербурга и федеральными подсистемами ЕГИСЗ.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный проект «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)» // Министерство здравоохранения РФ [Электронный ресурс]. URL: https://minzdrav.gov.ru/poleznye-resursy/natsproektzdravoohranenie/tsifra (дата обращения: 30.09.2021).
2. Распоряжение «О создании и ведении "Электронной медицинской карты петербуржца"» [Электронный ресурс]. URL: https://docs.cntd.ru/document/554224794 (дата обращения: 30.09.2021).

ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 004.056.5

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОТРУДНИКОВ ОВД В ПЕРИОД ПРОВЕДЕНИЯ ИНФОРМАЦИОННЫХ ВОЙН

Беляев Леонид Сергеевич, Локнов Алексей Игоревич
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: stevenson28@mail.ru, info_for_aleksey@mail.ru

Аннотация. Рассматривается вопрос обеспечения информационной безопасности сотрудников ОВД в период проведения информационных войн.

Ключевые слова: информационные технологии; информационное противоборство; имидж сотрудников ОВД.

FEATURES OF PROVIDING INFORMATION SECURITY OF ATS EMPLOYEES DURING INFORMATION WARS

Belyaev Leonid, Loknov Alexey
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: stevenson28@mail.ru, info_for_aleksey@mail.ru

Abstract. The issue of ensuring the information security of police officers during the period of information wars is considered.

Keywords: information Technology; information confrontation; image of police officers**.**

Введение. На сегодняшний день в обществе наметилось устойчивое развитие социальных изменений за счёт высокой скорости цифровых трансформаций [1]. За последние несколько десятилетий произошли колоссальные преобразования, как в мире информационных технологий, так и в восприятии и отношении к источникам информации. Стремительный рост социальной значимости Интернета стимулировал конкуренцию и соперничество за «вещательную инициативу» среди «поставщиков информации», размещающих в достаточном объёме непроверенные, провокационные и дезинформационные («фейковые») сообщения, тем самым перегружающих информационное пространство и воздействующих на мировоззрение и взгляды своих активных пользователей – будь то обычный интернет обыватель или государственный служащий. Из всего вышеизложенного вытекает мысль о том, что данное пространство обладает собственной тенденцией развития, имеет характеристики специфического мира, обладающего интерсубъективностью.

В рамках данной статьи вопрос обеспечения информационной безопасности сотрудников ОВД будет рассмотрен применительно к практической деятельности соответствующей структуры. Актуальность выбранного направления заключается в том, что на данный момент времени вопрос информационного противоборства с участием сотрудников МВД России остается открытым.

Деятельность органов внутренних дел постоянно находится в центре внимания современной общественности. Причём на данном этапе развития коммуникационных технологий общество все чаще стало использовать интернет-ресурсы для обсуждения работы данного органа, так как в большинстве своём при виртуальной дискуссии пользователи остаются анонимными. Многолетние социологические исследования в области изменения общественного мнения показывают, что в сознании россиян имидж органов внутренних дел не слишком высок. При этом критические оценки работы полиции зачастую основаны не на собственном жизненном опыте граждан, а на бытующих в обществе стереотипных представлениях об органах внутренних дел, имеющих под собой не всегда достоверные основания. Из-за колоссального количества информационных площадок, правоохранительные органы Российской Федерации не всегда в состоянии своевременно реагировать на процессы движения информационных потоков, тем самым допускается просачивание ложной, порой порочащей честь и достоинство сотрудника государственного органа (в данном случае говорится о сотрудниках полиции) информации касающейся его служебной деятельности [2].

На важность позитивного имиджа полиции в обществе в своих публичных выступлениях неоднократно обращало внимание руководство страны. Например, Президент Российской Федерации В.В. Путин на заседании расширенной коллегии МВД России в марте 2016 года указал, исходя из статистики и опросов граждан, что

общество доверяет именно тем сотрудникам, которым присущи такие качества как высокий профессионализм и приверженность моральным убеждениям. Было отмечено, что «граждане одобряют даже репрессивные меры со стороны честных сотрудников органов внутренних дел, если они осуществляются в интересах общества. А недостойное поведение самих полицейских воспринимается населением «как предательство» и крайне негативно сказывается на образе Министерства внутренних дел и государства в целом» [3].

В ходе исследования локального информационного противоборства было выявлено, что негативное информационно-психологическое воздействие на сотрудников нацелено на то, чтобы лишить их веры в справедливость своего дела, утратить чувство патриотизма и гордости за принадлежность к органам внутренних дел, заставить их считать неприемлемым выполнение своего служебного долга, отказываться или саботировать выполнение своих служебных обязанностей по защите прав и свобод граждан, противодействию преступности, охране общественного порядка и обеспечению общественной безопасности.

Выведение сотрудников из состояния психологической устойчивости необходимо для того, чтобы не дать им возможности анализировать события, заставить их совершать импульсивные, необдуманные, опрометчивые действия. Для этого используются такие способы, как физическое воздействие, моральное оскорбление, обвинения, устрашение и т.д. Самой распространенной формой такого воздействия являются видео сюжеты с комментариями о действиях сотрудников полиции. Одни из них носят постановочный характер, другие гиперболизируют и детализируют отдельные ошибки и недостатки в их деятельности. В этих сюжетах сотрудники показаны как субъекты, противостоящие народу, игнорирующие российские законы.

Субъекты негативного информационного воздействия на сотрудников ОВД в процессе выполнения ими «профессиональных» задач используют различные приемы. Д. Шарп («идеолог цветных революций») в своей книге порекомендовал 198 способов борьбы против власти [4]. Среди этих способов описываются такие конкретные приемы воздействия на представителей органов правопорядка, как письма протеста, карикатуры, листовки, памфлеты, аудио записи, надписи на земле, пикетирование, символические звуки, грубые жесты, выставление портретов, рисунки, насмешки над официальными лицами, пародии, символические похороны, молчание, неохотное и медленное подчинение, невыполнение приказа разойтись (собранию или митингу), сидячая забастовка, «голодовка морального давления». Анализ протестных событий в России показывает, что их организаторы используют рекомендации Д. Шарпа как прямое руководство к практическому действию.

Социологи выдвинули предположение о том, что в своих действиях, направленных на информационное противодействие ОВД, субъекты придерживаются следующего порядка: вначале дезориентация, затем деморализация, а в конечном итоге дезинтегрирация представителей правоохранительного органа.

Подходов к разрешению проблемы неуважения сотрудников правоохранительных органов в обществе существует множество:

Первое, безусловно, необходимо рассказывать на страницах печатных средств массовой информации и радио, показывать на телевидении и в кино, размещать в интернет-пространстве информацию об истории и героическом прошлом органов внутренних дел, о современном состоянии и особенностях деятельности всех служб и подразделений МВД России, результатах их деятельности, предоставляемых государственных услугах. Тем самым будет создано определенное впечатление об организации работы органов внутренних дел. Все это очень важно для создания положительного медийного образа

Второе, органы внутренних дел должны представлять не только итоги своей деятельности, но прежде всего своих конкретных сотрудников. Необходимо проработать концептуальные подходы к формированию имиджа органов внутренних дел как о современной структуре. Технология создания имиджа предполагает активное использование информационного направления деятельности, то есть представления образа учреждения и оценки существования как побуждающего эмоции, вызываемые информацией, рассчитанной на определенную эмоционально-психологическую реакцию (именно для этого в 2014 году был создан конкурс PR-проектов «Моя полиция», проводимый в территориальных органах ОВД по всей стране).

Заключение. Таким образом, приоритетным направлением в контексте решения обозначенных проблем является обеспечение защиты личности сотрудника ОВД от внутренних и внешних информационных угроз, а также планомерное развитие пропаганды деятельности правоохранительных органов по всей России. Стратегия по пропаганде деятельности ОВД, в частности полиции, должна быть продумана, хорошо организована и спланирована, а самое главное – научно и методически обеспечена. В результате проводимой «медийной» политики в итоге ожидается получить положительно воспринимаемый имидж сотрудника полиции.

СПИСОК ЛИТЕРАТУРЫ

1. Локнов А.И. Совершенствование электронной информационно-образовательной среды как структурного элемента развития цифровой экономики// Использование современных цифровых технологий в деятельности образовательных организаций силовых ведомств. Актуальные проблемы и тенденции развития: Сборник материалов Международной научно-практической конференции, Уфа, 16–17 мая 2019 года/Под общей редакцией А.С. Ханахмедова. – Уфа: УЮИ МВД России, 2019. – С. 27-32.
2. Соколова М.В., Дозорцева Е.Г. Склонность к аутоагрессивному поведению у подростков и информация, потребляемая ими в интернете // Психология и право. 2019. Т. 9. № 1. С. 22—35.
3. Расширенное заседание коллегии МВД 15 марта 2016 г. [Электронный ресурс] – Режим доступа. – URL: http://www.kremlin.ru/events/president/news/51515 (Дата обращения 07.09.2021 г.).
4. Д. Шарп // «От диктатуры к демократии: Стратегия и тактика освобождения», 1993 г.

УДК 004.056.5

О НЕКОТОРЫХ ВОПРОСАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИСОД МВД РОССИИ

Бобонец Сергей Алексеевич, Мясников Илья Олегович
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: sbobon@mail.ru, unkownsmail@gmail.com

Аннотация. Рассматривается вопрос о внутренних угрозах информационной безопасности системы информационной системы обеспечения деятельности (сокр. ИСОД) МВД России и освещаются некоторые требования по их устранению.

Ключевые слова: информационная система; угроза информационной безопасности; информационная безопасность.

SOME ISSUES OF INFORMATION SECURITY ISOD MIA RUSSIA

Bobonets Sergey, Myasnikov Ilya
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: sbobon@mail.ru, unkownsmail@gmail.com

Abstract. The article considers the issue of internal threats to information security of the information system for the support of activities (abbreviated ISOD) of the Ministry of Internal Affairs of Russia and highlights some requirements for their elimination.

Keywords: information system; information security threat; information Security.

Учитывая современные угрозы информационным объектам, и, в частности, ИСОД МВД России, следует признать необходимость мер по защите информации в системе МВД России. Наиболее значимой угрозой безопасности ИСОД МВД России является внутренняя. Для управления доступом пользователей в ИСОД МВД России служит сервис управления доступом к информационным системам и ресурсам – СУДИС. Несмотря на отработанные механизмы защиты информации при работе с ИСОД МВД России, у сотрудников ОВД возникают проблемы.

Аутентификация в ИСОД заключается в проверке СУДИС введенных сотрудником данных в форму аутентификации. При корректном ее заполнении сотрудник получает доступ к желаемому сервису. Одной из схем аутентификации является использование паролей. Однако для пользователей зачастую запоминание своих учетных данных для доступа к информационным системам является проблемой. В результате порядок использования учетных данных пользователями часто не удовлетворяет политикам безопасности, так пользователи записывают свои пароли на бумаге, устанавливают простейший пароль и т. п. Подобные нарушения допускаются как непредумышленно, так и сознательно, когда сотрудник относится к угрозе компрометации пароля с безразличием.

Также, одной из проблем является нарушение порядка использования учетной записи при работе на АРМ в многопользовательском режиме. Заключается нарушение в невыполнении требования использовать для входа в ОС только персональные идентификационные данные, а после завершения работы на АРМ - невыполнение обязательного выхода из ОС АРМ. Причинами могут быть личная недисциплинированность сотрудника, либо несвоевременная выработка представителем Удостоверяющего Центра ключа электронной подписи каждому из сотрудников в силу организационных проблем или фактического отсутствия в подразделении носителей электронной подписи.

К сотрудникам органов внутренних дел предъявляются достаточно высокие квалификационные требования, законодательно закреплена необходимость сотрудника полиции при исполнении своих служебных обязанностей использовать автоматизированные информационные системы, интегрированные банки данных, средства связи, а также современную информационно-телекоммуникационную инфраструктуру [1]. Обработка документов, осуществляемая с помощью средств вычислительной техники сотрудниками ОВД, должна выполнятся при условии жесткого соблюдения требований по защите информации. Контроль за вопросами информационной безопасности возложен на каждого сотрудника-пользователя ИСОД МВД России [2]. Данное требование прописано в должностных регламентах и в технических инструкциях, изучение которых - одно из условий допуска сотрудников к пользованию средствами ИСОД МВД России. Контроль за соблюдением требований исключает предпосылки для возникновения угроз безопасностей разных типов начального уровня.

На сегодняшний день средства защиты информационных систем МВД России работают в автоматическом режиме, не требуя от пользователя каких-либо действий с настройками программного обеспечения, сотрудникам ОВД достаточно неукоснительно выполнять правила, прописанные в инструкциях и регламентах сотрудников, допущенных к работе с ведомственными информационными ресурсами. Не менее важным является регулярное повышение квалификации действующих сотрудников в вопросах выполнения мер защиты информации при работе в информационно-телекоммуникационных системах МВД России.

СПИСОК ЛИТЕРАТУРЫ

1. О полиции: Федеральный закон от 07 февраля 2011 г. № 3-ФЗ ст. 11//Собрание законодательства РФ. 2011. – №7.
2. О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 30.11.2011 № 342-ФЗ// Собрание законодательства РФ. 2011. – №7.

УДК 004.056.5

МОДЕЛЬ «НУЛЕВОГО ДОВЕРИЯ» КАК ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БУДУЩЕГО

Игнатов Данил Юрьевич, Локнов Алексей Игоревич
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: da.ignatoff@gmail.com, info_for_aleksey@mail.ru

Аннотация. Анализируется модель информационной безопасности «нулевого доверия». Приводится алгоритм для создания системы защиты информации на основе «нулевого доверия». Рассматриваются достоинства и недостатки предложенной концепции и перспективы её применения в обеспечении информационной безопасности.

Ключевые слова: информационная безопасность; защита информации; модель «нулевого доверия»; кибератака.

THE "ZERO TRUST" MODEL AS THE BASIS OF INFORMATION SECURITY OF THE FUTURE

Ignatov Danil, Loknov Alexey
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: da.ignatoff@gmail.com, info_for_aleksey@mail.ru

Abstract. The model of information security of "zero trust" is analyzed. An algorithm for creating an information security system based on "zero trust" is given. The advantages and disadvantages of the proposed concept and the prospects for its application in ensuring information security are considered.

Keywords: information security; information protection; "zero trust" model; cyber-attack.

Введение. В настоящее время мы являемся свидетелями того, как стремительно меняется спектр угроз информационной безопасности, сегодня атаку следует ожидать отовсюду в любой момент. В связи с этим, наиболее целесообразно обезопасить себя не доверяя никому. Как бы утопично это не звучало, на этом строится одна из перспективных концепций информационной безопасности «нулевого доверия» (Zero Trust).

В традиционном подходе при построении модели защиты информационной инфраструктуры специалисты исходят из принципа «защиты периметра». Основная идея этого принципа состоит в том, что необходимо уделять особое внимание всем подключениям к ресурсам компании извне, хотя, при этом, внутри корпоративной сети образуется доверенная зона, в которой пользователи, устройства и приложения имеют определенную свободу действий и пользуются определенной степенью доверия [1].

Еще совсем недавно можно было утверждать, что защита периметра была эффективна, когда доверенная зона ограничивалась локальной сетью и подключенным к ней устройствам. Однако же информационные технологии развиваются семимильными шагами, что способствует появлению на рынке новых решений для построения инфраструктуры компании, к которым можно отнести облачные сервисы или мобильные устройства сотрудников, ставшие неотъемлемой частью информационных процессов организации. В связи с этим сегодня немалая часть корпоративных ресурсов компании находится за ее физическими пределами и понятие «периметра» размылось, что позволяет злоумышленникам использовать широкий спектр уязвимостей для проникновения внутрь доверенной зоны.

Авторство концепции «нулевого доверия» приписывают Джону Киндервагу (John Kindervag) аналитику компании Forrester Research, сотрудники которой еще в 2010 году официально признали недостатки модели «защищенного периметра» [2]. Вместо традиционного подхода «обороны границ», компаниям было предложено ориентировать системы обеспечения информационной безопасности на данные, а также отказаться от разделения ресурсов на внешние и внутренние. Предложенная концепция предполагала полное отсутствие доверенных зон, так как в рамках реализации этой модели, пользователи, устройства и приложения подлежат проверке при каждой попытке подключения к корпоративным ресурсам. Основным преимуществом модели «нулевого доверия», в таком случае, является отсутствие необходимости построения детальной модели угроз, поскольку авторы концепции исходили из того, что инцидент может возникнуть где угодно и когда угодно.

В первую очередь для реализации «нулевого доверия» потребуется собрать информацию об инфраструктуре, определить конфиденциальные данные, где они хранятся, как перемещаются, насколько они уязвимы, а также ограничить права доступа к ним.

Концепция «нулевого доверия» в ограничении прав доступа базируется на использовании модели наименьших привилегий и контроле доступа. Модель наименьших привилегий – это парадигма безопасности, основанная на ограничении прав доступа пользователя до того уровня, который необходим ему для выполнения служебных обязанностей. Такое решение позволяет нам препятствовать злоумышленнику в получении доступа к большому объему активов путем компрометации одного аккаунта. Также необходимо использовать ролевую модель контроля доступа (Role Based Access Control), позволяющую достичь наименьших привилегий и предоставить руководителям возможность самостоятельно управлять разрешениями к подконтрольным им

активам. Однако это будет эффективно работать только при условии проведения регулярной аттестации прав пользователей.

При построении защиты на основе «нулевого доверия» предполагается сегментирование корпоративной сети на небольшие узлы, чтобы затруднить боковое перемещение уже проникших в нее злоумышленников. На выходе получается, что вокруг каждого актива компании создается свой микропериметр со своей политикой безопасности и правами доступа. В таком случае, каждый корпоративный ресурс становится своеобразной «крепостью», для входа в которую пользователю необходимы «ключи». Под «ключами» следует понимать ряд процедур проверки, происходящих при обращении к какому-либо корпоративному ресурсу:

Идентификация и аутентификация пользователя. Первый этап проверки заключается в распознавании пользователя по его идентификатору, а также подтверждении своей личности путем аутентификации, при попытке доступа к ресурсу. Модель «нулевого доверия» призывает использовать на данном этапе многофакторную аутентификацию;

Проверка прав. На следующем этапе система проверяет наличие у авторизованного пользователя прав доступа к ресурсам, которыми он хочется воспользоваться;

Проверка безопасности соединения. Доступ к одним ресурсам разрешен из любой точки мира, к другим – исключительно по защищенному каналу, а к некоторым – только с определенных устройств внутри защищенных помещений.

Основная идея такой сложной проверки заключается в том, что необходимо рассматривать каждую попытку доступа к ресурсам как угрозу до тех пор, пока не подтвердится обратное. Если пользователь успешно прошел все стадии проверки своего запроса, то доступ предоставляется, в ином случае – подключение блокируется. Таким образом, мы получаем комплексную систему, обеспечивающую защиту нашей инфраструктуры на каждом этапе подключения к корпоративным ресурсам.

Принципы «нулевого доверия» подразумевают тотальный контроль всех корпоративных ресурсов. Для эффективного внедрения данной концепции подразделение информационной безопасности должно иметь возможность управлять всеми устройствами и приложениями. Помимо этого, необходимо вести учет и аналитику собранных логов на конечных устройствах, а также в других элементах инфраструктуры для оперативного обнаружения угрозы в сети.

За 11 лет с момента первого упоминания идеи модели «нулевого доверия» данная концепция хоть и развилась в достаточно формализованный подход к обеспечению информационной безопасности, однако сложно сказать, что существует единый подход к развертыванию системы безопасности, основанной на ее принципах. В то же время, специалисты все-таки выделяют основные пять шагов [3], которые необходимо пройти компании для создания системы защиты информации на основе «нулевого доверия»:

1 шаг. Внедрение решения для автоматизированного обнаружения и классификации конфиденциальных данных.

2 шаг. Определение потоков информации и настройка системы мониторинга. Это позволит компании получить наглядную карту перемещения конфиденциальной информации, а также возможность централизованно управлять правами доступа и отслеживать нестандартное поведение пользователей внутри сети.

3 шаг. Создание микропериметров «нулевого доверия». На данном этапе целесообразно внедрять уже готовые комплексные решения, позволяющие проводить границы и сканировать трафик, выявляя в нем аномалии и блокируя потенциальные векторы атаки.

4 шаг. Внедрение постоянного контроля и мониторинга с использованием аналитических инструментов безопасности. На этом этапе происходит оптимизация и интеграция уже существующих решений информационной безопасности в компании: осуществляется непрерывное сканирование данных, проверка списков контроля доступа в реальном времени, анализ событий, блокирование аномалий и оповещение подразделения информационной безопасности о возможном инциденте.

5 шаг. Адаптация и автоматизация работы системы. На последнем этапе необходимо внедрить средства автоматизации управления системой, ведь подобная система будет слишком сложна для ручного администрирования решений в области информационной безопасности.

Конечно, было бы неправильно осветить только преимущества модели «нулевого доверия», она также как и другие модели имеет свои слабые места. Хотя изначально подобная концепция информационной безопасности предназначена для борьбы с изъянами в защите вплоть до предотвращения выявленных угроз, однако исключить абсолютно все невозможно. Инсайдерские угрозы, как и в классической «защите периметра», очень сложно выявить, а тем более предотвратить: администратор, имеющий доступ к конфигурации ядра политики безопасности, может изменить правила. По-прежнему для снижения уровня этого риска используют системы аудита и регистрации событий. Также система на основе «нулевого доверия» подвержена атакам типа «отказ в обслуживании» (DoS), а также перехватам маршрутов в случае, когда злоумышленник нарушил доступ к точке реализации политик (PEP). Снизить подобный риск можно с помощью размещения PEP в облаке или ее репликация в нескольких местах. Различные отчеты о расследовании инцидентов компрометации данных показывают, что на сегодняшний день одной из самых серьезных угроз для любой модели безопасности является фишинг. Несмотря на постоянное обучение сотрудников основам информационной безопасности и повышение компьютерной грамотности, пользователи остаются самым слабым звеном в любой модели информационной безопасности. Вероятно, ничего так и не изменится, ведь основную причину такого поведения можно описать простым выражением: errare humanum est.

Заключение. Таким образом, переход от классической «защиты периметра» к обеспечению безопасности в рамках концепции «нулевого доверия» хотя и предполагает использование уже имеющихся решений, все-таки с точки зрения реализации может оказаться не таким быстрым и простым проектом. Однако, стоит отметить, что в дальнейшем переход на новую модель может обеспечить компании преимущества за счет снижения затрат на информационную безопасность, а также уменьшения числа инцидентов и ущерба от них.

СПИСОК ЛИТЕРАТУРЫ

1. Голубев Сергей «Концепция Zero Trust: не доверяй — всегда проверяй». – [Электронный ресурс] – Режим доступа. – URL: https://www.kaspersky.ru/blog/zero-trust-security/28780/ (Дата обращения 26.04.2021 г.).
2. Jeff Petters «What is Zero Trust? A Security Model». – [Электронный ресурс] – Режим доступа. – URL: https://www.varonis.com/blog/what-is-zero-trust/ (Дата обращения 26.04.2021 г.).
3. Stephanie Balaouras, Chase Cunningham, Peter Cerrato «Five Steps To A Zero Trust Network». – [Электронный ресурс] – Режим доступа. – URL: https://www.forrester.com/report/Five+Steps+To+A+Zero+Trust+Network/-/E-RES120510 (Дата обращения 26.04.2021 г.).

УДК 681.518 (004.031.42)

АВТОМАТИЗАЦИЯ ПРОЦЕССА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, СВЯЗАННОГО С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКИХ СРЕДСТВ НА ОБЪЕКТЕ ОРГАНА ВНУТРЕННИХ ДЕЛ ВТОРОЙ КАТЕГОРИИ

Кудрин Игорь Александрович, Потехин Владимир Семенович
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: f0rtuva0223@gmail.com, vsp1945@gmail.com

Аннотация. Излагается подход к автоматизации процесса обеспечения безопасности информации, связанного с использованием биометрических средств на объекте органа внутренних дел второй категории. Подход предполагает учет новых угроз, выявленных за время эксплуатации биометрических средств.

Ключевые слова: безопасность информации; биометрия; биометрические средства; биометрические данные; объект органов внутренних дел.

AUTOMATION OF THE INFORMATION SECURITY PROCESS RELATED TO THE USE OF BIOMETRIC PRODUCTS AT THE OBJECT OF THE INTERNAL AFFAIRS OF THE SECOND CATEGORY

Kudrin Igor, Potehin Vladimir
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: f0rtuva0223@gmail.com, vsp1945@gmail.com

Abstract. An approach to the automation of the process of ensuring the security of information associated with the use of biometric means at the object of the internal affairs body of the second category is presented. The approach involves taking into account new threats identified during the operation of biometric tools.

Keywords: information security; biometrics; biometric tools; biometric data; object of internal affairs bodies.

Введение. Использование биометрии приобретает все более повсеместный характер, в том числе находит применение в органах внутренних дел. Но одновременно с государственными структурами данная область привлекает внимание различных преступников, которые хотят использовать данную технологию в противоправных целях, а правоохранительные органы вынуждены постоянно совершенствовать и адаптировать средства защиты информации. В связи с этим тема данной работы, направленная на автоматизацию процесса обеспечения безопасности информации, связанного с использованием биометрических средств на объекте органа внутренних дел второй категории, является актуальной.

Для обеспечения автоматизации процесса обеспечения безопасности информации, связанного с использованием биометрических средств на объекте органа внутренних дел второй категории, представляется целесообразной следующая последовательность работ:

– выполнить анализ основных терминов в области биометрии [1];
– изучить возможности современных биометрических средств [2];
– проанализировать возможные угрозы использования биометрических данных преступниками, а также мер по их предотвращению [3];
– изучить типовые проектные решения оснащения техническими средствами объектов органов внутренних дел Российской Федерации, отнесённых ко второй категории [4];
– выполнить анализ общих аспектов и требований к форматам обмена биометрическими данными [5];
– изучить требования к средствам высоконадежной биометрической аутентификации [6];
– построить поведенческие модели (алгоритмы), обеспечивающие безопасность биометрических данных [7].

Заключение. Реализация перечисленных направлений, по мнению авторов, позволит поддерживать рассмотренную информационную технологию на приемлемом уровне и тем самым обеспечивать решение задачи автоматизации процесса обеспечения безопасности информации, связанного с использованием

биометрических средств на объекте органа внутренних дел второй категории в условиях появляющихся новых угроз.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ ISO/IEC 2382-37–2016 Информационные технологии. Словарь. Часть 37. Биометрия // М.: «Стандартинформ», 2006. – 27 с.
2. Мальцев А. Современные биометрические методы идентификации // Хабрахарб [Электронный ресурс] URL: https://habrahabr.ru/post/126144/ (дата обращения 30.07.2021).
3. Сборник практических рекомендаций Организации Объединенных Наций по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом [Электронный ресурс] URL: https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/_.pdf (дата обращения 30.07.2021).
4. Р 78.36.059-2016. Методические рекомендации «Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесенных к 2, 3 и 4 категориям». – М.: ФКУ «НИЦ «Охрана», 2016. – 386 с.
5. ГОСТ ISO/IEC 19794-1-2015 Биометрия. Форматы обмена биометрическими данными. Структура // М.: «Стандартинформ», 2015. – 32 с.
6. ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации // М.: «Стандартинформ», 2006. – 24 с.
7. ГОСТ 19.701-90 (ИСО 5807-85). Единая система программной документации. Схемы алгоритмов, программ, данных и систем. Условные обозначения и правила выполнения // М.: «Издательство стандартов», 1991. – 23 с.

УДК 004.056.5

СРЕДСТВА И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА РАБОЧЕМ МЕСТЕ СОТРУДНИКА ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Локнов Алексей Игоревич, Таранова Яна Эдуардовна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: info_for_aleksey@mail.ru, etoneyana39@gmail.com

Аннотация. Обеспечение безопасности информации в органах внутренних дел (ОВД) России представляет многогранную задачу, решаемую различными способами. Рассматриваются средства и методы, позволяющие обеспечить безопасность на рабочем месте сотрудника ОВД.

Ключевые слова: защита информации; информационная безопасность; средства; методы; рабочее место.

MEANS AND METHODS OF ENSURING INFORMATION SECURITY AT THE WORKPLACE OF AN EMPLOYEE OF THE INTERNAL AFFAIRS BODIES

Loknov Alexey, Taranova Yana
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: info_for_aleksey@mail.ru, etoneyana39@gmail.com

Abstract. Ensuring the security of information in the internal affairs bodies of Russia is a multifaceted task that can be solved in various ways. The means and methods that allow to ensure safety at the workplace of an employee of the Department of Internal Affairs are considered.

Keywords: information protection; information security; tools; methods; workplace.

Информация, обрабатываемая в органах внутренних дел Российской Федерации, имеет огромную важность в данный момент времени, так как ОВД работают с государственной, служебной тайной, персональными данными и прочей конфиденциальной информацией. Возможность неправомерного доступа к информации обусловливает различного рода источники угроз информационной безопасности.

Этому способствуют следующие факторы:

– многообразие форм несанкционированного (неправомерного, запрещенного) доступа к информации и обращения с нею;

– отсутствие адекватного механизма его предотвращения, выявления, и пресечения;

– рост организованности современной преступности, повышение ее криминального профессионализма и дальнейшее совершенствование технической оснащенности, базирующееся на новейших достижениях научно-технического прогресса.

Поэтому обеспечение защищённости на рабочем месте сотрудника – необходимая часть рабочего процесса.

Защищённость рабочего места обеспечивается следующими способами:

– Разграничение доступа к рабочим местам сотрудников.
– Использование средств антивирусной защиты информации.
– Использование защищенных каналов связи.
– Использование межсетевых экранов.
– Использование средств криптографической защиты информации.

Разграничение доступа к информации – разделение информации, циркулирующей в АС, на части, элементы, компоненты, объекты и т.д. и организация системы работы с информацией, предполагающей доступ пользователей к той части (к тем компонентам) информации, которая им необходима для выполнения своих функциональных обязанностей или необходима исходя из иных соображений.

Средства антивирусной защиты [1] – специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики – предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом. В ОВД в данный момент используется Антивирус Касперского.

Защищенные каналы связи – это такие каналы связи, которые выполняют три основных принципа [3]:

Доверие (Trust) – взаимная аутентификация абонентов при установлении соединения.

Шифрование (Encryption) – защита передаваемых по каналу сообщений от несанкционированного доступа. То есть, говорить и слушать во время диалога можете только вы и ваш собеседник.

Обеспечение целостности (Data Integrity) – подтверждение целостности поступающих по каналу сообщений, т.е. сообщения не могут подвергаться полной или частичной замене информации.

В ОВД в данный момент используется VipNet.

Межсетевой экран [2] – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

Средство криптографической защиты информации (СКЗИ) [2] – это программа или устройство, которое шифрует документы и генерирует электронную подпись (ЭП). Все операции производятся с помощью ключа электронной подписи, который невозможно подобрать вручную, так как он представляет собой сложный набор символов. В данный момент в ОВД используется КриптоПРО.

Таким образом, существуют различные средства и методы, позволяющие обеспечить информационную безопасность рабочего места сотрудника ОВД. Разнообразие видов используемой информации, целей защиты, вариантов угроз, применяемых технологий защиты определяют широкую номенклатуру таких средств и методов. В каждом случае необходимости защиты информации выбирается свой конкретный тип средства.

СПИСОК ЛИТЕРАТУРЫ

1. Информационная безопасность: основы правовой и технической защиты информации: учебное пособие / В.А. Мазуров, А.В. Головин, В.В. Поляков. – Барнаул: Изд-во Алт. ун-та, 2005. – 196 с.
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 168 с.
3. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. – М.: ГЛТ, 2016. – 58 с.

УДК 004.056.5

СРЕДСТВА КРИПТОЗАЩИТЫ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Примакин Алексей Иванович, Горбунова Дарина Алексеевна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: primakin@mail.ru, darin.gorbunova@yandex.ru

Аннотация. Рассматривается вопрос защиты персональных данных в информационных системах средствами криптографической защиты, нормативные документы в сфере защиты информации, виды и способы шифрования.

Ключевые слова: средства криптографической защиты информации; персональные данные; информационные системы; шифрование; криптография; алгоритм.

CRYPTO PROTECTION MEANS IN INFORMATION SYSTEMS OF PERSONAL DATA

Primakin Alexey, Gorbunova Darina
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: primakin@mail.ru, darin.gorbunova@yandex.ru

Abstract. The issue of protection of personal data in information systems by means of cryptographic protection, regulatory documents in the field of information protection, types and methods of encryption are considered.

Keywords: means of cryptographic information protection; personal data; Information Systems; encryption; cryptography; algorithm.

В мире информационных технологий информация является основным ресурсом, который приобретает первостепенную значимость. Поэтому вопрос обеспечения ее безопасности является актуальным на сегодняшний день. Особое внимание стоит уделить к защите информации ограниченного доступа, именно к такой категории относятся персональные данные. Важное место в обеспечении безопасности отводится средствам криптографической защиты информации (СКЗИ). Поскольку передача персональных данных может осуществляться по незащищенному каналу связи, сюда входит, например, удаленная работа сотрудников с базой данных, обмен информацией между территориальными органами. В том или ином виде подобные задачи присутствуют практически в каждом государственном органе.

Первоначально письменность сама защищала себя, поскольку ей могли пользоваться немногие. С течением времени появилась необходимость сохранения информации от несанкционированного доступа (НСД).

Обеспечивать сохранность сведений начинают шифры, проводимые над текстом действия по искажению «исходного текста» и превращению информации в нечитабельный вид. Появляются симметричные и ассиметричные шифры. Примером симметричного является шифр Цезаря, он заключается в замене букв открытого сообщения на иные, отличающиеся от исходных на некоторое число (ключ). Ассиметричные шифры являются сложными, поэтому получили большее распространение и используются в настоящее время [1].

Сегодня СКЗИ – это аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие индивидуальные действия по защите информации, в основном, шифрование, которое используется при защите персональных данных, сохранении конфиденциальной информации [2].

Информационная система персональные данные содержит информацию о сотрудниках или гражданах, которая в соответствии с 152-ФЗ «О персональных данных» должна быть защищена [3].

Цель исследования – повышение эффективности защиты персональных данных сотрудников ОВД в информационных системах посредством применения средств криптозащиты.

Для достижения поставленной цели необходимо решить ряд задач:

– провести анализ нормативно-правовой основы криптографической защиты персональных данных;

– провести анализ применения СКЗИ для защиты персональных данных;

– обосновать и разработать методику применения СКЗИ для защиты персональных данных в информационных системах, используемых в ОВД.

Объект исследования – криптографические алгоритмы и средства защиты информации.

Предмет исследования – средства криптографической защиты, применяемые в информационных системах относительно персональных данных.

СПИСОК ЛИТЕРАТУРЫ

1. Бутакова Н.Г. Криптографические методы и средства защиты информации: учеб. пособие /Н.Г. Бутакова, Н.В. Федоров. – СПб.: ИЦ «Интермедия», 2019. – 384 с.
2. Баранов А.С. Использование средств криптографической защиты информации в организациях // МНИЖ. 2020. № 6-1 (96). [Электронный ресурс] URL: https://cyberleninka.ru/article/n/ispolzovanie-sredstv-kriptograficheskoy-zaschity-informatsii-v-organizatsiyah (дата обращения: 27.07.2021).
3. Хачатурова С.С. Персональные данные под защиту! / С.С. Хачатурова// Международный журнал прикладных и фундаментальных исследований, 2016. № 5-4. – С. 666-668.

УДК 004.056.5

ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ МВД РОССИИ

Примакин Алексей Иванович, Кузнецова Виктория Романовна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: primakin@mail.ru, vkuznetcova@mail.ru

Аннотация. Рассматривается вопрос защиты персональных данных, обрабатываемых в автоматизированных системах МВД России.

Ключевые слова: защита; персональные данные; автоматизированные системы; система защиты персональных данных.

ORGANIZATION OF PERSONAL DATA PROTECTION IN AUTOMATED SYSTEMS OF THE MINISTRY OF INTERNAL AFFAIRS OF THE RUSSIAN

Primakin Alexey, Kuznetsova Viktoria
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: primakin@mail.ru, vkuznetcova@mail.ru

Abstract. The question of the protection of personal data processed in the automated systems of the Ministry of Internal Affairs of Russia is considered.

Keywords: protection; personal data; automated systems; personal data protection system.

Персональные данные (ПДн) в последние годы обретают все большую важность, поэтому они нуждается в защите. Персональные данные, обрабатываемые в автоматизированных системах органов внутренних дел, являются конфиденциальными, поэтому подлежат защите от несанкционированного доступа [1].

В целях обеспечения реализации требований законодательства Российской Федерации в области защиты ПДн при их обработке в органах внутренних дел необходимо создание соответствующей системы защиты ПДн (СЗПДн). Такая система призвана обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в информационных системах (ИСПДн) территориальных органов МВД России [2].

СЗПДн представляет собой совокупность органов, исполнителей и используемой ими техники защиты информации, а также объектов защиты информации. Она организуется и функционирует по правилам и нормам, установленным соответствующими, документами в области защиты информации.

СЗПДн представляет собой совокупности органов, исполнителей и используемой ими техники защиты информации, а также объектов защиты информации. Она организуется и функционирует по правилам и нормам, установленным соответствующими, документами в области защиты информации.

Таким образом, с учетом вышеизложенного, можно определить, что система защиты ПДн в органах внутренних дел состоит из следующих элементов: персональные данные и носители таких данных; должностные лица, подразделения и сотрудники, ответственные за организацию и проведение работ по защите ПДн; способы, техника и средства защиты: ПДн; меры и мероприятия, проводимые в целях защиты ПДн.

Проведем краткий анализ каждого элемента [3]:

1. Персональные данные и носители таких данных.

Персональные данные (данные о гражданах, подлежащие внесению в банки данных), обрабатываемые в органах внутренних дел, определены в ч. 3 ст. 17 ФЗ №3 «О полиции».

Помимо них в различных подразделениях и службах органов внутренних дел (медицинские учреждения, кадровые, финансово-экономические, тыловые подразделения) обрабатываются ПДн сотрудников, федеральных государственных служащих, работников, стажеров системы МВД России, а также членов их семей.

В органах внутренних дел обрабатываются ПДн, которые являются государственной тайной. Защита данной категории ПДн осуществляется в соответствии с нормами и правилами, установленными для сведений, составляющих государственную тайну.

В соответствии с ГОСТ Р 509222006 «Защита информации. Основные термины и определения» носителями защищаемой информации являются физические лица или материальные объекты (бумажные, магнитные, оптические и др.), в том числе – физические поля (акустическое, электромагнитное и др.), где информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

2. Должностные лица, подразделения и сотрудники, ответственные за организацию и проведение работ по защите ПДн.

В соответствии требованиями приказа МВД России руководители (начальники) территориальных органов МВД России, руководители структурных подразделений территориальных органов МВД России, эксплуатирующие ИСПДн, обеспечивают выполнение правовых, организационных и технических мер, направленных на обеспечение безопасности ПДн, и являются ответственными за соблюдение требований по защите ПДн при их автоматизированной обработке в подчиненном органе внутренних дел.

Кроме указанных выше должностных лиц ответственными за соблюдение требований по защите ПДн являются администраторы ИСПДн, пользователи, непосредственно обрабатывающие ПДн в ИСПДн, инженерно-технический персонал, имеющий доступ к элементам ИСПДы.

3. Способы, методы, техника и средства защиты ПДн.

К способам и методам защиты персональных данных в ИСПДн органов внутренних дел относится следующие:

– способы и методы защиты ПДн, обрабатываемой техническими средствами информационной системы, от несанкционированного доступа к ПД, а также иных несанкционированных действий;

– способы и методы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к ПДн.

4. Меры и мероприятия, проводимые в целях защиты ПДн.

В настоящее время порядок организации защиты ПДн, содержащихся в информационной системе персональных данных органов внутренних дел, установлен приказами ФСТЭК России и МВД России [4].

В целях обеспечения безопасности ПДн в органах внутренних дел создается система их защиты, призванная обеспечивать их конфиденциальность, целостность и доступность ПДн при их обработке в ИСПДн.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ // СЗ РФ. 2006. № 31 Ст. 3448. Ч. 1
2. Лебедев, В.Н. Система технической защиты персональных данных в органах внутренних дел Российской Федерации: основные положения и элементы Труды Академии управления МВД России. – 2014. – № 1 (29). – С. 38-41.
3. Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации: приказ МВД России от 6 июля 2012г. № 678.
4. Баглай, М.В. Конституционное право Российской Федерации. М., 2011.

УДК 004.031.6

АВТОМАТИЗАЦИЯ ПРОЦЕССА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОНТРОЛИРУЕМОЙ ЗОНЫ ТЕРРИТОРИАЛЬНОГО ОРГАНА МВД РОССИИ

Родин Владимир Николаевич, Карпова Мария Александровна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: vl.rodin@mail.ru, karpova_1505@mail.ru

Аннотация. В статье рассматривается проблема автоматизации процесса обеспечения безопасности контролируемой зоны территориального органа МВД России, актуальность и цель данного процесса, а также объект и предмет исследования.

Ключевые слова: контролируемая зона; безопасность контролируемой зоны; обеспечение безопасности; автоматизация процесса обеспечения безопасности; проектирование систем и средств защиты контролируемой зоны.

AUTOMATION OF THE PROCESS OF ENSURING THE SECURITY OF THE CONTROLLED ZONE OF THE TERRITORIAL BODY OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Rodin Vladimir, Karpova Maria
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: vl.rodin@mail.ru, karpova_1505@mail.ru

Abstract. The article discusses the problem of automating the process of ensuring the security of the controlled zone of the territorial body of the Ministry of Internal Affairs of Russia, the relevance and purpose of this process, as well as the object and subject of research.

Keywords: controlled area, safety of controlled area; security; automation of the process of ensuring security; design of systems and means of protection of the controlled area.

Каждый территориальный орган МВД России имеет свою контролируемую зону – территорию, в которой исключено неконтролируемое пребывание сотрудников и иных граждан, а также транспортных средств, технических и иных материальных средств. От безопасности контролируемой зоны во многом зависит работа отдела и всего Министерства в целом, ведь ее нарушение злоумышленником может привести к непоправимым последствиям.

Актуальность данной проблемы обусловлена тем, что территория каждого территориального органа МВД России имеет различную конфигурацию и оборудованы техническими средствами безопасности по-разному, следовательно, и контролируемые зоны у всех различные по структуре и содержанию. Важно учитывать особенности устройства каждого отдела. Также в связи с развитием информационных технологий появляются все новые и новые устройства и системы, которые в свою очередь увеличивают и количество уязвимостей в системе безопасности территориального органа МВД России, от которых необходимо избавиться либо взять под контроль техническими средствами [1].

Главной целью автоматизации процесса обеспечения безопасности контролируемой зоны является повышение уровня безопасности, упрощение работы системы охраны контролируемой зоны и увеличение ее эффективности посредством поиска необходимых средств защиты и разработки программного обеспечения для их совместного использования [2]. Объект исследования в данном случае – процесс обеспечения безопасности контролируемой зоны территориального органа МВД России, а предмет – автоматизация этого процесса.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ нормативно-правовых актов об обеспечении безопасности территориальных органов МВД России [1].

2. Проанализировать имеющуюся систему защиты контролируемой зоны территориального органа МВД России и определить уязвимости в ней [3].

3. Рассмотреть возможные способы и методы ее улучшения, учитывая при этом их эффективность и целесообразность использования [4].

4. Предложить систему построения контролируемой зоны в части применения технических средств безопасности для территориального органа МВД России.

4. Разработать программу для автоматизации всего процесса обеспечения безопасности контролируемой зоны территориального органа.

Выполнение поставленной задачи предполагает формирование комплексного подхода для создания системы безопасности в целом для объекта и в частности для контролируемой зоны территориального органа МВД России. Результатом исследовательской работы будет предложен процесс автоматизации безопасности контролируемой зоны типового территориального органа МВД России.

СПИСОК ЛИТЕРАТУРЫ

1. ФЗ от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями на 2 июля 2021 года).
2. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования.
3. Приказ ФСТЭК России № 21 от 18 февраля 2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями на 14 мая 2020 года).
4. Приказ МВД России от 31.12.2014 №1152 «Об утверждении Инструкции по обеспечению инженерно-технической укрепленности и повышению уровня антитеррористической защищенности объектов органов внутренних дел Российской Федерации от преступных посягательств».

УДК 004.031.6

СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРОЕКТИРУЕМОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ТЕРРИТОРИАЛЬНОГО ОРГАНА МВД РОССИИ

Родин Владимир Николаевич, Крылова Арина Евгеньевна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: vl.rodin@mail.ru, rinka-99@mail.com

Аннотация. Рассматривается проблема создания системы защиты информации. Актуальность и цель создания системы защиты информации территориального органа МВД России. Объект и предмет защиты.

Ключевые слова: информационная система; защита информации; информационная безопасность; система информационной безопасности; проектирование систем и средств защиты информации.

CREATION OF THE INFORMATION PROTECTION SYSTEM OF THE PROJECTED INFORMATION SYSTEM OF THE TERRITORIAL BODY OF THE MINISTRY OF INTERNAL AFFAIRS OF RUSSIA

Rodin Vladimir, Krylova Arina
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: vl.rodin@mail.ru, rinka-99@mail.com

Abstract. The article deals with the problem of creating an information security system. The relevance and purpose of creating an information protection system of the territorial body of the Ministry of Internal Affairs of Russia. The object and subject of protection.

Keywords: information system; information protection; information security; information security system; design of systems and means of information protection.

Информация, обрабатываемая в органах внутренних дел Российской Федерации, имеет огромное значение и важность как для силовых структур России, так и для граждан нашей страны, ведь сотрудники МВД России работают с государственной и служебной тайнами, персональными данными и прочей конфиденциальной информацией, поэтому необходимость защиты информации при создании информационной системы является приоритетной задачей [1].

Целью создания системы защиты информации территориального органа МВД России является, повышение эффективности и надежности проектируемой информационной системы территориального органа МВД России, посредством разработки методики создания СЗИ.

Объект защиты – информационная система территориального органа МВД России

Предмет защиты – системы защиты информации в информационных системах территориального органа МВД России.

Для достижения оставленной цели необходимо решить следующие задачи [2]:

1) Провести анализ предметной области (информационной системы территориального органа МВД России).

2) Провести анализ систем защиты информации в информационных системах территориальных органов МВД России).

3) Разработать методику создания системы защиты информации для информационной системы типового территориального органа МВД России.

Стадии создания системы защиты информации предполагают [3]:

1) Формирование требований к защите информации, содержащейся в информационной системе территориального органа МВД России.

2) Разработка системы защиты информации информационной системы территориального органа МВД России:

– предпроектная стадия, включающая предпроектное обследование информационной системы, разработку аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание;

– стадия проектирования (разработка проекта), включающая разработку СЗИ информационной системы территориального органа МВД России.

3) Стадия ввода в действие СЗИ, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию информационной системы территориального органа МВД России на соответствие требованиям безопасности информации.

Система защиты информации информационной системы не должна препятствовать достижению целей создания информационной системы и ее функционированию.

При разработке системы защиты информации информационной системы учитывается ее информационное взаимодействие с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также применение вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

При проектировании системы защиты информации информационной системы [4]:

– определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты;

– определяются методы управления доступом, типы доступа и правила разграничения доступа субъектов доступа к объектам доступа, подлежащие реализации в информационной системе;

– выбираются меры защиты информации, подлежащие реализации в системе защиты информации информационной системы;

– определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

– определяется структура системы защиты информации информационной системы, включая состав (количество) и места размещения ее элементов;

– осуществляется выбор средств защиты информации;

– определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации;

– определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

Создание Концепции обеспечения информационной безопасности обычно предшествует техническому проектированию системы обеспечения информационной безопасности. Целью создания Концепции является определение основных целей и задач, а также общей стратегии построения системы обеспечения информационной безопасности, выработка требований и базовых подходов к их реализации [5].

Концепция информационной безопасности организации определяет состав критичных информационных ресурсов и основные принципы их защиты. Принципы обеспечения ИБ обуславливают необходимость применения определенных методов и технологий защиты. Определение способов реализации этих принципов путем применения конкретных программно-технических средств защиты и системы организационных мероприятий является предметом конкретных проектов и политик безопасности, разрабатываемых на основе Концепции.

Концепция должна пересматриваться по мере выявления новых методов и технологий осуществления атак на информационные ресурсы. Подобный пересмотр также должен производиться по мере развития информационных систем организации.

Техническое проектирование систем обеспечения информационной безопасности является необходимым условием для реализации комплексного подхода к обеспечению ИБ. В отсутствии технического проекта возможно лишь реализация фрагментарных мер и механизмов безопасности, за счет которых в современных условиях невозможно решение основных вопросов обеспечения информационной безопасности.

Технический проект системы обеспечения информационной безопасности включает в себя:

– пояснительную записку, содержащую описание основных технических решений по созданию СОИБ и организационных мероприятий по подготовке СОИБ к вводу в действие;

– спецификацию на комплекс технических средств СОИБ;

– спецификацию на комплекс программных средств СОИБ.

Разработка технического проекта, осуществляется на основе согласованного с заказчиком Технического задания, а также существующей Концепции обеспечения информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (с изменениями и дополнениями).
2. ГОСТ Р ИСО/МЭК 21827-2010 Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости проекта.
3. Приказ ФСТЭК России от 11.02.2013 № 17. «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
4. Информационная безопасность: основы правовой и технической защиты информации: учебное пособие / В.А. Мазуров, А.В. Головин, В.В. Поляков. – Барнаул: Изд-во Алт. ун-та, 2005. – 196 с.
5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 168 с.

УДК 004.04

СОВЕРШЕНСТВОВАНИЕ МЕТОДИКИ ПОИСКА, СБОРА, ИССЛЕДОВАНИЯ И ЭКСПЕРТНОЙ ОЦЕНКИ ОБНАРУЖЕННОЙ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ КОМПЬЮТЕРНОЙ ЭКСПЕРТИЗЫ (ЭКСПЕРТИЗЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ)

Родин Владимир Николаевич, Маричева Евгения Владимировна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: vl.rodin@mail.ru, marichevazhenya@gmail.com

Аннотация. В тезисах рассматривается один из видов судебной экспертизы – компьютерно-техническая экспертиза, ее актуальность, задачи, цели, объекты исследования и виды. Данный вид экспертиз имеет высокую значимость в настоящее время, поскольку сейчас практически все сферы жизнедеятельности компьютеризированы.

Ключевые слова: судебная экспертиза; компьютерно-техническая экспертиза; эксперт; исследование системного блока; исследование носителей компьютерной информации.

IMPROVEMENT OF THE METHODS OF SEARCH, COLLECTION, RESEARCH AND EXPERT EVALUATION OF THE DETECTED INFORMATION DURING THE COMPUTER EXAMINATION (EXAMINATION OF COMPUTER INFORMATION)

Rodin Vladimir, Maricheva Eugenia
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: vl.rodin@mail.ru, marichevazhenya@gmail.com

Abstract. The theses consider one of the types of forensic examination – computer-technical expertise, its relevance, tasks, goals, objects of research and types. This type of expertise is of high importance at the present time, since now almost all spheres of life are computerized.

Keywords: forensic examination; computer-technical expertise; expert; study of the system unit; study of computer information carriers.

Современное российское общество характеризуется интенсивным развитием и стремительным внедрением информационных технологий во все сферы жизнедеятельности человека. Глобальное информационное сообщество с разветвленной информационно-телекоммуникационной системой сейчас практически полностью сформировано. Одним из негативных последствий процесса компьютеризации общества является появление так называемая компьютерная преступность. Борьба с компьютерными преступлениями для современного общества, насыщенного компьютерными технологиями, стала одной из приоритетных задач. Что касается конкретного объекта этих преступлений, возникает необходимость обращения к специалистам, обладающим знаниями в информационной сфере.

Компьютерно-техническая экспертиза является инженерно-технической экспертизой и относится к судебным экспертизам. Она позволяет комплексно выстроить систему доказательств, благодаря тому, что эксперт в процессе ее проведения решает задачи поиска, сбора, исследования и экспертной оценки обнаруженной информации [1].

Перед экспертом в процессе проведения компьютерно-технической экспертизы стоят следующие задачи:

- определить свойства, характеристики и качества компьютерных систем;
- установить особенности разработки и использования программных продуктов;
- установить факты использования определенного оборудования;
- получить доступ к информации на носителях;
- исследовать информацию, созданную пользователем или программой;
- установить особенности функционирования компьютерных средств, реализующих сетевую информационную технологию.

Объектами информационного исследования при проведении компьютерно-технических экспертиз и исследований, являются:

- накопители данных на магнитных дисках: дискеты, НЖМД;
- накопители данных на оптических дисках форматов CD, DVD;
- накопители данных на магнитооптических дисках;
- постоянные запоминающие устройства флеш-памяти: USB, SD;
- ЭВМ – персональные компьютеры, сервера, системы хранения данных;
- портативные компьютеры, а также ноутбуки, планшеты, смартфоны;
- сетевые устройства – модемы, маршрутизаторы, точки доступа, межсетевые экраны;
- компоненты ЭВМ;
- программное обеспечение;
- информационные объекты – базы данных, файлы и их служебная информация, содержимое файлов [2].

В связи с тем, что исследуются разные данные, просмотр и изучение информационного содержимого дает различные результаты. Анализ всего объема полученной информации позволяет выявлять следы программ и приложений, определять транзакции, проводимые через информационные сети, а также отслеживать действия и намерения пользователя компьютера из файлов, сохраненных или удаленных им на персональном компьютере.

Работа с информацией требует глубоких знаний в области информационных технологий и компьютерных методов хранения данных, так как содержимое устройств хранения информации должно быть сначала обнаружено и извлечено, то есть переведено в формат, доступный для восприятия специалистами. Опыт сотрудника, выполняющего компьютерно-техническую экспертизу, а также уровень его профессиональной компетенции играют решающую роль в получении полного и достоверного исследования и достижения целей, преследуемых инициатором анализа.

В уголовном производстве по объектам данного вида экспертизы отражены в следующем методическом подходе, который отражает сущность современной компьютерно-технической экспертизы. Исследование системного блока персонального компьютера проводится путем:

– визуального осмотра внутренних аппаратных компонентов системного блока;
– извлечения из системного блока жесткого диска;
– подключения к системному блоку монитора, клавиатуры и манипулятора «мышь» и прерывания его загрузки для определения установок программы SETUP BIOS;
– загрузки операционной системы с системной дискеты эксперта и диагностирования соответствующими программными средствами аппаратных компонентов системного блока (все выполняется без жесткого диска).

Исследование носителей компьютерной информации проводится путем:

– определения класса носителя;
– определения интерфейса, состояния перемычек и переключателей (для НЖМД);
– подключения к стендовому компьютеру исследуемого жесткого диска;
– определения основных технических параметров;
– выявления таблицы разделов диска с определением их основных характеристик (начало и конец раздела, тип файловой системы, идентификаторы и метки разделов, размер и количество кластеров);
– определения логической адресации системных областей разделов (загрузочной записи, таблиц FAT и корневого каталога).

Поиск признаков выполнения несанкционированных действий или использования специальных программ удаленного администрирования производится путем:

– поиска программ, предназначенных для подбора паролей, и результатов их работы;
– поиска фактов работы с использованием чужих учетных записей или других системных ресурсов;
– установления содержимого текстовых файлов и файлов электронной почты;
– выявления текстовых файлов, содержащих ключевые слова;
– выявления пользовательских файлов, имеющих обстоятельствам дела;
– исследования защищенных паролями файлов;
– сравнительного исследования нескольких версий программ, конфигурационных файлов (настроек) и файлов данных;
– изучения протоколов работы пользователя (или программ) и интерпретации их действий [3].

Эксперт в области компьютерно-технической экспертизы должен обладать специальными знаниями в области информационных систем и процессов, программировании, электротехники, радиотехники. Наличие таких системных знаний позволит специалисту провести качественную экспертизу. Хотя внешне алгоритм компьютерно-технической экспертизы сводится к поиску определенной информации, ее анализу и фиксированию в заключение, кроме того, необходимо обладать лабораторией для проведения компьютерно-технической экспертизы.

Современный методический и организационный уровень компьютерно-технических экспертиз характеризуется как этап становления нового рода судебной экспертизы. В связи с этим большинство экспертных задач могут решаться пока при разработке специальных экспертных методик для каждого частного случая. Причем, в каждой конкретной ситуации рекомендуется предварительно согласовать возможность проведения необходимого исследования, а также круг задач и вопросов, ставящихся на разрешение эксперта.

СПИСОК ЛИТЕРАТУРЫ

1. Баюш. А.А. Судебная компьютерно-техническая экспертиза в системе судебных экспертиз // Политехнический молодежный журнал № 8(37), 2019. – С. 18-26.
2. Антилова Е.С., Хаснутдинов Р.Р. Некоторые особенности судебной информационно-компьютерной экспертизы // Modern science, 2020. – С. 239-242.
3. Компьютерно-техническая экспертиза // [Электронный ресурс]. Режим доступа: http://dagsudexpert.ru/pages/Kompyuterno-tehnicheskaya-ekspertiza/ Дата обращения: 28.07.2021.

УДК 004.056.5

СПОСОБЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, ПЕРЕДАВАЕМОЙ ПО ТЕХНИЧЕСКИМ КАНАЛАМ СВЯЗИ

Саратов Дмитрий Николаевич, Гизатулин Сергей Алексеевич
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: saratovdn@mail.ru, kingblood99@gmail.com

Аннотация. Рассматриваются способы защиты конфиденциальной информации, не составляющей государственную тайну, передаваемой по техническим каналам связи.

Ключевые слова: конфиденциальная информация, не составляющая государственную тайну; технические каналы связи.

METHODS OF PROTECTING CONFIDENTIAL INFORMATION THAT DOES NOT CONSTITUTE A STATE SECRET TRANSMITTED THROUGH TECHNICAL COMMUNICATION CHANNELS

Saratov Dmitry, Gizatulin Sergey
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: saratovdn@mail.ru, kingblood99@gmail.com

Abstract. The methods of protecting confidential information that does not constitute a state secret; transmitted through technical communication channels, are considered.

Keywords: confidential information that does not constitute a state secret; technical communication channels.

В современных условиях развития общества усиливается роль информации в различных сферах жизни и деятельности человека. Сейчас информационная сфера, представляет собой системообразующий фактор современного общества, который сильно влияет на разные характеристики в экономической, оборонной, политической и других компонентов безопасности государств.

Требования по формированию надежной защиты информации определяют характеристики криптографических средств, предназначенных для защиты информации, которые содержат специальные методы и средства преобразования информации, в результате которых маскируется ее содержание.

Эта защита может проходить [1]:

1. Для осуществления защиты информации, когда проходит передача единичных сообщений (пакетов), которые могут подвергнуться как пассивным, так и активным вторжениям.

2. С целью формирования защиты, а также секретности операций, которые делают над сообщениями при осуществлении передачи по вычислительной сети необходимо проводить анализ объектов вторжений.

Существуют ситуации, когда целостность системы, применяющей защиту на основе криптографического подхода, может иметь риск подвергнуться опасности вторжения, в том случае, когда произошло разрушение криптографической системы. Существуют также случаи, при которых криптографическая система, применяемая для того, чтобы была конфиденциальность, ведет также к адекватной защите целостности сообщений.

Многие методы подтверждения подлинности получаемых зашифрованных сообщений должны применять какую-то избыточность для текста исходного сообщения.

Избыточность достигается на разных уровнях протокола в вычислительной сети: например, на канальном она применяется для контроля ошибок, на физическом (в том случае, если применяется шифрование) используется для осуществления проверки со стороны получателя. Так как такая проверка может рассматриваться как часть протокола передачи данных, то это ведет к тому, что прикладной процесс не связан необходимостью проверки избыточности.

Интересно отметить, что чем больше избыточность исходного текста, тем легче получателю осуществить проверку подлинности сообщения и тем сложнее для нарушителя провести модификацию сообщения.

Осуществление защиты содержимого сообщений может быть достигнуто шифрованием. Чтобы создать необходимую гибкость и скорость, необходимо использовать симметричные криптографические системы.

Достаточно распространенным методом борьбы с индустриальными помехами может быть применение магнитных антенн. Это связано с тем, что все промышленные и индустриальные помехи имеют, в основном, электрический, а не магнитный характер [2].

Вывод. Каналы связи представляют собой один из видов компонентов ИС, которые могут подвергнуться нападению злоумышленников. Среди них можно отметить большое число мест, которые потенциально опасны, через них злоумышленники имеют возможности проникновения в ИС.

СПИСОК ЛИТЕРАТУРЫ

1. Фучко М.М., Широких А.В., Захаров А.А., Несговоров Е.С., Оленников Е.А. Аудиовыход как скрытый канал утечки данных: технологии создания и методы защиты // Вестн. УрФО. Безопасность в информационной сфере. 2016. № 3(21).
2. Свиридов В.И. Вопросы защиты информации при передаче по каналам связи // Современные наукоемкие технологии. – 2014. – № 5-2. – С. 58-58; URL: http://top-technologies.ru/ru/article/view?id=33938 (дата обращения: 03.08.2021).

УДК 004.624

РАСКРЫТИЕ ИНФОРМАЦИИ О КУРСАНТАХ В ИНТЕРЕНЕТЕ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Чудаков Олег Евгеньевич, Прогин Павел Михайлович
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: oechuda@yandex.ru, proga017@mail.ru

Аннотация. Рассматривается проблема раскрытия информации о курсантах в сети Интернет. Актуальность информационной безопасности органов внутренних дел. Разработка комплекса мер по недопущению раскрытия курсантами своих данных в сети Интернет.

Ключевые слова: информационная безопасность; курсанты; раскрытие данных.

DISCLOSURE ABOUT COURSANTS ON THE INTERNET AND INFORMATION SECURITY OF THE INTERNAL AFFAIRS

Chudakov Oleg, Progin Pavel
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: oechuda@yandex.ru, proga017@mail.ru

Abstract. The article deals with the problem of disclosure of information about cadets on the Internet. The relevance of information security of internal affairs bodies. Development of a set of measures to prevent cadets from disclosing their data on the Internet.

Keywords: information security; cadets; data disclosure.

Информационная безопасность признается важнейшим компонентом, интересом в сфере национальной безопасности. В Стратегии национальной безопасности Российской Федерации обеспечение информационной безопасности закреплено в качестве одного из приоритетных направлений деятельности государства, правоохранительных органов [1].

Актуальность такого обеспечения связана с несколькими факторами, а именно:

1). Содержание информационных массивов ОВД. На сегодняшний день в ОВД скапливается существенное количество самой разнообразной информации, часть из которой носит специальные грифы секретности, относятся к разряду государственной тайны.

2). Последствия несанкционированного доступа к информационным массивам ОВД. Как показывает практика, несанкционированный доступ к сведениям, формируемым в ходе работы ОВД чреваты такими последствиями, как совершение тяжких преступлений, затруднение работы сотрудников ОВД и так далее.

Отдельно следует упомянуть о проблеме раскрытия информации о сотрудниках ОВД. Проходя службу в ОВД, все без исключения сотрудники выступают в роли специальных субъектов обеспечения информационной безопасности. Понимание их статуса нужно производить, исходя из двух основополагающих составляющих [2].

Первая – сотрудники ОВД, как субъекты обладания специальными сведениями, данными, информацией, разглашение которой может повлечь к последствиям, указанным выше.

Вторая – сотрудники ОВД, как субъекты, принадлежность которых к ОВД, факт прохождения службы в системе ОВД сам по себе является информацией ограниченного пользования.

Именно вторая составляющая приобретает существенную актуальность для некоторых категорий сотрудников ОВД, прежде всего, курсантов образовательных учреждений системы МВД России. Раскрытие данных о курсантах в информационно-телекоммуникационной сети Интернет – это существенная угроза информационной безопасности ОВД.

Особая актуальность именно для курсантов в данном случае связана со следующими факторами:

1. Вовлеченность курсантов в сеть Интернет. Как показывает практика, именно курсанты – самая распространенная по использованию различных интернет-сервисов социальная группа сотрудников ОВД.

2. Особенности личности курсантов. Будучи людьми достаточно молодого возраста, с часто недостаточным опытом, курсанты самостоятельно раскрывают свои данные в интернете, как о принадлежности к ОВД, так и о своих персональных данных (например, месте жительства).

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации»).
2. Белов, М. В. Проблемы информационной безопасности в системе ОВД: личностный аспект / М.В. Белов, Е.И. Аникин // Информационная безопасность регионов. – 2008. – № 2(3). – С. 53-56.

УДК 004.056

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ И РАЗГРАНИЧЕНИЯ ДОСТУПА ЧЕРЕЗ USB-НОСИТЕЛИ

Чудаков Олег Евгеньевич, Ципанович Анастасия Владимировна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: OEchuda@yandex.ru, nastea0797@mail.ru

Аннотация. USB-носители являются одним из наиболее опасных устройств, с помощью которых возможно распространение вирусов, кража конфиденциальной и другой ценной информации. Поэтому проблематика USB-устройств актуальна для информационной безопасности практически любой информационной системы.

Ключевые слова: USB-носители; предотвращение вторжений; разграничение доступа; информационная безопасность.

DEVELOPMENT OF A SOFTWARE PACKAGE FOR INTRUSION PREVENTION AND ACCESS CONTROL VIA USB DEVICES

Chudakov Oleg, Tsipanovich Anastasia
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: OEchuda@yandex.ru, nastea0797@mail.ru

Abstract. USB devices are one of the most dangerous devices that can spread viruses, steal confidential and other valuable information. Therefore, the problem of USB devices is relevant for the information security of almost any information system.

Keywords: USB devices; intrusion prevention; access control; information security.

Развитие информационных технологий в современном мире приводит к росту количества потенциальных угроз информационной безопасности, вследствие чего защита информации приобретает все большее значение.

Согласно 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации» защита информации представляет собой принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модификации, блокирования, распространения, а также от иных неправомерных действий.

Основными критериями обеспечения ИБ являются:

– конфиденциальность информации;
– целостность информации и методов ее обработки;
– доступность информации для авторизованных пользователей [1].

На сегодняшний день большинство инцидентов в области информационной безопасности предприятия связаны с воздействием внутренних угроз (в России доля утечек по вине сотрудников вдвое выше, чем в мире, - более 72%) [2].

Кража ценной информации, различные внедрения в систему предприятия происходят практически постоянно, и связано это как с недостаточной компетентностью сотрудников организации, так и с их злым умыслом.

В 2020 году в РФ количество утечек конфиденциальных данных возросло на 5,6 % (аналогичный показатель в мире снизился на 7,6 %). Данные приведены из отчетов компании InfoWatch – разработчика ПО для защиты информации в бизнесе.

С точки зрения информационной безопасности USB-носители являются одним из наиболее опасных устройств, с помощью которых возможно распространение вирусов, кража конфиденциальной и другой ценной информации. Поэтому проблематика USB-устройств актуальна для информационной безопасности практически любой информационной системы.

Проанализировав различные методы решения проблемы подключения посторонних USB-устройств, выявлено, что каждый способ имеет свои недостатки и необходимо разработать удобную и интуитивно понятную программу для защиты информации от утечек с возможностями аудита действий пользователя и разграничения доступа USB-носителей согласно категории (уровню доступа).

Объектом исследования данной работы является информационная безопасность.

Предмет исследования: защита USB-портов; защита информации от НСД.

Цель работы: разработка и тестирование программного комплекса предотвращения вторжений и разграничения доступа через USB-носители.

Основные задачи, необходимые для реализации выполнения поставленной цели:

1. Анализ основных угроз безопасности информации.
2. Исследование возможных методов решения проблемы подключения посторонних USB-устройств.
3. Создание приложения для настройки доступа USB-носителей к ПК (часть администратора), в котором будут выполняться все необходимые настройки для каждого персонального компьютера:
   – настройка списка разрешенных USB-устройств, разграничение доступа к ним согласно категории;
   – настройка уровня доступа к ПК;
   – контроль за действиями пользователя ПК, связанные с подключением USB-устройств (аудит лог-файла).
4. Создание приложения для разграничения доступа USB-носителей к ПК (часть пользователя), осуществляющее контроль действий пользователя:
   – запрет подключения к компьютеру посторонних USB-устройств;
   – отслеживание действий пользователя ПК, связанных с подключением USB-устройств (ведение лог-файлов);
   – защита созданной программы от попыток закрытия посредством штатных средств ОС.

Среда разработки программного комплекса Microsoft Visual Studio 2015, язык программирования C#.

Для реализации данного проекта были задействованы следующие методы научного исследования:

– опрос ведущих специалистов в области информационных технологий;
– метод сравнения известных решений проблемы подключения посторонних USB-устройств.

При изучении данной темы использовались различные источники: законы и постановления РФ, техническая литература, учебники и справочники, статьи из научных журналов.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.07.2021) «Об информации, информационных технологиях и о защите информации».
2. Казарин О.В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О.В. Казарин, А.С. Забабурин. – Москва: Издательство Юрайт, 2020. – 312 с.
3. Шилдт Герберт. Справочник по C#. – Москва: Издательский дом Вильямс. – 2015. – 752 с.

УДК 004.65

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ SQL-ИНЪЕКЦИЙ

Якушев Денис Игоревич, Вайберт Наталия Антоновна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: d.i.ya@yandex.ru, tasha.vaybert@mail.ru

Аннотация. Рассматривается вопрос защиты информации от SQL-инъекций, выявляются основные причины появления таких уязвимостей, а также сами методы защиты от подобного типа атак.

Ключевые слова: защита; SQL-инъекция, база данных.

METHODS FOR PROTECTING INFORMATION FROM SQL-INJECTIONS

Yakushev Denis, Vaybert Natalia
St. Petersburg University of the Russian Interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: d.i.ya@yandex.ru, tasha.vaybert@mail.ru

Abstract. The issue of protecting information from SQL injections is considered, the main reasons for the appearance of such vulnerabilities are identified, as well as the methods of protection against this type of attacks themselves.

Keywords: protection; SQL-injection, database.

На сегодняшний день многие организации, компании, государственные службы, в том числе и МВД России используют в своей деятельности базы данных и различные веб-приложения. По статистике Positive Technologies, каждое четвертое веб-приложение подвержено критически опасной уязвимости «Внедрение операторов SQL». В результате использования SQL-инъекций в базу данных злоумышленникам удалось получить доступ к клиентским данным (включая имена, адреса и телефоны), доменным именам, FTP-паролям, сведениям о банковском счете (без данных кредитных карт) [1].

SQL-инъекция – это метод (как и другие механизмы веб-атак) для атаки на приложения, управляемые данными [2]. Злоумышленник использует преимущество плохо отфильтрованных или неправильно экранированных символов, встроенных в операторы SQL, при разборе переменных данных из пользовательского ввода. Он вставляет произвольные данные, чаще всего запрос к базе данных, в строку, которая в конечном итоге выполняется базой данных через веб-приложение.

Целью работы является анализ эффективности наиболее распространенных средств защиты от SQL-инъекций.

Поставленная цель требует решения следующих задач:

– изучение особенностей внедрения операторов SQL (SQL-инъекции);
– исследование методов обнаружения аномалий в SQL-запросах к базам данных;
– изучение методов защиты от исследуемого типа атак.

Объектом исследования выступают методы защиты информации от SQL-инъекций.

Предметом работы выступают SQL-запросы, базы данных.

Основными причинами появления уязвимости типа SQL-инъекции являются:

– динамическое построение SQL-запросов;
– некорректная обработка исключений;
– некорректная обработка специальных символов;
– некорректная обработка типов данных;
– небезопасная конфигурация СУБД [3].

В дальнейшем необходимо рассмотреть основные классификацию методов защиты от SQL-инъекций:

– методы защиты, основанные на изменении кода веб-приложения;
– методы защиты без изменения кода веб-приложения.

Первый тип реализуется следующими мерами:

– экранирование специальных символов. Использование функции, экранирующей специальные символы строки, и тем самым изменяя синтаксис SQL-запроса и уменьшая вероятность проведения атаки типа SQL-инъекции;

– явное преобразование типов полей ввода. Примером может служить функция языка PHP CAST («Varchar» AS INT), преобразующая строковый тип в числовой;

– подготавливаемые запросы. Подготавливаемые запросы или параметризованные запросы используются для повышения эффективности, когда один запрос выполняется многократно, а также для повышения безопасности баз данных [4].

Второй тип защиты реализуется посредством использования специальных межсетевых экранов для SQL-серверов, такие как GreenSQL [4].

Таким образом, были выявлены основные причины появления SQL-инъекций, а также методы защиты от подобного рода атак, которые позволяют свести возможность проведения таких атак злоумышленниками к минимуму, что значительно усиливает свойства безопасности информации, циркулирующей в информационной системе.

СПИСОК ЛИТЕРАТУРЫ

1. Positive research. «Актуальные киберугрозы IV квартал 2017 года.» [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-Q4-rus.pdf (дата обращения: 01.08.2021 г.).
2. Учебник по SQL-инъекциям [Электронный ресурс]. Режим доступа: http://kodesource.top/sql/sql-injection/sql-injection.php (дата обращения: 01.08.2021 г.).
3. SQL-инъекции – распространённый метод взлома веб-приложений и сайтов [Электронный ресурс]. Режим доступа: https://web-creator.ru/articles/sql_injection (дата обращения: 01.08.2021 г.).
4. Соколин Д.Д., Тимохович А.С. Методы комплексного обеспечения безопасности SQL-сервера от атак типа SQL-инъекции. // Academy. 2017. 3 (18). – С. 7-9.

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

УДК 004.056

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ХРАНЕНИЯ И ИСПОЛЬЗОВАНИЯ ГРАФИЧЕСКИХ ИЗОБРАЖЕНИЙ WEB-РЕСУРСОВ

Бариков Леонид Николаевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП)
Большая Морская ул., 67, Санкт-Петербург, 190000, Россия
e-mail: lnbarikov@gmail.com

Аннотация. Рассматриваются вопросы обеспечения информационной безопасности хранения и использования графических изображений в процессе функционирования web-ресурсов; предлагаются варианты решения возникающих проблем на этапе разработки конкретного web-ресурса.

Ключевые слова: информационная безопасность изображений; формат WebP; несанкционированная конвертация изображений.

ENSURING THAT WEB IMAGES ARE STORED AND USED SECURE

Barikov Leonid
Saint Petersburg State University of Aerospace Instrumentation (SUAI)
67 Bolshaya Morskaya St, St. Petersburg, 190000, Russia
e-mail: lnbarikov@gmail.com

Abstract. The information security of storing and using graphic images in the course of web resources is being considered; options are offered to address emerging issues during the development phase of a particular web resource.

Keywords: image information security; WebP format; unauthorized conversion of images.

Обеспечение безопасности хранения и использования изображений в процессе функционирования web-ресурса является достаточно сложной задачей, требующей решения большого количества частных задач. Многообразие возникающих проблем и их решение рассмотрим на конкретных примерах.

Одним из самых распространенных web-ресурсов является Internet-магазин, обычно представляющий из себя web-сайт, который позволяет продавцам предоставлять товары или услуги, а покупателям приобретать эти товары или услуги с помощью сети Internet. На страницах Internet-магазина покупателю предоставляется не только общая информация о товарах, но и различная дополнительная информация: изображения, видео-обзоры продукции, информация о доставке и способах оплаты.

Работая с клиентской частью Internet-магазина, покупатель просматривает информацию о товарах и услугах, набирает товары в виртуальную корзину, просматривает итоговую информацию о выбранных товарах, указывает необходимые для оформления покупки данные. Кроме того, покупатель может воспользоваться личным кабинетом для того, чтобы отредактировать свои контактные данные или уточнить информацию и статус осуществлённых заказов.

Администратор Internet-магазина при использовании административного раздела клиентской части работает с информацией о поступивших заказах, осуществляет управление ассортиментом Internet-магазина, редактирует информационные страницы.

Internet-магазин можно разделить на следующие функциональные части [1]:

- информационный интерфейс;
- торговый интерфейс;
- система аутентификации и авторизации;
- административный интерфейс;

Информационный интерфейс представляет собой разделы Internet-магазина, в которых покупателю предоставляется текстовая, графическая и иная информация, не относящаяся непосредственно к конкретным товарам, но способствующая принятию решения о покупке. В информационный интерфейс также входит главная страница web-сайта.

Торговый интерфейс представляет собой каталог товаров, корзину покупателя, страницу оформления заказа. Каталог товаров служит для упорядочивания ассортимента Internet-магазина и обычно представляет собой структуру, в которой каждый товар относится к определённой категории. Такой способ создания связей между

товарами и категориями помогает покупателю легче находить необходимые товара из ассортимента Internet-магазина.

В работе Internet-магазина важно организовать презентацию товара. Для этого используются изображения, видео, тексты. При этом не всегда можно заранее угадать, какие именно форматы или размеры изображений потребуются в будущем. Часто на существующие и загруженные на сервер изображения необходимо добавить новый водяной знак с логотипом Internet-магазина, изменить размер изображений или применить какие-то иные модификаторы.

Одним из вариантов решения этой проблемы является предварительная обработка изображений в фоторедакторе и сохранение всех необходимых версий, форматов и т. д. Однако такой подход полностью перестаёт работать, как только возникает необходимость обновить десятки, сотни или тысячи изображений.

Для решения этой задачи предлагается использовать подход, при котором исходное изображение хранится на сервере Internet-магазина, а все его варианты генерируются по запросу в момент обращения.

Система доставки контента — это географически распределённая система серверов, которая служит буфером между сервером Internet-магазина и конечным пользователем. В системе доставки контента кэшируются изображения, файлы HTML, JavaScript и т. д. В дальнейшем они предоставляются конечном пользователю с географически близкого к нему сервера. Таким образом, нагрузка, связанная с передачей статических данных от сервера Internet-магазина пользователю, переходит к специально оптимизированной сети серверов.

Также система доставки контента участвует при решении задачи оптимизации и обработки изображений. Для каждого изображения, которое используется в Internet-магазине, может одновременно требоваться множество вариантов в различных форматах и размерах. Каждый вариант будет генерироваться по запросу.

Обработка изображения требует вычислительных ресурсов и если совершать такую обработку каждый раз, то в определённый момент сервер Internet-магазина столкнётся с перегрузкой и не сможет обеспечить быстрый отклик. Чтобы избежать такой ситуации, предлагается подход, при котором все сгенерированные изображения будут переданы в кэш системы доставки контента. Это позволит тратить вычислительные ресурсы, требуемые для генерации вариантов изображения, только один раз – в момент первого обращения к варианту. Все дальнейшие запросы будут обработаны системой доставки контента и не потребуют траты вычислительных ресурсов.

Для снижения количества потребляемого сайтом трафика и ускорения загрузки необходимо оптимизировать используемые на сайте изображения. Для этого предлагается все статические изображения, которые добавляются в процессе разработки сайта и позже используются на сервере, заранее обрабатывать в графическом редакторе или сжимать при копировании из ресурсной директории в публичную.

Предлагается использовать подход, который позволяет загружать изображения на сервер, а в процессе эксплуатации сайта получать различные варианты имеющихся исходных изображений. При этом одной из задач является генерация для изображений, загруженных в формате JPEG, вариантов в формате WebP. WebP – это новый формат сжатия изображений, который набирает популярность в сети Internet. Конвертация изображений в этот формат позволяет уменьшить размер изображения на 25–35% без потерь в качестве [2].

Для решения этой задачи предлагается использовать специальный сервер imgproxy, написанный на языке Go и позволяющий очень быстро выполнять необходимую конвертацию [3]. Базовый алгоритм работы заключается в следующем: на web-сайте ссылка на изображение заменяется ссылкой, ведущей на сервер, на котором работает imgproxy. В ссылке содержится URL исходного изображения и параметры, на основе которых следует выполнить конвертацию. Imgproxy выполняет конвертацию и возвращает обработанное изображение.

Для обеспечения всех перечисленных задач решению подлежат две дополнительные задачи:

– так как imgproxy будет обращаться за любым изображением, переданным на обработку, необходимо обеспечить защиту от несанкционированного использования сервиса конвертации;

– конвертация и обработка занимают вычислительные ресурсы, а, следовательно, необходимо обеспечить кеширование результатов, чтобы создание одного варианта происходило только один раз.

Для решения первой задачи предлагается использовать подписи ссылок. Подпись осуществляется через механизм HMAC(SHA256) - код проверки подлинности сообщений, использующий хеш-функции.

Процесс выглядит следующим образом:

– на сервере и клиенте задаются параметры ключа и соли (строка данных, которая передаётся хеш-функции вместе с входным массивом данных для вычисления хеша);

– к ожидаемой сервером ссылке добавляется соль;

– с использованием хеш-функции SHA256 вычисляется HMAC;

– результат кодируется с помощью Base64 (стандарт кодирования двоичных данных при помощи только 64 символов ASCII).

Таким образом, сервер может проверить подпись полученной для обработки ссылки и не обрабатывать несанкционированные ссылки.

В первой части пути будет подпись, а во второй - закодированный в Base64 путь к исходному файлу. Расширение webp сообщает серверу о необходимости произвести конвертацию.

Для решения второй задачи запросы к серверу imgproxy проксируются через nginx, который выступает промежуточным звеном и кеширует ответы от imgproxy. Для проверки работоспособности данной схемы в конфигурацию nginx был включён специфичный для данной задачи заголовок ответа x-nginx-cache (название

может быть любым). Он отображает состояние HIT, при котором на запрос был получен ответ из кеша, или же состояние MISS, при котором запрос был обработан через сервис обработки изображений.

В результате оптимизации программного кода и изображений, а также за счет реализации мер по защите информации (использование криптографических методов, интеграция с защитными сервисами и экранирование входных данных) безопасность хранения и использования изображений в процессе функционирования web-ресурса значительно повышается и доводится до приемлемого уровня.

СПИСОК ЛИТЕРАТУРЫ

1. Кириченко А., Дубовик Е. Динамические сайты на HTML, CSS, JavaScript и Bootstrap. Практика, практика и только практика – СПб.: Наука и Техника, 2018. 272 с.
2. WebP - формат изображений [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/WebP (дата обращения: 25.06.2021).
3. OWASP Top Ten [Электронный ресурс] URL: https://owasp.org/www-project-top-ten/ (дата обращения: 25.06.2021).

УДК 004.056

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ АНАЛИЗА НАСТРОЕНИЙ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНОЙ СЕТИ REDDIT

Браницкий Александр Александрович [1], Шарма Яш[2], Федорченко Елена Владимировна[1]
[1] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: branitskiy@comsec.spb.ru, yash3498@gmail.com, doynikova@comsec.spb.ru

Аннотация. В докладе представлено применение методов машинного обучения в задаче анализа настроений пользователей социальной сети. В качестве исследуемого набора данных выступают посты, собранные из социальной сети Reddit и размеченные как принадлежащие одному из шести типов настроений. Проведены эксперименты, связанные с оценкой таких методов машинного обучения, как машина опорных векторов, классификатор fastText и сверточная нейронная сеть; точность определения корректного класса составила более 80%.

Ключевые слова: анализ настроений; социальные сети; машинное обучение; классификаторы; посты.

APPLYING MACHINE LEARNING METHODS FOR SENTIMENT ANALYSIS OF USERS OF THE SOCIAL NETWORK REDDIT

Branitskiy Alexander[1], Sharma Yash[2], Fedorchenko Elena[1]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[2] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: branitskiy@comsec.spb.ru, yash3498@gmail.com, doynikova@comsec.spb.ru

Abstract. The report presents the application of machine learning methods in the problem of sentiment analysis of the social network users. The analyzed data set is the posts collected from the social network Reddit and marked as belonging to one of six types of sentiments. Experiments related to the evaluation of such machine learning methods as support vector machine, fastText classifier and convolutional neural network were carried out; the precision of determining the correct class was 80%.

Keywords: sentiment analysis; social networks; machine learning; classifiers; posts.

Введение. В настоящее время социальные сети являются одним из наиболее популярных Интернет-сервисов, в котором пользователи могут объединяться в группы и обсуждать интересующие их вопросы. Созданный одним пользователем пост может вызвать множество острых дискуссий и разногласий со стороны других пользователей. В собственных сообщениях и комментариях к посту пользователи выражают мнение, которое зачастую содержит и их эмоциональное настроение. В данном случае социальная сеть Reddit предоставляет такие возможности ее пользователям, а использование интерфейса прикладного программирования Pushshift Reddit Dataset public API позволяет собрать посты и выполнить построение анализируемого набора данных. Применение методов машинного обучения в качестве инструмента анализа данных позволяет избежать ручного задания правил для определения настроения пользователей и предполагает построение моделей, в которых будет выполнена настройка их параметров посредством последовательной обработки записей из набора данных.

Разработка системы, предназначенной для решения поставленной задачи, имеет важное значение, поскольку раннее выявление психоэмоциональных отклонений в поведении человека позволяет вовремя предупредить развитие более серьезных заболеваний. Кроме того, разработанное средство может быть нацелено на дополнительную поддержку в принятии решений экспертами-психологами.

Предлагаемый подход. В предлагаемом подходе можно выделить три этапа. На первом этапе выполняется сбор данных. С этой целью каждому посту присваивается метка, которая характеризует эмоциональное

настроение ее адресанта. В исследуемом наборе данных выделяется шесть классов: норма, депрессия, беспокойство, самовредительство, стресс, злость. На втором этапе выполняется предобработка данных, которая заключается в разбиении текста на отдельные предложения и разбиении предложений на отдельные слова (с назначением каждому слову уникального числового значения). Формат предобработанных данных зависит от типа классификатора, который предназначен для классификации постов. К примеру, для машины опорных векторов строятся целочисленные признаки на основе методов мешка слов и TF-IDF, для сверточной нейронной сети выполняется преобразование каждого слова в соответствующий ему идентификатор, для классификатора fastText [1] подразумевается предобработка исходного текста внутри самого классификатора. Третий этап характеризуется настройкой классификаторов машинного обучения. Данный этап является наиболее ресурсоемким как в терминах времени, так и в терминах задействования процессорной мощности машины.

Эксперименты. Экспериментальный набор данных содержит 129748 записей. При проведении экспериментов для создания сбалансированных выборок использовался метод SMOTE (Synthetic Minority Oversampling Technique) [2]. Наилучшие результаты были получены с использованием комбинирования классификаторов, построенных на основе линейной машины опорных векторов по принципу one-vs-rest [3]: точность 80%, полнота 81%, F-мера 80% и достоверность 80%.

Заключение. В докладе был рассмотрен подход к определению настроений пользователей социальной сети. В качестве классификаторов экспериментально были исследованы три типа классификаторов: машина опорных векторов, классификатор fastText и сверточная нейронная сеть. Направление дальнейших исследований может быть связано с использованием классификатора BERT, а также с расширением набора классов, характеризующих настроения пользователей социальной сети.

Работа выполнена при финансовой поддержке РФФИ (проект 18-29-22034 мк).

СПИСОК ЛИТЕРАТУРЫ

1. Joulin A., Grave E., Bojanowski P., Mikolov T. Bag of tricks for efficient text classification // arXiv preprint arXiv:1607.01759. 2016.
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. Pp. 321-357.
3. Galar M., Fernández A., Barrenechea E., Bustince H, Herrera F. An overview of ensemble methods for binary classifiers in multi-class problems: Experimental study on one-vs-one and one-vs-all schemes // Pattern Recognition. 2011. Vol. 44. no. 8. Pp. 1761-1776.

УДК 004.056

КЛАССИФИКАЦИЯ ПОДХОДОВ К ПОСТРОЕНИЮ МОДЕЛЕЙ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ ЗАДАЧИ ОБНАРУЖЕНИЯ КИБЕР-ИНСАЙДЕРОВ

Быстров Илья Сергеевич, Котенко Игорь Витальевич
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН),
14-я линия В.О., д. 39, (812) 328-71-81, Санкт-Петербург, 199178, Россия
e-mails: ilya.bystrov@outlook.com, ivkote@comsec.spb.ru

Аннотация. В работе рассматриваются подходы к построению моделей поведения пользователей для задачи обнаружения кибер-инсайдеров. Подходы классифицируются по типу входных данных, по способу изменения профиля и по способу выбора профилей для сравнения.

Ключевые слова: модель поведения пользователей; аналитика поведения пользователей; обнаружение кибер-инсайдеров; машинное обучение.

CLASSIFICATION OF APPROACHES FOR USER BEHAVIOR MODELING FOR INSIDER THREATS DETECTION

Bystrov Ilya, Kotenko Igor
St. Petersburg Federal Research Center of the Russian Academy of Sciences.
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: ilya.bystrov@outlook.com, ivkote@comsec.spb.ru

Abstract. Approaches for user behavior modeling are considered. This work proposes a classification of approaches: by nature of input data, by the way of profile change, by the way of choosing profiles for comparison.

Keywords: insider threats; insider threat detection; anomaly detection; machine learning; user behavior analytics.

В настоящее время информационные системы применяются практически во всех компаниях. Информационные системы используются для бухгалтерского учета, ведения документооборота, управления производством и т.д. Во многих случаях сотрудники взаимодействуют с информационными системами: выполняют ввод данных, обработку информации, осуществляют коммуникации как внутри компании, так и вне ее, создают документы различного вида с помощью программных средств и т.п. Сотрудник может использовать имеющийся доступ к информационной системе для того, чтобы нанести вред компании [1, 2]. Действия кибер-инсайдеров наносят ущерб компаниям и количество компаний, пострадавших от таких действий, растет.

В отличие от проблемы обнаружения внешних вторжений, кибер-инсайдер находится "внутри" организации, выполняет должностные обязанности, и его злонамеренные действия могут лишь незначительно отличаться от повседневных.

В литературе предлагаются различные подходы к решению проблемы обнаружения кибер-инсайдеров. Следует отметить, что не все подходы к обнаружению кибер-инсайдеров требуют построения моделей пользователей. Модели поведения пользователя создаются, в частности, при использовании машинного обучения. Машинное обучение наиболее часто используется для решения задачи обнаружения кибер-инсайдеров [1]. В рамках этого подхода создается модель, которая описывает поведение пользователя информационной системы (для каждого пользователя создается профиль). Идея заключается в сравнении профилей и нахождении таких профилей, которые отличаются от других в большей степени по тем или иным параметрам.

Целью данной работы является классификация существующих подходов к построению модели поведения пользователей. В общем случае, модель поведения не эквивалентна набору параметров из входных данных и не эквивалентна модели машинного обучения.

В первом случае, модель может иметь избыточные данные, и, что более важно, может не использовать параметры, которые получаются путем агрегации исходных входных данных. Например, на основе информации о входе в систему и выходе из нее можно получить информацию о времени сессии. Или на основе анализа адресатов сообщений электронной почты возможно получить соотношение, характеризующее соотношение между внутренними и внешними по отношению к компании адресатами, и т.д. Подобные параметры модели выбираются произвольно с целью получения наиболее репрезентативных параметров [3].

Во втором случае, модели машинного обучения существенно зависят от метода. Пропуск данных, наличие корреляций между параметрами, представление параметров в числовой форме - все это особенности, которые учитываются при построении модели машинного обучения. Соответственно на основе одной модели поведения пользователей может быть построено несколько моделей машинного обучения.

Наиболее простым подходом к построению модели поведения пользователь является использование входных данных без дополнительной обработки: между параметрами входных данных и параметрами модели существует однозначное соответствие. Однако часто требуется обработка входных данных [4,5], например, в случае анализа электронных писем. В этом случае применяется, например, построение n-грамм, статистика ключевых слов и т.п. Существует два типа источников технических данных: сетевые устройства и устройства пользователя. В зависимости от источника данных изменяется доступный набор параметров входных данных. Также в некоторых работах используются контекстные данные, не связанные напрямую с взаимодействием между сотрудником и информационной системой. Примерами таких данных будут: организационная структура компании и место сотрудника в ней, его должность; участие и роль в проектах компании (на основе этой информации мы можем, например, в первую очередь сравнивать активность сотрудника с активностью его коллег по проекту). Также могут использоваться данные о мотивации и поведении сотрудника, которыми располагает менеджер по персоналу. Возможно использование данных с таких физических устройств, как двери: информация об открытии дверей [1]. В некоторых работах упоминаются возможности использования биометрических данных [6].

В дальнейшем, при сравнении профилей пользователей, построенных согласно модели, помимо набора профилей, с которыми происходит сравнение (это могут все сотрудники или только сотрудники, обладающие какой-либо схожестью [4]: например, по должности или по исполняемому проекту) необходимо учитывать временной аспект. В некоторых работах предполагается построение профилей пользователей каждый час на основе последних данных. В других работах предполагается использование всех доступных данных. Соответственно, можно выделить две характеристики профиля: временной диапазон используемых входных данных и способ изменения профиля при получении данных: пересоздание профиля или обновление профиля (возможен учет устаревания информации, с помощью, например, применения весовых коэффициентов). Также возможно сопоставление профилей сотрудников с их же профилями, созданными ранее [7].

Соответственно, подходы к построению моделей поведения пользователей можно классифицировать по типу входных данных (данные о сетевых устройствах и устройствах пользователя, контекстные данные, субъективные данные о поведении сотрудника), по способу изменения профиля (пересоздание профиля, инкрементальное обновление профиля), по способу выбора профилей для сравнения (полный набор профилей сотрудников, выбор групп профилей сотрудников по определенным правилам, более ранние профили этого же сотрудника).

Следует отметить, что сравнение профилей происходит после построения и использования модели, но предполагаемый способ сравнения существенно влияет на набор параметров модели. Также следует отметить, что переход от параметров входных данных к параметрам модели, как правило, происходит путем обработки входных данных. Нет какого-то стандартного набора применяемых операций.

Таким образом, классификация подходов к построению модели поведения пользователей создает предпосылки для построения системы обнаружения кибер-инсайдеров, как подкласса системы мониторинга [8], в которой модель поведения пользователей может учитывать параметры, полученные с помощью обработки входных данных, и использоваться в дальнейшем для построения различных моделей машинного обучения.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations / M.N. Al-Mhiqani [et al.] // Applied Sciences. – 2020. – Vol. 10. – A Review of Insider Threat Detection. – № 15. – P. 5208.
2. Le D.C. Machine learning based Insider Threat Modelling and Detection / D.C. Le, A.N. Zincir-Heywood. – 2019. – P. 9.
3. Maloof M.A. ELICIT: A System for Detecting Insiders Who Violate Need-to-Know / M.A. Maloof, G.D. Stephens // Recent Advances in Intrusion Detection

/ eds. C. Kruegel, R. Lippmann, A. Clark ELICIT. – Berlin, Heidelberg: Springer Berlin Heidelberg, 2007. – Vol. 4637. – elicit. – P. 146-166.
4. Insider Threat Detection Based on User Behavior Modeling and Anomaly Detection Algorithms / Kim [et al.] // Applied Sciences. – 2019. – Vol. 9. – № 19. – P. 4018.
5. Automated Insider Threat Detection System Using User and Role-Based Profile Assessment / P.A. Legg [et al.] // IEEE Systems Journal. – 2017. – Vol. 11. – № 2. – P. 503-512.
6. Employee profiling via aspect-based sentiment and network for insider threats detection / C. Soh [et al.] // Expert Systems with Applications. – 2019. – Vol. 135. – P. 351-361.
7. Tabash K.A. Insider-threat detection using Gaussian Mixture Models and Sensitivity Profiles / K.A. Tabash, J. Happa // Computers & Security. – 2018. – Vol. 77. – P. 838-859.
8. Котенко И. В., Полубелова О.В., Саенко И.Б., Чечулин А.А. Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности, Т.8, № 2, 2012. С.100-108.
9. Котенко И.В., Саенко И.Б. Создание новых систем мониторинга и управления кибербезопасностью // Вестник Российской академии наук, Том 84, № 11, 2014, С.993–1001.

УДК 004.716:004.056

ПРОЕКТИРОВАНИЕ СИСТЕМЫ МОНИТОРИНГА СОСТОЯНИЯ ОБЪЕКТА НАБЛЮДЕНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ ИНТЕРНЕТА ВЕЩЕЙ

Воробьев Андрей Игоревич, Гербовец Даниил Сергеевич, Крыжановская Ксения Сергеевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: vorobiov_a@inbox.ru

Аннотация. Проектируется программно-аппаратная система сбора статистики и программного реагирования в сфере мониторинга показателей состояния объекта наблюдения. Система позволяет автоматически производить сбор, анализ и хранение информации, связанной с состоянием объекта наблюдения. Для проектирования системы были рассмотрены основные технологии Интернета вещей, проведен обзор литературы по используемому программно-техническому инструментарию, разработан прототип системы по сбору статистики состояния объекта наблюдения в режиме реального времени. Информационная безопасность сети Интернета Вещей поддерживает безопасность состояния объекта наблюдения в границах обеспечения безопасных границ параметров.

Ключевые слова: интернет вещей; умные вещи; мониторинг состояния объекта; информационная безопасность сети; nodemcu, wittycloud.

DESIGNING A MONITORING SYSTEM FOR THE OBSERVATION OBJECT BASED ON THE INTERNET TECHNOLOGY OF THINGS

Vorobev Andrey, Gerbovetc Danyyl, Krydhanovskaya Ksenia
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: vorobiov_a@inbox.ru

Abstract. A software and hardware system for collecting statistics and software response in the field of monitoring indicators of the observation object is designed. A system is designed to automatically collect, analysis and storage of information associated with the state of observation object. To design the system, the main technologies of the Internet were considered, a review of literature was reviewed on the software-technical tool, a prototype system was developed to collect the statistics of the object of observation object in real time. Information security of the Internet of the Internet maintains the security of the state of observation object within the boundaries of ensuring safe boundaries of parameters.

Keywords: internet of things; smart things; monitoring the status of the object; information security; Internet maintains the security of the state; nodemcu; wittycloud.

В системе мониторинга состояния объекта наблюдения на основе технологии интернета вещей в качестве объекта наблюдения может находиться объект технологии интернета вещей, находящийся под влиянием внешних источников, показатели которых являются контролируемыми параметрами внешней среды. Параметрами могут быть пульсации освещения, громкие звуки, низкочастотные вибрации, электромагнитные поля, концентрация определенных веществ в воздухе, температура и влажность в помещении. По ряду параметров наблюдения может устанавливаться широкая палитра показателей контроля: кислород, водород, углекислый газ, метан, - все эти вещества, могут являться предметом принятия управленческого решения в системе умного дома, умного города, IoT (Internet of Things) Интернет Вещей [1].

Технологии Интернета вещей позволяют подключать к сети в качестве объекта наблюдения автономные устройства; комплексы устройств, способные связываться между собой; устройства межсетевого общения. Технологии Интернета вещей позволяют получать и обрабатывать данные с объектов наблюдения в режиме реального времени, для чего используют как беспроводные, так и проводные сети с предъявляемыми к ним характеристиками эффективности в условиях низких скоростей, отказоустойчивости, адаптивности и возможность самоорганизации [2].

При разработке системы мониторинга объекта наблюдения технология Интернета вещей может обеспечить сбор информации, установить связь между устройствами межсетевого общения, провести анализ и

вывод статистики в удобном беспроводном формате [3]. В аппаратные элементы системы мониторинга включены модули мониторинга, например, температуры, включая контроль пограничных температурных значений; данные при этом обрабатываются и отсылаются на концентрирующее устройство, в случае превышения пограничного значения, модуль позволяет сформировать и отослать оповещение по сети Интернет на Web-сервер для сбора статистики. Для удобства последующего анализа состояния параметров предусмотрена аналитика границ параметров.

В состав модулей мониторинга входят следующие устройства: датчики температуры, микроконтроллеры, которые могут хранить значение измерений, сигнализировать о выходе температуры за установленные границы (сами границы пользователь может устанавливать и изменять), устанавливать точность измерений, способ взаимодействия с контроллером. Датчик может иметь сервисное приложение с открытым исходным кодом, способное отображать кривую изменения температуры в режиме реального времени в виде графика.

Аналогичным образом может работать комплексный газоанализатор с установленными параметрами оценки состава воздуха, определением утечки опасных веществ, сбором статистики и информированием пользователя о высоком содержании вредных веществ в воздухе. Датчик широкого спектра газов MQ-2 способен обнаруживать утечки пропана, бутана, метана и водорода. Также его можно использовать для контроля и определения концентрации задымленности производственных помещений. Датчик построен на базе полупроводникового газоанализатора MQ-2. Пропорционально содержанию газов в окружающей среде на логический выход датчик выдаёт аналоговый сигнал, при программном включении и выключении нагревателя, время автономной работы устройства может быть значительно продлено. Для контроля концентрации углекислого газа в воздухе может быть применен датчик MQ-135, на логический выход датчик выдаёт аналоговый сигнал, пропорциональный концентрации углекислого газа и также оснащенный функцией сбора статистики и информированием пользователя о высоком содержании углекислого газа в воздухе. Датчик MQ-7, анализатор угарного газа позволяет определить уровень угарного газа в воздухе, чтобы предупредить пользователя и избежать негативных последствий опасных доз угарного газа, поскольку по своим параметрам не обладает запахом, бесцветен, крайне токсичен. Датчик построен на базе полупроводникового газоанализатора и на логический выход датчик выдаёт аналоговый сигнал, пропорциональный концентрации угарного газа.

Набор датчиков-газоанализаторов входит в модуль мониторинга активности внешней среды, показания с датчиков собираются, обрабатываются и отсылаются на концентрирующее устройство, с которого по беспроводной сети интернет-ресурса IoT передаются на Web-сервер. Программная часть модуля представляет собой программное обеспечение Android приложения, которое пересылает статистику на web-сервер и транслирует пользователю установленные оповещения. Web-сервер, написанный на языке программирования Python, собирает статистику изменения уровней содержания веществ в воздухе, и, при необходимости, сопровождающих биологических параметров. В случае, если по одному из измеряемых значений будет превышен допустимый уровень значений, анализатор вышлет сигнал прерывания на концентрирующее устройство с наименованием газа и указанием уровня, который был превышен и имеет рекомендуемую качественную интерпретацию состояния внешней среды как объекта мониторинга.

СПИСОК ЛИТЕРАТУРЫ

1. Грингард, С. Интернет вещей. Будущее уже здесь, Альпина Паблишер, 2017. 188 с.
2. Блум, Д. Изучаем Arduino. Инструменты и методы технического волшебств, BHV, 2015. 336 с.
3. И.Е. Артемьев, Е.П. Зараменских. Интернет вещей. Исследования и область применения, Инфра-М. – 2017. 188 с.

УДК 004.056

ОСНОВНЫЕ КРИТЕРИИ СИСТЕМАТИЗАЦИИ ПОДХОДОВ К КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ

Гайфулина Диана Альбертовна
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: gaifilina@comsec.spb.ru

Аннотация. В данном исследовании рассматриваются критерии систематизации подходов корреляции событий безопасности, применяющихся в различных системах анализа защищенности. Систематизация на основе предлагаемых критериев позволит описать существующие подходы к корреляции событий безопасности и сформировать рекомендации по использованию того или иного решения в зависимости от задач применения и особенностей системы анализа защищенности.

Ключевые слова: информационная безопасность; корреляция событий безопасности; корреляция предупреждений; многошаговые атаки; анализ защищенности.

BASIC SYSTEMATIZATION CRITERIA FOR APPROACHES TO SECURITY EVENTS CORRELATION

Gaifulina Diana
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: gaifilina@comsec.spb.ru

Abstract. This research examines the systematization criteria for the approaches to security events correlation used in various security analysis systems. The systematization based on the proposed criteria will allow describing the existing approaches to security events correlation and formulating recommendations for using one or another solution depending on the application tasks and the characteristics of the security analysis system.

Keywords: information security; security event correlation; alert correlation; multi-step attacks; security analysis.

Подходы к анализу защищенности современных информационных систем постоянно совершенствуются, что продиктовано как соответствующим усложнением самих систем и ростом объема обрабатываемых данных, так и растущим разнообразием атак. Для обеспечения безопасности важными задачами являются мониторинг и анализ системных событий, которые представляют собой сообщения или сигналы тревоги, относящиеся к действиям в системе или сети. Таким образом, событие может содержать информацию как о содержимом сетевого пакета, так и сообщение об использованной атакующем уязвимости. Во втором случае подобные события часто называют предупреждениями, которые, как правило, содержат информацию о необычной активности [1]. Данный термин часто применяется авторами в качестве синонима «события безопасности». Примером системы, которая генерирует предупреждения является система обнаружения вторжений.

Важное место среди задач управления событиями безопасности занимает корреляция, позволяющая выявлять взаимосвязи между разнородными событиями и предупреждениями, что способствует лучшему пониманию развития атаки и выявлению наиболее значимых событий в наборе записанных данных. При этом связанные между собой события безопасности могут быть идентифицированы как шаги атакующего для достижения цели, и, следовательно, принадлежать определенному сценарию атаки. Таким образом, использование различных подходов к корреляции событий безопасности позволяет обнаруживать события, несущие возможную угрозу или являющиеся частью многошаговой атаки, а также определять их первопричины для предупреждения в будущем.

Целью данного исследования является определение основных критериев систематизации подходов к корреляции событий безопасности. Используя предлагаемый набор критериев, можно построить схему классификации для унифицированного описания как существующих подходов, так и для принимаемых к разработке. Для определения критериев систематизации необходимо рассмотреть подходы к корреляции событий безопасности, ответив на следующие вопросы:

- как осуществляется корреляция событий безопасности?
- какие знания необходимы для осуществления корреляции событий безопасности?
- возможно ли обнаруживать ранее неизвестные события безопасности?
- каковы источники событий безопасности?
- на каком уровне целевой системы возможна корреляция событий безопасности?
- как организована корреляция событий безопасности с точки зрения архитектуры системы?

Рассмотрев некоторые существующие исследования подходов к корреляции событий безопасности и предупреждений [2-4] с точки зрения поставленных вопросов, можно выделить следующие основные критерии систематизации подходов.

1. Метод корреляции. Методы корреляции событий безопасности можно разделить на три основные категории: на основе сходства, пошаговые и смешанные. Методы на основе сходства сравнивают несколько событий на основе атрибутов или временных меток, а также на основе фильтров. Корреляция событий на основе сходства их атрибутов, например, IP-адресов, номеров портов или сервисов, применяется для выявления похожих предупреждений, что помогает сократить количество обрабатываемых событий для администратора безопасности. Основной принцип такой корреляции заключается в том, что группа похожих предупреждений может соответствовать одному типу атаки. В качестве основного признака сходства может также использоваться метка времени события. При этом нахождение взаимосвязей между событиями безопасности основано на их временном отношении, поэтому корреляция происходит в пределах определенного временного окна. Для уменьшения нерелевантных событий и предупреждений также применяются алгоритмы фильтрации, которые назначают приоритет различным событиям по их критичности для безопасности системы или сети.

Пошаговые методы составляют цепочки событий, восстанавливают действия атакующего и анализируют связи между несколькими событиями. Данный класс методов включает построение сценариев атак, метод предпосылок и последствий, структурные методы, статистические методы и машинное обучение. Подходы на основе сценариев коррелируют события безопасности на основе определенных сценариев атак, заданным сигнатурами. Методы с использованием предпосылок и последствий сопоставляет и связывает между собой события и предупреждения на основе причинности, если условия появления одного события соответствуют предварительным условиям другого события. К категории методов, основанных на структурных моделях, относятся методы, использующие графовые модели, такие как графы и деревья атак. Статистические методы корреляции позволяют делать выводы из распределения исторических данных, анализируя последовательности событий безопасности с точки зрения вероятностей. Среди популярных статистических методов корреляции событий безопасности можно выделить Байесовские сети и Марковские модели. Корреляция на основе машинного обучения и интеллектуального анализа данных использует автоматически генерируемые коэффициенты сравнения. Смешанные методы используют комбинированные алгоритмы. Некоторые подходы и системы объединяют в себе несколько методов корреляции событий безопасности, без явного преобладания одного над другим.

2. Извлечение знаний. Подходы к корреляции событий безопасности можно разделить по происхождению информации об атаках. Так по способу извлечения знаний выделить ручные, обучаемые с учителем и автоматические методы. Ручные методы используют знания, закодированные экспертом в виде правил или сигнатур атак. Экспертные правила создаются путем описания условий совершения атаки, например, с использованием логических выражений, онтологий и других способов описания экспертных знаний. Сигнатуры представляют собой известные и задокументированные шаблоны атак. Методы обучения с учителем используют набор данных, содержащий информацию об атаках. Автоматические методы не используют какие-либо предварительные знания.

3. Тип обнаружения. Подходы к корреляции можно классифицировать по их возможности обнаруживать новые проблемы безопасности. Это зависит от того исследует ли подход злоупотребления или. Первая категория анализирует события, предположительно содержащие данные о конкретных атаках, и не позволяет обнаруживать новые атаки на защищаемую систему. Вторая категория анализирует отклонения от нормального поведения, что может свидетельствовать о новом типе атаки.

4. Количество источников данных. Источник данных событий безопасности может быть как один, так их может быть несколько. Первые используют данные из одного типа источника информации, вторые объединяют различные типы информации.

5. Уровни корреляции событий. В зависимости от этапа обработки предупреждений можно выделить уровни необработанных данных, событий и отчетов. На уровне сырых данных может осуществляться отбор пакетов, сканирование портов, идентификация приложений или анализ полезной нагрузки пакетов. На уровне событий производится агрегирование нескольких событий путем локальной или распределенной корреляции. Уровень отчетов выполняет генерацию возможных активных контрмер и верификацию событий безопасности.

6. Архитектура системы корреляции событий безопасности может быть централизованной, распределенной или иерархической. В подходах с централизованной корреляцией предупреждений сбор данных осуществляется локально различными сетевыми агентами, а затем передается в виде предупреждений на центральный сервер управления, где выполняется корреляционный анализ. Распределенная корреляция позволяет каждому агенту выполнять частичную корреляцию, результаты которой агрегируются, при этом все агенты имеют одинаковый вес. В иерархической архитектуре агенты управления разделены на несколько групп в соответствии с различными функциями, такими как географическое положение, административный контроль и другие.

Подходы к корреляции событий безопасности, разрабатываемые исследователями, необходимы для обнаружения и прогнозирования проблем безопасности с пошаговым характером, таких как многоэтапные или целевые атаки и другие причинно-связанные последовательности аномальных событий. В рамках данной работы была составлена систематизация подходов к корреляции событий безопасности, основываясь на применяемых методах, способах извлечения знаний, количестве используемых источников, уровню анализа и архитектуре.

Работа выполнена при частичной финансовой поддержке РНФ (проект № 21-71-20078).

СПИСОК ЛИТЕРАТУРЫ

1. Wood M., Erlinger M. Intrusion detection message exchange requirements // RFC 4766. IETF. 2007.
2. Федорченко А. В., Левшун Д. С., Чечулин А. А., КотенкоИ. В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1 // Информатика и автоматизация. 2016. Том 4, №. 47. С. 5-27.
3. Navarro J., Deruyver A., Parrend P. A systematic survey on multi-step attack detection // Computers & Security. 2018. Vol. 76. P. 214-249.
4. Ramaki A. A., Rasoolzadegan A., Bafghi A. G. A systematic mapping study on intrusion alert analysis in intrusion detection systems // ACM Computing Surveys (CSUR). 2018. Vol. 51, №. 3. P. 1-41.

УДК 004.056

АНАЛИЗ ПОДХОДОВ К ФОРМИРОВАНИЮ АТРИБУТОВ ДЛЯ АНАЛИЗА ВРЕДОНОСНОГО КОДА НА ОСНОВЕ ЕГО ГРАФИЧЕСКОГО ПРЕДСТАВЛЕНИЯ

Голубев Сергей Александрович, Муренин Иван Николаевич, Новикова Евгения Сергеевна
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: ser9800@mail.ru, imurenin@gmail.com, novikova.evgenia123@gmail.com

Аннотация. Выбор атрибутов при решении задач анализа данных является критически важным этапом, во многом определяющим эффективность их решения. В настоящем докладе обсуждаются подходы к формированию атрибутов вредоносного кода для его дальнейшего анализа на основе его графического представления. Показано, что такой способ генерации признаков позволяет эффективно решать задачи выявления вредоносного кода и установления авторства программных продуктов за счет применения методик глубокого обучения для анализа изображений. Более того, было показано, что использование атрибутов, извлеченных из графического представления исполняемых кодов, позволяет разрабатывать подходы по установлению авторства, независимые от операционной системы.

Ключевые слова: анализ вредоносного кода; выбор атрибутов; графическое представление данных; установление авторства кода.

ANALYSIS OF APPROACHES TO ATTRIBUTE SELECTION FOR MALWARE ANALYSIS BASED ON IMAGES

Golubev Sergei, Murenin Ivan, Novikova Evgenia
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: ser9800@mail.ru, imurenin@gmail.com, novikova.evgenia123@gmail.com

Abstract. The choice of attributes when solving data analysis problems is a critical issue that determines the efficiency of their solution. This report discusses approaches to the formation of malware attributes for its further analysis based on its graphical representation. It is shown that this method of generating features makes it possible to effectively solve the problems of detecting malicious code and establishing authorship of software products by adopting deep learning techniques for image analysis. Moreover, it has been shown that the use of attributes extracted from the graphical representation of executable codes allows the development of platform independent approaches to code authorship attribution.

Keywords: malware analysis; feature selection; image-based features; authorship attribution.

Выбор атрибутов объектов является критически важным этапом при решении различных задач анализа данных. В настоящем докладе анализируются подходы к формированию признаков для исследования программного кода, в основе которых применяется преобразование исходного и исполняемого кода в двумерное изображение. Авторы исследуют преимущества таких подходов для решения задач выявления вредоносного кода и установления его авторства.

Построение графического изображения исполняемого кода для его исследования не является новым подходом к анализу вредоносного кода. В [1] черно-белые изображения исполняемых файлов с последующими выделениями текста и признаков используется для выявления вредоносного кода, при этом не требуется ни дизассемблирование исполняемого файла, ни выполнение потенциально опасного вредоносного кода. Авторы показали, что вредоносный код, который принадлежит одному и тому же семейству, характеризуется схожими графическими паттернами. Точность классификации при этом достигает 98% на множестве образцов вредоносного кода, принадлежащих 25 различным семействам. В [2] авторы применили глубокие нейронные сети, предобученные на базе изображений ImageNet, для классификации изображений, построенных на основе исполняемого кода, полученная точность достигла 99.25%.

Для установления авторства исполняемых файлов обычно используются признаки, извлеченные из анализа последовательности кодов операций, вызовов функций API [3]. Однако в [4] авторы также исследовали применимость признаков, построенных на основе графического представления бинарных кодов. Бинарный файл считывается по байтам, каждый байт сопоставляется с цветом, а полученное изображение сжимается до квадрата для дальнейшей классификации. Эксперименты показали, что классификатор, построенный на таких признаках, показывает лучшие результаты в случае установления принадлежности авторства нескольким авторам и использования различных настроек оптимизации компилятора.

Таким образом, данный подход к анализу программного кода позволяет классифицировать вредоносные программы и их принадлежность к какому-то семейству; а также определять авторство программного кода независимо от того, на каком языке программирования был написана программа или для какой платформы. Это позволяет авторам предположить перспективность его использования для решения других задач информационной безопасности, в частности, для обнаружения аномалий в сетевом трафике. Авторы считают, что его применение для формирования атрибутов, извлеченных из сетевого трафика, позволит разрабатывать подходы для обнаружения аномалий, которые не зависят от типов устройств, сетевых протоколов, обеспечивая тем самым переносимость («кросс-платформенность») модели анализа между различными конфигурациями и устройствами Интернета вещей. Также с помощью этого метода можно перейти на другой уровень оперирования данными: вместо того, что работать, например, с числовыми данными и применять необходимый математический аппарат, работа будет происходит с изображениями, где можно применить другие методы анализа.

СПИСОК ЛИТЕРАТУРЫ

1. L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath. 2011. Malware images: visualization and automatic classification. In Proceedings of the 8th International Symposium on Visualization for Cyber Security (VizSec '11). Association for Computing Machinery, New York, NY, USA, Article 4, 1–7. DOI: https://doi.org/10.1145/2016904.2016908
2. C Li. Malware Analysis Using Visualized Image Matrices, arXiv preprint: arXiv:1812.07606v1
3. V. Kalgutkar, R. Kaur, H. Gonzalez, N. Stakhanova, and A. Matyukhina. 2019. Code Authorship Attribution: Methods and Challenges. ACM Comput. Surv. 52, 1, Article 3 (February 2019), 36 pages. DOI: https://doi.org/10.1145/3292577
4. Alrabaee S., Karbab E.B., Wang L., Debbabi M. BinEye: Towards Efficient Binary Authorship Characterization Using Deep Learning. In: Sako K., Schneider S., Ryan P. (eds) Computer Security – ESORICS 2019. ESORICS 2019. Lecture Notes in Computer Science, vol 11736. Springer, Cham. https://doi.org/10.1007/978-3-030-29962-0_3.

УДК 004.056

АНАЛИЗ ПРИМЕНИМОСТИ И ТЕОРЕТИЧЕСКАЯ ОЦЕНКА СРЕДСТВ АНАЛИЗА ЗАЩИЩЕННОСТИ КОМПОНЕНТОВ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

Десницкий Василий Алексеевич
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: desnitsky@comsec.spb.ru

Аннотация. Проводится анализ применимости и теоретическая оценка построенных средств анализа защищенности беспроводных сенсорных сетей (БСС) в условиях наличия разнородных и взаимодействующих между собой устройств, использующих беспроводные коммуникационные протоколы связи с учетом повышенных требований к информационной безопасности таких сетей.

Ключевые слова: беспроводная сенсорная сеть; информационная безопасность; анализ применимости; теоретическая оценка.

ANALYSIS OF APPLICABILITY AND THEORETICAL EVALUATION OF MEANS FOR ANALYSIS OF PROTECTION OF THE COMPONENTS IN WIRELESS SENSOR NETWORKS

Desnitsky Vasily
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: desnitsky@comsec.spb.ru

Abstract. An analysis of the applicability and theoretical evaluation of the constructed tools for analyzing the security of wireless sensor networks in the presence of heterogeneous and interacting devices using wireless communication protocols is performed. It is fulfilled, taking into account the increased requirements for information security of such networks.

Keywords: wireless sensor network, information security; applicability analysis; theoretical evaluation.

Введение. Проводятся анализ применимости и теоретическая оценка разработанных трех методик – методики верификации моделей представления БСС на предмет выполнимости условий осуществления атак; методики распределенных сбора, обработки и анализа больших массивов данных от программных и аппаратных сенсоров БСС; методики выявления аномальных данных от сенсоров БСС [1].

Теоретическая оценка предложенных методик выражается в выяснении их корректности путем проверки обоснованности применения подходов и методов, лежащих в основе каждой из методик. Методика верификации моделей представления БСС базируется на применении средств формальной верификации с использованием базы правил, сформулированных экспертным путем, и сопоставляющих наборам факторов структурно-функционального представления сети и ее узлов конкретные виды атакующих воздействий, необходимыми условиями возникновения которых являются данные факторы.

Методика распределенных сбора, обработки и анализа больших массивов данных от программных и аппаратных сенсоров БСС осуществляется с использованием методов параллельных и кластерных вычислений в пределах узлов БСС. Применимость этих методов обосновывается получением выигрыша в обеспечении эффективного ресурсопотребления, во-первых, в результате динамического перераспределения операций между узлами сети и, во-вторых, за счет возможности распараллеливания алгоритмов сбора, обработки и анализа данных. Методика выявления аномальных данных от сенсоров БСС строится на методах машинного обучения и искусственных нейронных сетей, корректность применения которых обосновывается получением сбалансированных исходных данных большого объема; расширенным перечнем анализируемых методов обучения, в том числе использованием механизма эффективного перебора гиперпараметров; тестированием на контрольной выборке данных и вычислением показателей качества выявления. Возможно обобщение указанных трех методик на более широкий перечень атак. Однако в соответствии с используемым подходом такие атаки должны быть известного вида, причем соответствующие наборы исходных данных должны быть размечены под эти новые виды атак. Перспективными для дальнейшего развития данного направления видятся технология Больших Данных в ее приложении к БСС [2] и технология облегченных обучающих моделей [3].

Заключение. На базе построенных трех научно-технических решений по анализу защищенности БСС проведены их теоретическая оценка и анализ их применимости на практике.

Работа выполнена при финансовой поддержке гранта РФФИ № 19-07-00953.

СПИСОК ЛИТЕРАТУРЫ

1. Десницкий В.А., Котенко И.В. Проектирование защищенных встроенных устройств на основе конфигурирования // Проблемы информационной безопасности. Компьютерные системы, 2013, № 1. С. 44-54.
2. Abrahamsson P. et al. Affordable and Energy-Efficient Cloud Computing Clusters: The Bolzano Raspberry Pi Cloud Cluster Experiment // Proceedings of 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, 2013. P. 170-175.
3. Sliwa B., Piatkowski N., Wietfeld C. LIMITS: Lightweight Machine Learning for IoT Systems with Resource Limitations // Proc. of IEEE International Conference on Communications (ICC), 2020. P. 1-7.

УДК 004.056

ПОДХОД К МОНИТОРИНГУ АТАК ТИПА DENIAL-OF-SLEEP В БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЯХ С ПРИМЕНЕНИЕМ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ

Десницкий Василий Алексеевич
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: desnitsky@comsec.spb.ru

Аннотация. В работе предложен и апробирован подход к мониторингу атак типа Denial-of-Sleep в беспроводных сенсорных сетях (БСС) на основе методов интеллектуального анализа данных. Данный вид атак применим к автономно работающим беспроводным устройствам и узлам, беспроводных сенсорных сетей. Путем прямого или опосредованного воздействия на узлы сети, за счет препятствования их перехода в режим энергосбережения (режим сна), атакующий способен за короткий срок истощить имеющиеся энергоресурсы узлов и тем самым сделать их неработоспособными. Мониторинг производится на основе детектирования признаков данного вида атак и представляет собой один из модулей комплексной системы мониторинга безопасности БСС.

Ключевые слова: беспроводная сенсорная сеть; информационная безопасность; атака типа Denial-of-Sleep; энергопотребление; сетевая коммуникация.

AN APPROACH TO MONITORING DENIAL-OF-SLEEP ATTACKS IN WIRELESS SENSOR NETWORKS USING INTELLIGENT DATA ANALYSIS

Desnitsky Vasily
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: desnitsky@comsec.spb.ru

Abstract. In the work an approach to monitoring Denial-of-Sleep attacks in wireless sensor networks (WSN) based on intelligent data analysis is proposed and tested. This type of attack is applicable to autonomous wireless devices and nodes of the wireless sensor network. By directly or indirectly affecting the nodes of the network, by preventing them from switching to the energy-saving mode (sleep mode), the attacker is able to deplete the available energy resources of the nodes in a short time and thereby make them inoperable. The monitoring is based on the detection of features of this type of attacks and is one of the modules of the integrated security monitoring system of WSN.

Keywords: wireless sensor network; information security; Denial-of-Sleep attack; energy consumption; network communication.

Введение. Предлагаемый подход к мониторингу атакующих воздействий типа Denial-of-Sleep в беспроводных сенсорных сетях апробируется на фрагменте разрабатываемого лабораторного прототипа системы оперативного управления и реагирования в чрезвычайных ситуациях [1-2]. Такие системы представляют сети самоорганизующихся устройств различного вида, объединенных в единое сетевое пространство, перемещающихся в пространстве, и обеспечивающие функции надежной защищенной коммуникации пользователям сети.

К основным признакам такой сети можно отнести:

– автономное функционирование устройств – автономные источники питания;

– беспроводные коммуникации – мобильность, возможность перемещения в пространстве без потери коммуникации;

– наличие энергоэффективного режима работы – для решения продолжающихся во времени прикладных задач;

– подверженность атакам типа Denial-of-Sleep – как результат автономности, мобильности и энергоэффективного режима.

Для обеспечения возможностей разработки средств мониторинга на фрагменте разрабатываемого программно-аппаратного прототипа производится моделирование атак типа Denial-of-Sleep. Атакующее устройство представляет собой беспроводной модуль XBee, работающий в непосредственной связке с персональным компьютером или другом стационарным элементом информационно-телекоммуникационной инфраструктуры. При этом модуль XBee также может интегрироваться с другим электронным и коммуникационно-вычислительным к нему могут непосредственно подключаться различные сенсор и исполнительные элементы для их прямого взаимодействия с другими узлами беспроводной сенсорной сети и ее окружения.

Атакующий отправляет серии множественных запросов через доступный ему беспроводной коммуникационный интерфейс (в данном случае запросов GPS/ГЛОНАСС-координат узла - жертвы атаки) с исходящим адресом, подмененным на адрес жертвы. В рамках проводимого в работе моделирования запросы не отправляются непосредственно на сторону узлы-жертвы в целях повышения скрытности осуществляемой атаки [3].

Таким образом, атакующие данные поступают на эксплуатируемый модуль XBee, который, в свою очередь, формируя ответы, отправляет их на узел-жертву. Тем самым, атакующий препятствует переходу узла-жертвы в режим сна.

В целях обеспечения возможности перехода автономного узла беспроводной сенсорной сети в режим сниженного энергопотребления, все сообщения, передаваемые по беспроводной сенсорной сети в соответствии с шаблоном нормального поведения такой сети, отправляются в сгруппированном виду – в виду «пачек» сообщений.

Используются параметры моделируемого нормального поведения с использованием трех основных характеристик (осей признакового пространства) и значений их погрешности [4]. Учитываются следующие характеристики: интервал времени между пачками, число сообщений в пачке и интервал внутри пачек. Значения каждой характеристики выбирались из двух вариантов – значений, которые могут быть описаны как «условно низкое» и «условно высокое».

Строятся графики зависимости числа сообщений от времени – для случая нормального поведения в сети отмечается характерное «ступенчатое» поведение графика отображаемой функции.

Моделирование атакующего воздействия включает запись поступающего на узел трафика, являющегося смесью нормального трафика (в виде, так называемых, ступенек) и непрерывного наводнения (flooding) узла атакующим трафиком. Результирующие графики показывают, во-первых, значительно более резкий рост энергопотребления с течением времени, и, во-вторых, сглаживание ступенек.

Помимо установки возможности и потенциальной эффективности визуального анализа, в качестве альтернативного метода мониторинга разработан прототип компонента детектирования таких атак на основе методов интеллектуального анализа данных, включающих в первую очередь методы машинного обучения с учителем [5-6].

В качестве основных формальных признаков атакующего трафика рассматривались следующие характеристики:

- общее количество сообщений в единицу времени;
- отношение максимального интервала между сообщениями и минимального.

В качестве обучающих моделей используются следующие:

- KNN (метод ближайших соседей);
- SVN (метод опорных векторов);
- DT (деревья решений);
- RF (случайный лес);
- и другие, в том числе комбинирование различных моделей методами мажоритарного голосования и стекинга.

Кроме того, применялся метод подбора наилучших гипер-параметров указанных обучающих моделей (механизм GridSearch).

Значение показателей качества детектирования, в частности, показателя F1-меры при комбинировании обучающих моделей приблизительно равняется 96%, что подтверждает применимость разработанного подхода на практике.

Заключение. Предложен и апробирован подход к мониторингу атак типа Denial-of-Sleep в беспроводных сенсорных сетях (БСС) на основе методов интеллектуального анализа данных [7]. Подход апробирован на лабораторном прототипе сети управления в чрезвычайных ситуациях с использованием беспроводной технологии XBee. Высокие значения показателя качества детектирования позволяют говорить о применимости подхода на практике.

Работа выполнена при частичной финансовой поддержке гранта РФФИ № 19-07-00953 и гранта Президента Российской Федерации № МК-5848.2018.9.

СПИСОК ЛИТЕРАТУРЫ

1. Shakhov V., Koo I., Rodionov A. Energy exhaustion attacks in wireless networks // Engineering, Computer and Information Sciences (SIBIRCON), Proceedings of 2017 International Multi-Conference on, IEEE, 2017. P. 1-3.
2. Desnitsky V., Kotenko I., Rudavin N. Ensuring Availability of Wireless Mesh Networks for Crisis Management // Intelligent Distributed Computing XII. Studies in Computational Intelligence. Springer-Verlag. Vol.798, 2018. P. 344-353.
3. Hsueh C.T., Wen C.Y., Ouyang Y.C. A secure scheme for power exhausting attacks in wireless sensor networks // Proceedings of 2011 IEEE Third International Conference on Ubiquitous and Future Networks (ICUFN), 2011. P. 258-263.
4. Десницкий В.А., Котенко И.В. Проектирование защищенных встроенных устройств на основе конфигурирования // Проблемы информационной безопасности. Компьютерные системы, 2013, № 1. С. 44-54.
5. Adi E., Anwar A., Baig Z., Zeadally S. Machine learning and data analytics for the IoT // Neural Computing and Applications, 2020. Volume 32. P. 16205–16233.
6. Hussain F., Hussain R., Hassan S., Hossain E. Machine Learning in IoT Security: Current Solutions and Future Challenges // IEEE Communications Surveys & Tutorials, 2020. P. 1-37.
7. Alsheikh A.M., Lin S., Niyato D., Tan H.P. Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications // IEEE Communications Surveys & Tutorials, 2014. Volume 16 (4). P. 1-23.

УДК 004.451:004.056

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ «ОПЕРАЦИОННЫЕ СИСТЕМЫ»

Егоров Сергей Сергеевич, Широков Владимир Владимирович, Щиголева Марина Андреевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: ssegorov@mail.ru, vvshirokov@mail.ru, vvcehanovsky@mail.ru

Аннотация. Преподавание дисциплины «Операционные системы» включает учет необходимых требований при создании перспективных современных программных продуктов и средств разработки программных продуктов для соответствия курса обучения профессиональному стандарту выпускников бакалавриата по направлению «Информационные системы и технологии» и специалитета по направлению «Компьютерная безопасность». Формат обучения сочетает теоретический материал, практические задания по каждой теме и фонды оценочных средств.

Ключевые слова: безопасность информационных технологий; информационные системы и технологии; компьютерная безопасность; операционная система.

INFORMATION TECHNOLOGY SECURITY IN THE REMOTE STUDY OF THE "OPERATING SYSTEMS"

Egorov Sergey, Shirokov Vladimir, Schigoleva Marina
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: ssegorov@mail.ru, vvshirokov@mail.ru, vvcehanovsky@mail.ru

Abstract. Teaching of the discipline "Operating Systems" includes taking into account the necessary requirements when creating promising modern software products and software development tools to meet the professional standard of graduates of the bachelor's degree in the direction of "Information Systems and Technologies "and the specialty in the direction of "Computer Security". The training format combines theoretical material, practical tasks on each topic and assessment funds.

Keywords: information technology security; information systems and technologies; computer security; operating system.

Рассмотрена модернизация дисциплины «Операционные системы» направления бакалавриата «Информационные системы и технологии» (ИСТ) и специалитета по направлению «Компьютерная безопасность» (КБ). Выбрана стратегия сближения учебного материала направления обучения «Информационные системы и технологии» в части программно-технических и вычислительных средств обеспечения безопасности информационных технологий и направления «Компьютерная безопасность» в части применимости инструментального аппарата информационной и компьютерной безопасности (ИКБ) при проектировании, реализации и применении информационных систем, в том числе, целевых и проблемно-ориентированных.

Материал дисциплины содержит конспект лекций [1, 2] с фиксированным набором тем и комплект практических заданий по каждой теме дисциплины. Методология учебного курса учитывает требования профессионального стандарта программиста, которому должны соответствовать выпускники направлений «Информационные системы и технологии» и «Компьютерная безопасность», необходимо включая выполнение профессиональных трудовых функций, поддержанных необходимыми знаниями, умениями и навыками по разработке и проектированию программного продукта.

В комплекте практических заданий материал по безопасности информационных технологий акцентирован с различной степенью разрабатываемости и отчетности именно по тематике ИКБ: от предметного тематического задания по ИКБ до задания по информационным технологиям со встроенным блоком, решающим задачи безопасности внутри блока с входными и выходными конструктивными параметрами информационной системы. На каждый тематический раздел приходится от одного до пяти заданий [3, 4]. Лекции и практические занятия поддерживаются единой технологией представления материала и формируют общее представление о срезе работы операционной системы, относящемуся к изучаемому разделу и единым программным интерфейсом (API) операционной системы.

СПИСОК ЛИТЕРАТУРЫ

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. — СПб.: Питер, 2015. — 1120 с.: ил. — (Серия «Классика computer science»).
2. Система электронного обучения и тестирования Moodle: обзор возможностей. [Электронный ресурс] URL: https://www.ispring.ru/elearning-insights/moodle. (Дата обращения: 27.09.2021)
3. [Электронный ресурс] URL: http://manpages.org/namespaces/7 (Дата обращения: 27.09.2021)
4. [Электронный ресурс] URL: http://manpages.org/acl/5 (Дата обращения: 27.09.2021)

УДК 004.5

БЕЗОПАСНЫЙ ИНТЕРФЕЙС ДЛЯ УПРАВЛЕНИЯ УСТРОЙСТВОМ ТИПА «УМНОЕ ЗЕРКАЛО»

Жернова Ксения Николаевна
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: zhernova@comsec.spb.ru

Аннотация. По мере распространения технологии Интернета вещей, появляется всё больше разнообразных устройств, поддерживающих эту технологию. Одним из таких устройств является «Умное зеркало». Данный тип устройств может управляться с помощью различных видов интерфейсов: кнопочные, сенсорные, жестовые и т.п. Также эти устройства часто имеют различные функции и приложения, которые содержат конфиденциальные данные пользователя. Таким образом, личная информация пользователя может оказаться под угрозой, если интерфейс «Умного зеркала» не защитить. В докладе будут рассмотрены возможные модели взаимодействия с «Умным зеркалом», а также методы защиты его интерфейса.

Ключевые слова: пользовательский интерфейс; жестовый интерфейс; человеко-компьютерное взаимодействие; Интернет вещей; компьютерная безопасность.

SECURE INTERFACE TO CONTROL DEVICE TYPE «SMART MIRROR»

Zhernova Ksenia
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: zhernova@comsec.spb.ru

Abstract. As the technology of the Internet of Things spreads, more and more various devices support this technology. One of these devices is the «Smart Mirror». This type of device can be controlled using various types of interfaces: pushbutton, touchscreen, gesture, etc. Also, these devices often have various functions and applications that contain sensitive user data. Thus, the user's personal information may be at risk if the «Smart Mirror» interface is not protected. The report will consider possible models of interaction with the «Smart Mirror», as well as methods of protecting its interface.

Keywords: user interface; gesture interface; human-computer interaction; Internet of things; computer security.

В настоящее время получила большое распространение технология Интернета вещей. Эта технология охватывает самые разные области жизни человека. По этой причине всё больше различных устройств присоединяется к сети Интернета вещей и обменивается огромным количеством данных. Среди подобных устройств также встречаются устройства типа «Умное зеркало».

«Умное зеркало» представляет собой устройство с зеркальной поверхностью, под которой спрятан экран. Во включенном состоянии на экране отображаются данные, необходимые пользователю. В выключенном состоянии устройство выглядит как обычное зеркало. «Умное зеркало» может быть подключено к сети «Умного дома» и управлять остальными устройствами. Также оно может быть подключено к сети Интернет и получать актуальные данные о погоде, новостях, сообщениях для пользователя в мессенджерах и т.д.

«Умное зеркало» может иметь различные интерфейсы управления. В настоящее время распространены кнопочный и сенсорный интерфейсы. Недостатки таких интерфейсов достаточно очевидны: зеркало часто устанавливается в общественных местах или в местах с повышенной влажностью, что приводит к быстрому загрязнению поверхности. В общественных местах это также может быть сопряжено с распространением инфекций, так как, в случае кнопочного интерфейса, требуется прикасаться к кнопкам, а в случае сенсорного – выполнять жесты пальцами рук, прикасаясь при этом к сенсорному экрану [1]. Ввиду напряжённой эпидемиологической обстановки, в общественных местах используются перчатки, поэтому управление на основе сенсорного интерфейса может быть затруднено. По этой причине необходим интерфейс с бесконтактным управлением.

Среди бесконтактных интерфейсов иногда встречаются зеркала с голосовым управлением, однако для управления голосом не всегда существует возможность. По этой причине предлагается управление с помощью жестового интерфейса, основанного на жестах рук, улавливаемых специальной камерой. Такой интерфейс не требует касания экрана, что позволит избежать загрязнения поверхности, а также передачи болезнетворных микроорганизмов от человека к человеку. Для повышения точности регистрации жестов может использоваться несколько камер по углам зеркала.

Однако, в домах и квартирах, в которых иногда бывают посторонние, может потребоваться ограничить доступ к интерфейсу, поскольку устройство может содержать данные пользователя, которые нежелательно распространять. Многие устройства подвержены рискам несанкционированного доступа к ним посторонних лиц. Приложения, которые могут быть подключены, могут содержать конфиденциальные данные пользователя. Например, злоумышленник имеет возможность получить доступ к сообщениям пользователя в мессенджерах и социальных сетях.

Для защиты от несанкционированного доступа применяются различные способы аутентификации [2, 3]. Ниже перечислены некоторые примеры методов аутентификации:

– биометрическая аутентификация с помощью распознавания лиц;
– биометрическая аутентификация с помощью распознавания голоса;
– аутентификация на основе пароля или PIN-кода;

Также чаще всего рекомендуется применять двухфакторную аутентификацию [3] для повышения надёжности защиты данных, к которым можно получить доступ с помощью «Умного зеркала».

В докладе рассмотрены разные типы интерфейса для управления устройством «Умное зеркало», а также предложен жестовый интерфейс как наиболее безопасный, рассмотрена угроза несанкционированного доступа к устройству типа «Умное зеркало», предложены возможные способы защиты от данного типа угроз, представлены основные надёжные методы аутентификации пользователя.

Работа выполнена при финансовой поддержке Фонда Содействия Инновациям по программе «УМНИК» (договор 504ГУЦЭС8-D3/61980).

Работа представлена научным руководителем, к.т.н., доцентом А.А. Чечулиным.

СПИСОК ЛИТЕРАТУРЫ

1. Zhernova K. et al. Adaptive Touch Interface: Application for Mobile Internet Security //International Symposium on Mobile Internet Security. – Springer, Singapore, 2019. – С. 53-72.
2. Roesner F., Kohno T., Molnar D. Security and privacy for augmented reality systems //Communications of the ACM. – 2014. – Vol. 57. – №. 4. – Pp. 88-96.
3. Shrestha P., Saxena N. An offensive and defensive exposition of wearable computing //ACM Computing Surveys (CSUR). – 2017. – Vol. 50. – №. 6. – Pp. 1-39.

УДК 004.5

ОБЗОР УГРОЗ БЕЗОПАСНОСТИ ДЛЯ СОВРЕМЕННЫХ ВИДОВ ИНТЕРФЕЙСОВ

Жернова Ксения Николаевна, Чечулин Андрей Алексеевич
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: zhernova@comsec.spb.ru, chechulin@comsec.spb.ru

Аннотация. В разных областях деятельности человека, в том числе в компьютерной безопасности, применяются различные технологии человеко-компьютерного взаимодействия. Применяются также и относительно новые технологии, такие как сенсорные экраны и виртуальная/дополненная реальность. Однако с развитием этих технологий становятся актуальными и новые проблемы безопасности. Появляются также угрозы, специфичные для новых типов интерфейсов. В докладе описаны основные выявленные типы угроз, характерные для обоих новых типов интерфейсов, а также представлены угрозы, специфичные для каждого из этих интерфейсов.

Ключевые слова: пользовательский интерфейс; сенсорный интерфейс; виртуальная реальность; дополненная реальность; человеко-компьютерное взаимодействие; компьютерная безопасность.

OVERVIEW OF SECURITY THREATS FOR MODERN INTERFACES

Zhernova Ksenia, Chechulin Andrey
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: zhernova@comsec.spb.ru, chechulin@comsec.spb.ru

Abstract. In different areas of human activity, including computer security, various technologies of human-computer interaction are used. Relatively new technologies such as touch screens and virtual/augmented reality are also being applied. However, with the development of these technologies, new security issues become relevant. There are also emerging threats specific to new types of interfaces. The report describes the main identified types of threats, typical for both new types of interfaces, and also presents the threats specific to each of these interfaces.

Keywords: user interface; touch interface; virtual reality; augmented reality; human-computer interaction; computer security.

Для защиты данных пользователя в приложениях постоянно разрабатываются новые методы. Однако не только конфиденциальные данные пользователя, но и сами интерфейсы взаимодействия с приложениями могут быть подвержены угрозам безопасности. Данная проблема особенно актуальна для относительно новых типов интерфейсов, которые в настоящий момент активно развиваются: сенсорные экраны и виртуальная/дополненная реальность.

Предложена модель угроз, в которой выделены несколько групп угроз:

1) угрозы системе взаимодействия, когда опасности подвергаются данные в системе [1];

2) угрозы оператору, когда опасности подвергается сам оператор [1];

3) угрозы устройствам интерфейса, когда существует вероятность несанкционированного доступа к устройствам [2];

4) угрозы при пересечении виртуальной и реальной сред, когда угроза возникает при взаимодействии с другими пользователями в виртуальной среде или третьей стороной в реальной среде [2].

Рассмотрим первую и вторую группы более подробно. Данные группы также делятся на три составляющих. Так, угрозы системе взаимодействия подразделяются на следующие подгруппы:

– угрозы, возникающие при вводе данных, так как входные данные могут быть скомпрометированы и/или перехвачены сторонним наблюдателем;

– угрозы, возникающие при хранении и обработке данных, так как с помощью вредоносного программного обеспечения могут быть нарушены конфиденциальность, целостность и доступность данных, хранящихся и обрабатываемых в системе;

– угрозы, возникающие при выводе данных, так как изменение данных влияет на их отображение.

В свою очередь, угрозы оператору также могут быть разделены на три подгруппы:

– угрозы, направленные на искажение восприятия оператором виртуальной среды;

– угрозы, направленные на искажение вводимых оператором данных;

– угрозы самочувствию оператора.

Угрозы оператору – это угрозы, специфичные для новых типов интерфейсов, особенно для виртуальной/дополненной реальности, поскольку, благодаря шлему виртуальной реальности, визуализация данных находится вокруг пользователя, таким образом, пользователь полностью погружён в виртуальную среду. В случае сенсорных экранов полного погружения не происходит, поскольку человек управляет визуализацией с помощью жестов рук на сенсорном экране [3]. По этой причине, оператор интерфейса сенсорных экранов гораздо менее подвержен данному типу угроз, чем пользователь виртуальной/дополненной реальности. Кроме того, угрозой являются возможные нарушения безопасности при пересечении виртуальной и реальной сред, поскольку и в том, и в другом случае, в отличие от традиционных интерфейсов, оператор взаимодействует не с самими данными, а с их визуализацией.

В докладе описаны основные группы угроз безопасности новых типов интерфейсов взаимодействия оператора с приложениями компьютерной безопасности. Также выделены типы угроз, ставшие специфичными именно для новых типов интерфейсов. Специфичность этих угроз объясняется тем, что оператор с помощью интерфейсов, основанных на сенсорных экранах и виртуальной/дополненной реальности, управляет не данными, а визуализацией этих данных.

Работа выполнена при финансовой поддержке РФФИ (проект 20-37-90130 Аспиранты).

СПИСОК ЛИТЕРАТУРЫ

1. Жернова К. Н. Использование интерфейсов виртуальном реальности в области информационной безопасности //Информатизация и связь. – 2021. – №. 2. – С. 118-127.
2. De Guzman J. A., Thilakarathna K., Seneviratne A. Security and privacy approaches in mixed reality: A literature survey //ACM Computing Surveys (CSUR). – 2019. – Т. 52. – №. 6. – С. 1-37.
3. Жернова К.Н., Коломеец М.В., Котенко И.В., Чечулин А.А. Применение адаптивного сенсорного интерфейса в приложениях информационной безопасности // Вопросы кибербезопасности. 2020. № 1 (35). С. 18-28.

УДК 681.1.003

РАЦИОНАЛЬНЫЙ АЛГОРИТМ ПРОВЕРКИ ГИПОТЕЗ КОМПЛЕКСНОГО ИССЛЕДОВАНИЯ НА БАЗЕ ГЕОХРОНОЛОГИЧЕСКОГО ТРЕКИНГА

Ивакин Ян Альбертович[1], Потапычев Сергей Николаевич[2]

[1]АО «Концерн «Океанприбор»

Чкаловский пр., 46, Санкт-Петербург, 198226, Россия

[2]Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)

14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия

e-mails: potapychev@mail.ru, yan_a_ivakin@mail.ru

Аннотация. Полнофункциональное развитие компьютерной интерпретации методов теории графов на базе геохронологического трекинга способно обеспечить новое качество логистического планирования с использованием современного ГИС-инструментария. Рассмотрению качественно новых возможностей такого подхода, а также оптимизации соответствующего алгоритмического аппарата посвящен данный доклад.

Ключевые слова: географические информационные системы; ГИС-технологии для комплексных исследований; геохронологический трек и трекинг; изоморфизм графов; рациональный алгоритм; рационализация алгоритма; комплексных исследований на базе ГИС.

REFINEMENT ALGORITM OF HYPOTHESES TESTING COMPLEX RESEARCH BASED ON GEOCHRONOLOGICAL TRACKING

Ivakin Yan[1], Potapychev Sergey[2]

[1]JSC «Concern «Oceanpribor»

46 Chkalovsky Av, St. Petersburg, 198226, Russia

[2]St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)

39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia

e-mails: potapychev@mail.ru, yan_a_ivakin@mail.ru

Abstract. Dispatching for geospatial processes of transport with implementation of geochronological tracking tools is tightly related with completion of more developed model of data processing in the automated vessel traffic control system. The mathematic and algorithmic apparatus defines the effectiveness of its application. This requires a specific refinement task and searching for corresponding extremums. The report is dedicated to the thorough consideration of this feature.

Keywords: geographic information systems; GIS-technologies for complex research; geochronological track and tracking; graphs isomorphism; optimal algorithm; refinement of algorithm; GIS-based complex research; refinement tasking.

Комплексный анализ прикладных пространственно распределенных процессов есть основа для выработки решений по развитию и оптимизации соответствующих маршрутных сетей, количеству привлекаемых ресурсов, по объемам необходимого финансирования и пр. Одним из наиболее эффективных средств указанного анализа является информационная технология геохронологического трекинга или геохронотрекинга. Программные средства геохронотрекинга становятся одним из наиболее популярных пользовательских приложений в интегрируемых в состав геоинформационных систем (ГИС) пакетов прикладных программ.

На основе геохронотрекинга разработана процедура проверки исследовательских гипотез об устойчивых тенденциях в процессах миграции, перемещений объектов, контроля трафика и пр. Сегодня эта процедура используется для анализа логистики современных транспортно-поставочных сетей, оптимизации транспортных потоков, систем диспетчеризации транспорта. Ее математическая сущность сводится к поиску и оценке статистической значимости изоморфизма соответствующих графов: итоговый граф геохронотрекинга представляется как граф-базис, в структуре которого выявляется подграф изоморфный заданному, т. е. устанавливается наличие взаимно однозначного отображения одного графа на подграф другого, при котором сохраняется отношение инцидентности. Граф, на изоморфность к которому в составе базового графа геохронологического трекинга определяется подграф, топологически описывает ту или иную определенную гипотезу исследования об устойчивой особенности в перемещениях исторических личностей, объектов или других сущностей в географическом пространстве. Далее определяется степень устойчивости в признании гипотезы исследования о выявляемой особенности в перемещениях с использованием статистического аппарата доверительной вероятности и доверительных интервалов.

Вместе с тем особенности алгоритмизации указанной процедуры геохронотрегинга во многом определяют результативность и точность ее применения в процессе прикладных исследований на базе ГИС. Очевидно, что высокая вычислительная и временная сложность базового алгоритма определения изоморфного вложения в граф предъявляет высокие требования именно к корректной программной реализации указанной процедуры при ее практическом внедрении. Этот факт определил необходимость задания соответствующей задачи рационализации, установления граничных условий ее решения и алгоритмизации поиска соответствующих экстремумов.

Постановка такой задачи должна учитывать ограничения, налагаемые реальными условиями объекта исследования – предметной областью ретроспективного исследования.

Указанная рационализация позволяет обеспечить возможность вариабельности в применении наилучшим образом алгоритма проверки гипотез ретроспективных исследований на основе геохронологического трекинга для различных комбинаций входных данных и требований к точности, ресурсоемкости и быстроте алгоритма получения выходных данных. Такая рационализация также способствует широкому внедрению и автоматизации геохронотрекинга, как прикладного метода научных исследований.

Рассмотрение математических и системологических сторон представленной рационализации описанного алгоритма статистической проверки гипотез комплексного исследования на основе геохронологического трекинга в ГИС и есть предмет представляемого доклада.

В рамках такого представления определены основные параметры и условия рациональности рассматриваемого алгоритма, а также учтены результаты последних разработок по тематике геохронологического трекинга.

Работа выполнена при поддержке РФФИ (проект №19-07-00006).

СПИСОК ЛИТЕРАТУРЫ

1. Ивакин Я. А. Рациональный алгоритм проверки гипотез ретроспективных исследований использования водного транспорта на базе геохронологического трекинга/ Я. А. Ивакин, С. Н. Потапычев, Р. Я. Ивакин // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2019. — Т. 11. — No 3. — С.448–460. DOI: 10.21821/2309-5180-2019-11-3-448-460.
2. Потапычев, С.Н. Геохронологический трекинг – специализированный ГИС-инструментарий исторического исследования [Текст] // Ивакин Я.А., Потапычев С.Н. – Журнал «Историческая информатика. Информационные технологии и математические методы в исторических исследованиях и образовании», № 1-2 -2016; с. 3-11.
3. Ивакин Я. А. Информационная технология геохронологического трекинга для проверки гипотез ретроспективных исследований использования водного транспорта / Я. А. Ивакин, С. В. Потапычев //Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2018. — Т. 10. — № 2. — С. 452–461.

УДК 004.5

ИССЛЕДОВАНИЕ РЫНКА БОТОВ СОЦИАЛЬНЫХ СЕТЕЙ

Коломеец Максим Вадимович
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: kolomeec@comsec.spb.ru

Аннотация. В работе рассматривается русскоязычный сегмент рынка ботов, которые используются для манипуляции репутацией в социальных сетях. Цель этого исследования - увидеть, как соотносятся цена, качество и тип действия ботов в различных социальных сетях, исходя из рыночных предложений.

Ключевые слова: информационная безопасность; анализ социальных сетей; обнаружение ботов; корреляционный анализ.

SOCIAL NETWORK BOTS MARKET RESEARCH

Kolomeets Maxim
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: kolomeec@comsec.spb.ru

Abstract. The study examines the Russian-speaking segment of the market of bots that are used to manipulate reputation in social networks. The purpose of this study is to see how the price, quality and type of action of bots on various social networks correlate, based on market offerings.

Keywords: information security; analysis of social networks; detection of bots; correlation analysis.

Введение. В социальных сетях боты используются для воздействия на репутацию, недобросовестной конкуренции и распространения дезинформации. При этом сформировался вполне устойчивый рынок, на котором существует множество предложений услуг ботов различного качества. Попытки анализировать ботов предпринимались и ранее. Например, типизация ботов по видам уже проводилась исследователями [1] и даже использовалась для оценки эффективности средств обнаружения [2]. Анализ цен ботов Европейского сегмента интернета представлен в отчете [3]. Данное исследование посвящено исследованию рынка ботов русскоязычного сегмента интернета.

Методология исследования. Были проанализированы предложения 7 компаний-продавцов ботов, которые предоставляют услуги аренды, и 1 форум, где продаются боты. Компании были выбраны из русскоязычного сегмента Интернета. Проанализированы предложения аренды на 5 платформах: ВКонтакте, Instagram, Telegram, YouTube и TikTok. Всего было изучено 1 657 предложений аренды и 45 предложений продажи. На основе данных предложений, проведен анализ цен и корреляционный анализ параметров ботов (корреляция Пирсона). Для этого были проанализированы HTML-страницы с описаниями предложений, определены цены на одного бота по каждому предложению, а сами предложения были разделены по: виду социальной сети, качеству ботов, действию ботов. Качество ботов было преобразовано в количественный тип по шкале от 0 (низкое качество) до 1 (высокое качество). Действие ботов было также преобразовано в количественный тип по шкале от 0 (не оставляет цифровых следов) до 1 (оставляет много цифровых следов).

Результаты. Для ботов всех 5-ти социальных сетей присутствует корреляция между ценой и качеством, а также между ценой и действием бота. Наиболее сильно корреляция выражена для Telegram (0.65 и 0.58 соответственно), а наименее сильно для Instagram (0.16 и 0.32 соотв.). Только в Telegram и Youtube присутствует корреляция между качеством и действием (0.47 для Telegram и 0.26 для Youtube).

Заключение. Присутствие корреляции между качеством ботов и ценой, а также между действием ботов и ценой, позволяет косвенно определять стоимость атаки в социальной сети посредством анализа характеристик ботов. Чем сильнее корреляция, тем проще средству обнаружения ботов будет определить цену атаки исходя их качества и действия бота. Кроме того, наличие корреляции между качеством и действием говорит о том, что в таких социальных сетях более сложные действия выполняют боты более высокого качества. В то время как в других социальных сетях, при анализе одних и тех же действий, разновидности ботов будут распространены более равномерно. Данные результаты можно учитывать при проектировании средств обнаружения ботов и определения их характеристик. В будущих исследованиях планируется проследить динамику рынка ботов во времени.

Работа выполнена при финансовой поддержке РНФ (проект № 18-71-10094).

СПИСОК ЛИТЕРАТУРЫ

1. Orabi M., Mouheb D., Aghbari Z. Detection of bots in social media: A systematic review //Information Processing & Management. – 2020. – Vol. 57. – №. 4. – P. 102250.
2. Kolomeets M., Tushkanova O., Levshun D., Chechulin A. Camouflaged bot detection using the friend list //2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP). – IEEE, 2021. – С. 253-259.
3. Singularex NATO StratCom COE, The black market for social media manipulation // NATO Report – 2018.

УДК 004.5

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИНТЕРФЕЙСА ВЗАИМОДЕЙСТВИЯ СИСТЕМА-ПОЛЬЗОВАТЕЛЬ БЕСПИЛОТНОЙ ТРАНСПОРТНОЙ СРЕДЫ УМНОГО ГОРОДА

Коломеец Максим Вадимович, Жернова Ксения Николаевна, Чечулин Андрей Алексеевич
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: {kolomeec,zhernova,chechulin}@comsec.spb.ru

Аннотация. В работе представлена концептуальная модель интерфейса взаимодействия система-пользователь на уровне взаимодействия типов интерфейсов беспилотной транспортной среды умного города. Концептуальная модель показывает пути передачи информации между различными компонентами, с которыми взаимодействует человек или ИИ, а также зависимость этих компонентов друг от друга.

Ключевые слова: человеко-машинное взаимодействие; транспортная среда умного города; интерфейсы взаимодействия.

CONCEPTUAL MODEL OF SYSTEM-USER INTERFACE OF UNMANNED VEHICLE ENVIRONMENT IN A SMART CITY

Kolomeets Maxim, Zhernova Ksenia, Chechulin Andrey
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: {kolomeec,zhernova,chechulin}@comsec.spb.ru

Abstract. The study presents a conceptual model of the system-user interaction interface at the level of interaction between the types of interfaces of the unmanned transport environment of a smart city. The conceptual model shows the ways in which information is transmitted between the various components with which a human or AI interacts, as well as the dependence of these components on each other.

Keywords: computer-human interaction; smart city transport environment; interaction interfaces.

Введение. На уровне взаимодействия типов интерфейсов [1] человек является частью окружения и может взаимодействовать с беспилотным транспортным средством или элементом инфраструктуры посредством использования какого-либо устройства. Для того, чтобы определить пути передачи информации между различными компонентами, с которыми взаимодействует человек или ИИ, а также зависимость этих компонентов друг от друга была построена концептуальная модель.

Концептуальная модель. Можно выделить пять видов взаимодействия между компонентами среды:

1) Окружение → Беспилотное транспортное средство. К взаимодействию данного вида относятся взаимодействия между человеком или пассивным окружением и активными сенсорами транспортного средства. Например, распознавания сенсорами автомобиля пешеходов, дорожных знаков и т.п.

2) Окружение → Инфраструктура. К взаимодействию данного вида относится взаимодействия между человеком или пассивным окружением и активными сенсорами умной транспортная инфраструктуры. Например, оплата человеком проезда, распознавание различных участников дорожного движения и т.п..

3) Транспортное средство ↔ Инфраструктура. К взаимодействию данного вида относится взаимодействия между сенсорами транспортного средства и умными объектами транспортной инфраструктуры. Например, обоюдная передача информации между транспортным средством и шлагбаумом.

4) Транспортное средство ↔ Транспортное средство. К взаимодействию данного вида относится взаимодействия между приемо-передающими модулями одного транспортного средства и приемо-передающими модулями другого транспортного средства (“connected cars”).

5) Инфраструктура ↔ Инфраструктура. К взаимодействию данного вида относится взаимодействие между сенсорами элементов умный транспортной инфраструктуры (“smart city”).

Выводы. При атаках на отдельную не подключённую единицу транспорта другие участники движения и инфраструктура не испытывают последствий. В транспортной среде, где все подключены к сети, атака на одно устройство может оказать влияние на среду всего города [2-3]. Концептуальная модель интерфейса взаимодействия позволяет определить зависимости компонентов беспилотной транспортной среды.

Работа выполнена при финансовой поддержке РФФИ (проект № № 19-29-06099 мк).

СПИСОК ЛИТЕРАТУРЫ

1. Sladkowski A., Pamula W. Intelligent transportation systems – problems and perspectives (Vol. 32). Springer, 2016. 303 pp.
2. Kolomeec M., Zhernova K., Chechulin A. Unmanned Transport Environment Threats // Proceedings of 15th International Conference on Electromechanics and Robotics "Zavalishin's Readings". April 15-18, 2020, Ufa, Russia. Smart Innovation, Systems and Technologies – Springer. 2020. – vol. 187. – pp. 395-408. 2021.
3. Bishop R. Intelligent Vehicle Technology And Trends. Artech House. – 2005. – 362 pp.

УДК 004.056.5

АНАЛИЗ ЗАЩИЩЕННОСТИ РЕСУРСОВ КРИТИЧЕСКИ ВАЖНЫХ ИНФРАСТРУКТУР С ТОЧКИ ЗРЕНИЯ ИХ ДОСТУПНОСТИ: ПОКАЗАТЕЛИ И КРИТЕРИИ

Котенко Игорь Витальевич, Саенко Игорь Борисович, Паращук Игорь Борисович
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: ivkote@comsec.spb.ru, ibsaen@comsec.spb.ru, shchuk@rambler.ru

Аннотация. Предложены подходы к формулировке объема и номенклатуры системы показателей доступности авторизированных пользователей критически важной инфраструктуры к защищаемым информационным, телекоммуникационным и другим ресурсам. Эти показатели описывают пространство параметров защищенности инфраструктур такого класса с точки зрения доступности ресурсов. Рассмотрены частные критерии оценивания временной и топологической доступности, а обобщенный вероятностный критерий оценки доступности авторизированных пользователей и администраторов к защищаемым критически важным ресурсам представлен как совместная условная вероятность выполнения требований по временной и топологической доступности.

Ключевые слова: инфраструктура; критически важный ресурс; показатель; доступность; критерий; анализ; защищенность.

ANALYSIS OF THE SECURITY OF CRITICAL INFRASTRUCTURE RESOURCES IN TERMS OF THEIR AVAILABILITY: INDICATORS AND CRITERIA

Kotenko Igor, Saenko Igor, Parashchuk Igor
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: ivkote@comsec.spb.ru, ibsaen@comsec.spb.ru, shchuk@rambler.ru

Abstract. Approaches to the formulation of the scope and nomenclature of the system of indicators of the availability of authorized users of critical infrastructure to protected information, telecommunications and other resources are proposed. These indicators describe the space of parameters for the security of infrastructures of this class in terms of resource availability. Particular criteria for evaluating temporary and topological availability are considered, and a generalized probabilistic criterion for evaluating the availability of authorized users and administrators to protected critical resources is presented as a joint conditional probability of meeting the requirements for temporary and topological availability.

Keywords: infrastructure, critical resource, indicator, availability, criterion, analysis, security.

Введение. Все больший интерес у аналитиков и практиков в современных условиях вызывает проблема мониторинга и аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности в интересах оценки состояния, поддержки принятия решений и расследования компьютерных инцидентов в критически важных инфраструктурах [1].

Одной из ключевых задач при этом выступает задача разработки моделей, методов, алгоритмов и программных средств оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов на основе аналитической обработки больших массивов гетерогенных данных. Понятие информационных, телекоммуникационных и других критически важных ресурсов, в общем случае, может включать в себя любой класс средств, доступ к которым может нанести ущерб кибербезопасности критически важных инфраструктур.

Рассматривая современную ситуацию, к таковым классам средств могут относиться дата-центры, узлы телекоммуникационных сети, серверы, а также исполняемые файлы, Web-сайты или их отдельные страницы, электронные почтовые сообщения и т.д.

Поэтому вопросы оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов продолжают оставаться актуальными. Эти вопросы могут быть решены, например, на основе использования моделей и методов параллельных вычислений [2, 3]. Иногда могут быть использованы методы нейросетевого моделирования, нечеткой классификации и кластеризации, нечеткой оптимизации и нечеткого логического вывода [4, 5].

Вместе с тем, важнейшим вопросом остается обеспечение защищенности при доступе пользователей к ресурсам системы [6, 7]. Главным, основополагающим этапом при разработке научно-методического инструментария для оперативной оценки защищенности информационных, телекоммуникационных и других критически важных ресурсов, важной стадией аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности, является этап формулировки показателей и критериев оценки защищенности. В рамках аналитической обработки больших массивов гетерогенных данных о событиях кибербезопасности необходимо определить состав векторов показателей защищенности и критерии оценки защищенности критически важных ресурсов, сформулировать их физическую сущность и определить способы их измерений и вычислений.

Например, в составе комплексного векторного показателя защищенности критически важных ресурсов важную роль играет вектор показателей доступности авторизованных пользователей и администраторов системы к этим защищаемым ресурсам. При этом вектор показателей доступности авторизированных пользователей и администраторов системы к защищаемым информационным, телекоммуникационным и другим критически важным ресурсам имеет две составляющие – временную (когда) и топологическую (где).

Временная доступность (своевременность) к критически важным ресурсам рассматривается как способность системы обеспечивать доступ авторизированных пользователей и администраторов к этим защищаемым ресурсам и предоставление им требуемого перечня безопасных информационных, телекоммуникационных и других критически важных ресурсов в установленные сроки.

Так, например, показатель защищенности (с точки зрения своевременности) доступа авторизированных пользователей и администраторов к защищаемому ресурсу может быть выражен через время ожидания доступа к ресурсу. Кроме того, временная доступность авторизированных пользователей и администраторов системы может количественно характеризоваться интенсивностью отказов в доступе к ресурсу [8].

Помимо обеспечения ресурсами за необходимое время, авторизированным пользователям и администраторам системы должна быть обеспечена топологическая доступность к защищаемому информационному, телекоммуникационному или другому критически важному ресурсу, т.е. доступ к защищенным ресурсам в необходимом пользователю месте.

Таким образом, векторный показатель доступности авторизированных пользователей и администраторов системы к защищаемым информационным, телекоммуникационным и другим критически важным ресурсам, характеризующий способность обеспечивать безопасный доступа к этим ресурсам тогда, когда это им необходимо и там, где это необходимо, включает: вектор показателей временной доступности, характеризующий способность системы не препятствовать доступу ее авторизированных пользователей и администраторов к защищаемым критически важным ресурсам в установленные сроки (своевременность предоставления ресурсов); вектор показателей топологической доступности, характеризующий способность системы не препятствовать доступу ее авторизированных пользователей и администраторов к защищаемым информационным, телекоммуникационным и другим критически важным ресурсам в установленном месте их нахождения и при их перемещении.

Критерий оценивания временной доступности может быть задан в вероятностно-временном виде, через вероятность обеспечения своевременного доступа пользователей и администраторов к защищаемым критически важным ресурсам. Критерий оценивания топологической доступности может быть сформулирован аналогичным образом [8].

Заключение. Таким образом, предложен состав и оговорена физическая сущность множества показателей доступности авторизированных пользователей и администраторов сложной управляемой критически важной инфраструктуры к защищаемым информационным, телекоммуникационным и другим ресурсам. Элементы этого множества характеризуют одну из множества граней безопасности – пространство параметров защищенности инфраструктур такого класса с точки зрения доступности ресурсов. Рассмотрены частные критерии оценивания временной и топологической доступности.

Исследования проводятся при поддержке гранта РНФ № 21-71-20078 в СПб ФИЦ РАН (СПИИРАН).

СПИСОК ЛИТЕРАТУРЫ

1. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей. Пер. с англ. – М.: ЛОРИ, 2002. – 350 с.
2. Саенко И.Б., Кушнеревич А.Г., Котенко И.В. Реализация платформы распределенных параллельных вычислений для сбора и предварительной обработки больших данных мониторинга в киберфизических системах // Международный конгресс по информатике: информационные системы и технологии (CSI ST-2016). Материалы международного научного конгресса. Республика Беларусь, Минск, 24-27 октября 2016 г., С. 641-645.
3. Kotenko I., Fedorchenko A., Saenko I., Kushnerevich A. Parallelization of security event correlation based on accounting of event type links // Proceedings of the 25th Euromicro International Conference on Parallel, Distributed and network-based Processing (PDP 2018). Cambridge, UK, March 21-23, 2018. Los Alamitos, California. IEEE Computer Society. 2018. 462-469 pp.
4. Паращук И.Б., Бобрик И.П. Нечеткие множества в задачах анализа сетей связи. – СПб.: ВУС, 2001. – 80 с.
5. Паращук И.Б., Иванов Ю.Н., Романенко П.Г. Нейросетевые методы в задачах моделирования и анализа эффективности функционирования сетей связи. – СПб.: ВАС, 2010. – 103 с.
6. Авраменко В.С. Адаптивный контроль защищенности информации от несанкционированного доступа // Информация и космос. 2010. №3. С. 116-119.
7. Михайличенко Н.В. Проблемы и перспективы обеспечения безопасности центров обработки данных // Региональная информатика и информационная безопасность. Выпуск 4. – СПб.: СПОИСУ, 2017. С. 137-138.
8. Паращук И.Б., Крюкова Е.С., Ясинский С.А. Временная и топологическая доступность пользователей к информационному ресурсу электронных библиотек: показатели и критерии оценивания в рамках системных исследований // Труды ЦНИИС. Санкт-Петербургский филиал. Научно-технический сборник статей. Т. 1. № 9. 2020. – 51 с. С. 8-16.

УДК 004.056

АЛГОРИТМ ФОРМИРОВАНИЯ КОМПОНЕНТНОГО СОСТАВА ЗАЩИЩЕННОЙ СИСТЕМЫ НА ОСНОВЕ МИКРОКОНТРОЛЛЕРОВ

Левшун Дмитрий Сергеевич
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: levshun@comsec.spb.ru

Аннотация. Рассматривается алгоритм формирования компонентного состава, используемый на одном из этапов работы методики проектирования защищенных систем на основе микроконтроллеров. Предлагаемый алгоритм формирует компонентный состав системы в виде множества взаимосвязанных абстрактных элементов устройств и их подэлементов. При этом необходимые для обеспечения защищенности методы и средства защиты или встраиваются в качестве абстрактных элементов и подэлементов, или представляются в виде требований к безопасности, необходимых к учету при эксплуатации системы.

Ключевые слова: система на основе микроконтроллеров; проектирование защищенных систем; формирование компонентного состава; анализ атакующих действий.

ALGORITHM FOR THE FORMATION OF THE COMPONENT COMPOSITION OF A SECURE MICROCONTROLLER-BASED SYSTEM

Levshun Dmitry
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: levshun@comsec.spb.ru

Abstract. An algorithm for the formation of the component composition is considered, which is used at one of the stages of the design methodology for secure microcontroller-based systems. The proposed algorithm forms the component composition of the system in the form of a set of interconnected abstract elements of devices and their sub-elements. At the same time, the methods and means of protection necessary to ensure security of the system are either embedded as abstract elements and sub-elements or presented in the form of security requirements necessary to be taken into account during the operation of the system.

Keywords: microcontroller-based systems; design of secure systems; forming the component composition; attack actions analysis**.**

В настоящее время системы на основе микроконтроллеров – это неотъемлемая часть любой сферы жизнедеятельности человека, что обусловливает критическую важность обеспечения их защищенности [1]. Последствия отказа подобных систем, в том числе связанные с деятельностью злоумышленников, включают в себя как финансовый и репутационный ущерб, так и угрозу жизни и здоровью человека. Одним из возможных направлений атаки является использование уязвимостей, наличие которых в системах на основе микроконтроллеров обусловлено различными факторами.

Наиболее опасные из них – внесенные из-за ошибок на этапе проектирования, т.к. их устранение, как правило, представляет собой трудно решаемую задачу [2]. Особенно когда устранение ошибки подразумевает изменения в аппаратной или программной составляющих отдельных устройств, в то время как их фирм-производителей уже не существует. Распространенность таких уязвимостей связана с тем, что системы на основе микроконтроллеров зачастую проектируются без участия специалистов в области безопасности с применением слабозащищенных протоколов передачи данных, выходом в сеть Интернет и использованием непроверенного на наличие ошибок кода.

Решение данной проблемы является важной задачей, именно поэтому были разработаны и применяются на практике различные методики проектирования. Часть из них сфокусирована на программном обеспечении, часть на аппаратном, а некоторые – на узкоспециализированных областях приложения. Ключевая проблема подобных решений – сфокусированность на отдельных аспектах безопасности, что обуславливает их неприменимость для обеспечения защищенности систем на основе микроконтроллеров в целом [3]. При этом объединение отдельных решений является сложной задачей ввиду их несовместимости. Это связано с тем, что в основе каждой методики лежит собственная модель системы или ее элемента, представленная во внутреннем формате. Именно поэтому сложно или даже невозможно преобразовать одну конкретную модель в другую без потерь значимых данных [4].

В рамках данной работы представлен алгоритм формирования компонентного состава защищенных систем на основе микроконтроллеров, используемый на одном из этапов работы разработанной автором методики проектирования [5]. Рассмотрим выходные и выходные данные, а также процесс работы алгоритма более подробно.

Входные данные алгоритма:

– список устройств системы: задается в виде кортежа таблицы реляционной базы данных, состоящего из уникального идентификатора и названия устройства, например (1, «server»);

– требования к устройствам системы: задаются в виде кортежей таблицы реляционной базы данных, состоящих из уникального идентификатора и текста требования, например (11, «wireless access point») или (37, «parking detection algorithm»);

– доступные устройству уровни коммуникаций: задаются в виде кортежей таблицы реляционной базы данных, состоящих из уникального идентификатора и уровня коммуникации, например (1, «electronic component to microcontroller»);

– список возможных атакующих действий: задаются в виде кортежей таблицы реляционной базы данных, состоящих из уникального идентификатора, наименования и описания атакующего действия, например (10, «cad», «cryptographic analysis of transmitted data»).

Процесс работы алгоритма для каждого устройства может быть представлен следующим образом:

Преобразование требований к устройству в абстрактную основу и абстрактные элементы. Например, основой могут быть: (1, «one-board computer»), (2, «connected microcontrollers»), (3, «microcontroller»).

Преобразование требований к устройству в абстрактные элементы устройства.

Извлечение абстрактных элементов, связанных с основой устройства, полученной на шаге 1.

Извлечение абстрактных элементов, связанных с элементами, полученными на шаге 2 и 3.

Извлечение абстрактных подэлементов, связанных с элементами, полученными на шагах 2, 3 и 4.

Извлечение атакующих действий, которые могут быть направлены на устройство в соответствии с доступными ему уровнями коммуникации.

Извлечение атакующих действий, которые могут быть направлены на устройство в соответствии с абстрактными элементами и подэлементами.

Выявление актуальных атакующих действий на основе пересечения атакующих действий, полученных на шагах 7 и 8 с атакующими действиями, полученными на основе параметров атакующего.

Извлечение необходимых методов и средств защиты в виде элементов безопасности в соответствии с актуальными атакующими действиями, полученными на шаге 8.

Преобразование элементов безопасности в абстрактные элементы и поделементы, рекомендации безопасности для устройства и системы.

В дальнейшем, рекомендации для системы, полученные в рамках формирования компонентного состава каждого из устройств, объединяются и представляются в виде требований к безопасности, необходимых к учету при эксплуатации системы. Например, (2, «to educate operators and users of the system about social engineering attacks»).

Выходные данные алгоритма:

– абстрактные элементы устройств: задаются в виде кортежей таблицы реляционной базы данных, состоящих из уникального идентификатора и наименования элемента, например (1, «32-bit operating system») или (17, «microcontroller for electronic components»);

– абстрактные подэлементы устройств: задаются в виде кортежей таблицы реляционной базы данных, состоящих из уникального идентификатора и наименования подэлемента, например (6, «application-database connection») или (14, «obstacles detection algorithm»);

– рекомендации для обеспечения защищенности устройств системы: задаются в виде кортежей таблицы реляционной базы данных, состоящих из уникального идентификатора и описания рекомендации, например, (1, «to hide monitoring sensors of this device»).

Новизна предложенного алгоритма заключается в работе с абстрактным представлением системы на основе микроконтроллеров, извлечении абстрактных элементов и их подэлементов на основе предъявляемых к устройству требований, его основы и уже извлеченных элементов. При этом элементы защиты представляются в качестве абстрактных элементов и подэлементов, что позволяет сделать их неотъемлемой частью компонентного состава системы. Если же элемент безопасности не может быть использован в качестве компонента, он представляется в виде рекомендаций, необходимых к учету при эксплуатации системы.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90082.

СПИСОК ЛИТЕРАТУРЫ

1. Левшун Д.С., Гайфулина Д.А., Чечулин А.А., Котенко И.В. Проблемные вопросы информационной безопасности киберфизических систем // Информатика и автоматизация. Т. 19. № 5. 2020. С. 1050-1088. ISSN 2078-9181 (2078-9599). DOI: 10.15622/ia.2020.19.5.6.
2. Левшун Д.С., Чечулин А.А., Котенко И.В. Жизненный цикл разработки защищенных систем на основе встроенных устройств // Защита информации. Инсайд, № 4(76), 2017. С. 53-59.
3. Левшун Д.С., Котенко И.В., Чечулин А.А. Методика проектирования и верификации защищенных киберфизических систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1. Естественные и технические науки. 2019, № 4. С. 19-22.
4. Левшун Д.С., Чечулин А.А., Котенко И.В. Комплексная модель защищенных киберфизических систем для их проектирования и верификации // Труды учебных заведений связи. 2019. Т. 5. № 4. С. 114–123. DOI: 10.31854/1813-324X-2019-5-4-114-123.
5. Dmitry Levshun, Igor Kotenko, Andrey Chechulin. The application of the methodology for secure cyber-physical systems design to improve the semi-natural model of the railway infrastructure // Microprocessors and Microsystems, November 2020, P. 103482. ISSN 0141-9331. DOI: 10.1016/j.micpro.2020.103482.

УДК 004.056

МОДЕЛЬ АТАК ДЛЯ ДЕЦЕНТРАЛИЗОВАННОЙ САМООРГАНИЗУЮЩЕЙСЯ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

Мелешко Алексей Викторович

Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)

14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия

e-mail: meleshko.a@iias.spb.su

Аннотация. В работе представлена модель атак для беспроводной сенсорной сети. Рассматривается децентрализованная самоорганизующаяся беспроводная сенсорная сеть, свойства которой могут порождать новые виды атак, которые не нереализуемы для в рамках обыкновенных сетей. Кроме того, рассматриваемая сеть может быть подвержена и атакам, которые справедливы для централизованных сетей с фиксированной

топологией. Поэтому в данной работе рассматривается систематизация различных атак – строится модель атак на самоорганизующиеся децентрализованные беспроводные сенсорные сети.

Ключевые слова: модель атак; децентрализация; самоорганизация; беспроводная сенсорная сеть.

ATTACK MODEL FOR A DECENTRALIZED SELF-ORGANIZING WIRELESS SENSOR NETWORK

Meleshko Aleksei
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: meleshko.a@iias.spb.su

Abstract. The paper presents an attack model for a wireless sensor network. A decentralized self-organizing wireless sensor network is considered, the properties of which can generate new types of attacks that are not unrealizable for ordinary networks. In addition, the network in question can be susceptible to attacks that are valid for centralized networks with a fixed topology. Therefore, in this paper, the systematization of various attacks is considered – a model of attacks on self-organizing decentralized wireless sensor networks is being built.

Keywords: attack model; decentralization; self-organization; wireless sensor network.

Развитие беспроводных сенсорных сетей (БСС) на сегодняшний день делает их персептивными для применения в различных сферах деятельности. Промышленные процессы, транспортная промышленность, контроль физических процессов среды – лишь не полный список сфер, где могут быть применимы БСС. Подверженность БСС различным атакам обусловлена возможно работой узлов в незащищенной физической среде, а также критическим характером объектов, на которых они применяются. В настоящей работе рассматриваются БСС, обладающие свойствами самоорганизации и децентрализации. Данные свойства также могут являться уязвимым местом, которое эксплуатируют злоумышленники. Для построения эффективной системы защиты таких БСС необходимо понимать какие атаки реализуемы в зависимости от расположения БСС, источники этих атак и возможные последствия. То есть необходимо построить модель атак, опираясь на которую, выбираются средства защиты. Таким образом, именно построению модели атак посвящена данная работа.

Для начала, ориентируясь на конкретную БСС, необходимо определить возможности злоумышленника. БСС мониторинга загрязнения окружающего воздуха может быть расположена в отрытой местности, например в черте города или на охраняемом производстве. В случае расположения на охраняемой территории возможности злоумышленника будут ограничены и воздействие на узлы БСС будет возможно только удаленно. А если узлы БСС расположены в открытой местности, то доступ к узлам не ограничен, и злоумышленник может воздействовать на них физически, подключаться своим оборудованием или же изменять физические параметры, которые измеряет сенсор узла.

Также на успех атак на БСС влияет используемый протокол общения между сенсорами. Если используется общеизвестный протокол, например ZigBee, то злоумышленнику будет проще внедрять ложные узлы. Если использовать собственный протокол передачи или децентрализации сети, то отсутствие общедоступной информации о нем будет препятствием для атакующего.

Отдельные проблемы в области безопасности вносят свойства самоорганизации и децентрализации сети. Самоорганизация подразумевает динамическое формирование структуры сети, которое может меняться во времени, а также динамическое выстраивание маршрутов в сети между источником и получателем через другие, расположенные между ними узлы сети. То есть свойство самоорганизации позволяет добавлять новые узлы «на лету», а также менять маршруты передачи пакетов данных. Таким образом злоумышленник может подключиться к сети под видом легитимного узла. Например, если используется протокол ZigBee, то злоумышленнику необходимо подобрать атрибут PAN_ID для сети, который он может получить, подключившись к любому расположенному в открытой местности узлу. Децентрализация предполагает распределение функций обработки, безопасности, хранения данных на несколько узлов сети, причем данное распределение может меняться. Например, в определенный момент времени один узел проводит обработку информации, а в другой момент времени уже может проводить анализ защищенности БСС. В таком случае подключив свой узел к сети, злоумышленник может получить одну из функций и вмешиваться в работу сети.

В целом атаки на БСС, также как и атаки на другие системы, можно разделить на атаки, направленные на нарушения одного или несколько свойств безопасности: конфиденциальности, доступности, целостности. Например, атака отказа в обслуживании (DoS) направлена на нарушение доступности сети. Или атака типа Tampering, направленна на фальсификацию одного или нескольких узлов и относится к атакам на нарушение конфиденциальности и целостности. Далее будут рассмотрены конкретные атаки на БСС мониторинга загрязненности воздуха.

В статье [1] авторы выделили наиболее частые атаки на БСС, такие как атаки связывания (linking attack), атака «человек по середине» и атаки распределенного отказа в обслуживании. Атаки связывания направлены на идентификацию каких-либо данных из анонимного набора, сопоставляя их с исходной информацией. То есть применительно к системе мониторинга воздуха, не зная точного местоположения сенсора с конкретным идентификатором можно его вычислить, например сопоставляя показания других сенсоров, местоположение которых известно. Данную атаку можно отнести к атакам на конфиденциальность.

Атака «человек посередине» направлена на нарушение конфиденциальности, а в некоторых случаях и целостности передаваемых данных. При такой атаке на пути данных от источника к получателю имеется третье лицо, которое просматривает передаваемую информацию и может её модифицировать. В рассматриваемой БСС данный вид атак реализуем из-за наличия свойства самоорганизации, то есть злоумышленник присоединяется к сети под видом легитимного узла и проводит мониторинг передаваемой информации. А в определенных случаях даже получить функции обработки или обеспечения безопасности (эксплуатация децентрализации). Подвидом атаки «человек посередине» можно выделить атаку «человек в конце (man-in-the-end)» и просто как-то воздействовать на сеть, передавая ложные показания.

Атаки отказа в обслуживании являются довольно большим классом атак и направлены на разрушение нормальной работы сети вплоть до полного вывода ей из строя. Применительно к рассматриваемой БСС данная атака может выражаться рядом более мелких атак, таких как:

– зашумление (jamming) канала связи и как следствие потеря доступности одного или нескольких узлов сети;

– взлом одного или нескольких узлов, выполняющих различные функции, например обработки информации или функции безопасности. Общее нарушение функциональности сети из-за некорректной работы отдельных узлов. Можно отнести к атакам на конфиденциальность и целостность данных в сети;

– атаки отказа от сна – направлены на вывод автономно работающих узлов из спящего режима. В виду ограниченности энергоресурсов узлы не постоянно передают информацию и иногда уходят в спящий режим. Данная атака не позволяет им это делать и в результате узлы могут вовсе перестать работать из-за полного исчерпания энергии.

Отдельно можно рассмотреть атаки физического разрушения узлов, которые реализуемы в случае открытого их расположения. Из-за свойства самоорганизации данная атака может быть не сразу замечена и принята за легитимное отключение узла. Также злоумышленник может получить доступ к узлу, который обеспечивает функции детектирования аномалий и вмешиваться в данный процесс.

В результате можно сделать вывод, что применительно к БСС мониторинга загрязненности окружающего воздуха злоумышленник может иметь практически полный доступ к узлам сети, проводить эксплуатацию свойств самоорганизации и децентрализации БСС и реализовать любую из перечисленных в работе атак, направленных на нарушение доступности, конфиденциальности и целостности. В качестве мер противодействия можно выделить следующие: использование защищенных протоколов самоорганизации и децентрализации, физическая защита узлов сети – например, аппаратное отключение портов с целью предотвращения нелегитимного подключения к узлам, использование механизмов интеллектуального анализа данных от сенсоров сети, которые могут определить наличие злоумышленника в БСС.

Работа выполнена в СПб ФИЦ РАН при финансовой поддержке РФФИ (проект № 19-07-00953).

СПИСОК ЛИТЕРАТУРЫ

1. Guerrero-Sanchez A.E., Rivas-Araiza E.A., Gonzalez-Cordoba J. L., Toledano-Ayala M., Takacs A. Blockchain Mechanism and Symmetric Encryption in A Wireless Sensor Network / Sensors, 2020, v. 20, n. 2798, pp. 1-20, doi: 10.3390/s20102798.

УДК 004.056

ПОДХОД К ПОСТРОЕНИЮ БЕЗОПАСНОЙ САМООРГАНИЗУЮЩЕЙСЯ ДЕЦЕНТРАЛИЗОВАННОЙ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

Мелешко Алексей Викторович

Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)

14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия

e-mail: meleshko.a@iias.spb.su

Аннотация. В работе рассматривается подход к построению безопасных беспроводных сетей, обладающих свойствами самоорганизации и децентрализации. Механизм децентрализации позволяет динамически распределять функции обработки данных, а также функции обеспечения безопасности на несколько узлов сети, что снижает нагрузку на узел координатор и повышает общее качество исполнения данных функций. Механизм самоорганизации дает возможность динамически масштабировать сеть и выполнять функции перераспределения функций узлов.

Ключевые слова: беспроводная сенсорная сеть; децентрализация; самоорганизующаяся сеть; безопасность беспроводных сенсорных сетей.

APPROACH TO DESIGNING A SAFE SELF-ORGANIZING DECENTRALIZED WIRELESS SENSOR NETWORK

Meleshko Aleksei

St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)

39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia

e-mail: meleshko.a@iias.spb.su

Abstract. The paper considers an approach to building secure wireless networks with self-organization and decentralization properties. The decentralization mechanism allows you to dynamically distribute data processing functions and security functions to several network nodes, which reduces the load on the coordinator node and improves the overall quality of these functions. The self-organization mechanism makes it possible to dynamically scale the network and perform the functions of redistributing the functions of nodes.

Keywords: wireless sensor network; decentralization; self-organizing network; security of wireless sensor networks.

Развитие сфер применения беспроводных сенсорных сетей (БСС) ставит перед разработчиками новые требования к таким сетям и принципам их построения. БСС – это сети, в которых узлами являются сенсоры, осуществляющие измерение определенных параметров. Применяться такие сети могут для контроля производственных процессов, интеллектуального транспорта, контроля загрязнения окружающей среды. Среди требований к построению БСС можно выделить следующие: масштабируемость, возможность динамической смены состава узлов и их местоположения, безопасность данных, которые передаются по БСС. Для удовлетворения данных требований следует закладывать в БСС свойства самоорганизации и децентрализации.

Под самоорганизацией понимается меняющаяся во времени структура сети, её состав, а также динамическое выстраивание маршрутов между источником и получателем. Данное свойство позволяет быстро расширять или уменьшать количество узлов в сети, так как узлы могут добавляться автоматически. При смене местоположения узлов также автоматически происходит перераспределение маршрутов в сети. Децентрализация обуславливает введение определенных ролей для нескольких узлов. То есть обработка информации производится не на одном центральном узле, а на нескольких, что может помочь повысить производительность. Кроме того, функции анализа безопасности БСС также могут быть распределены на несколько узлов, что позволяет повысить безопасности сети, так как даже при компрометации одного узла, анализ безопасности дублируется на другие. Таким образом применение механизмов децентрализации позволяет снять нагрузку с одного центрального узла и перераспределить её на другие, что положительно сказывается на производительности и ресурсопотреблении, и повысить общий уровень безопасности БСС.

Был рассмотрен ряд работ, посвященных применению децентрализованного подхода в БСС. Большинство из них направлены на создание децентрализованных методов анализа безопасности БСС, а не на построение БСС, работающих в децентрализованном режиме. Например, статья [1] описывает метод обнаружения повреждений в БСС, который основан на механизме децентрализации. Авторы используют одномерные сверточные нейронные сети. Такая нейронная сеть обучается индивидуально для каждого узла так, что она работает только с его локальными данными. В качестве подтверждения применимости предложенного подхода авторы провели ряд экспериментов на лабораторном стенде, который включает в себя ряд современных БСС. Также есть ряд работ описывающих протокол децентрализованной идентификации данных в БСС. Например, статья [2] описывает схему децентрализации идентификации данных для БСС. Данные на каждом узле обрабатываются отдельно с целью получения предварительных результатов локальной структурной идентификации. Далее они передаются на базовую станцию, где происходит их объединение. Для объединения используется Байесовский подход слияния.

Однако, в представленных работах узлы сети проводят некоторые функции предобработки локально, основной анализ все равно выполняет центральный узел. Также в явном виде рассмотрение атак, которые эксплуатируют свойства децентрализации или самоорганизации не приводится. В настоящей работе предлагается схема построения самоорганизующейся децентрализованной БСС, которая позволяет не только выполнять действия по предобработке локально на узлах, а также позволяет распределить функции анализа всех данных в сети и её безопасности на несколько узлов.

Предлагаемая БСС предназначена для сбора и обработки физических и пользовательских данных в области мониторинга загрязненности атмосферного воздуха, а также в других областях приложения. Узлами сети являются устройства, имеющие в своем составе следующие элементы: сенсоры для изменения показателей, микроконтроллер или одноплатный компьютер Raspberry PI – для возможности ограниченной предобработки данных, а также для возможности выполнения других функций, модуль для связи с другими узлами БСС. Использование протокола ZigBee версии 2 позволяет реализовать функции самоорганизации БСС.

Для реализации свойства децентрализации предлагается протокол децентрализации, которые реализует введение ролей узлов, каждая из которых отвечает за выполнение определенных функций сети:

– сбор и предобработка данных – собор данных со всех узлов сети, реализация их предобработку (фильтрация, нормализация, агрегация);

– хранение данных за последний промежуток времени t;

– анализ защищенности – выявление аномалий на основе интеллектуального анализа данных со всех узлов сети. Например, учитываются показания сенсоров, местоположения узлов, скорость ветра и т.п., в том числе данные из внешних источников, баз данных.

Каждый узел независимо производит выявление аномалий локально – на основе данных только с него самого. Например, контроль предельных, пороговых значений для отдельных сенсоров, скорость изменения показаний, или максимальное отклонение показаний за некоторый промежуток времени. И результаты такого анализа защищенности отправляются на узлы, выполняющие функции анализа защищенности, в качестве дополнительных данных, необходимых для комплексного анализа защищенности. К преимуществам такого

протокола децентрализации можно отнести возможность динамического перераспределения управляющих и прикладных функций сети в условиях ограничений на вычислительные и другие аппаратные ресурсы узлов. Это позволяет для БСС, функционирующих в условиях отсутствия централизованного устройства, формировать сенсорные сети с высокими вычислительными возможностями и параллельной децентрализованной обработкой данных.

В результате был предложен подход к построению самоорганизующейся децентрализованной БСС, который призван улучшить производительность и безопасность сетей. В дальнейшем планируется программно-аппаратная реализация БСС, а также реализация функций безопасности и анализ эффективности предлагаемого решения. Анализируется производительность и эффективность противостояния различным атакам, например атакам отказа в обслуживании (DoS) или атакам внедрения ложного узла сети.

Работа выполнена в СПб ФИЦ РАН при финансовой поддержке РФФИ (проект № 19-07-00953).

СПИСОК ЛИТЕРАТУРЫ

1. Avci O., Abdeljaber O., Kiranyaz S., Hussein M., Inman D. J. Wireless and real-time structural damage detection: A novel decentralized method for wireless sensor networks / Journal of Sound and Vibration, 2018, v. 424, pp. 158–172, doi: 10.1016/j.jsv.2018.03.008.
2. Huang, K., Yuen, K. Online dual□rate decentralized structural identification for wireless sensor networks / Structural Control and Health Monitoring, 2019, doi:10.1002/stc.2453

УДК 654.9

СПОСОБ УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ ПРОГРАММНОГО ИЗДЕЛИЯ

Олимпиев Алексей Александрович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mail: aao_82@mail.ru

Аннотация. Предлагается способ управления жизненным циклом программного изделия, базирующийся на методологии метауправления функциональностью и предназначенный для повышения качества программного изделия с точки зрения информационной безопасности и использования без участия разработчиков.

Ключевые слова: метауправление функциональностью; управление жизненным циклом программного изделия; адаптивное программное обеспечение.

THE METHOD OF SOFTWARE LIFECYRCLE MANAGEMENT

Olimpiev Aleksey
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: aao_82@mail.ru

Abstract. The method for managing the lifecycle of a software product is proposed. Method is based on the methodology of meta-control of functionality and designed to improve the quality of a software product from the point of view of information security and use without the participation of developers.

Keywords: metacontrol of functionality; software lifecyrcle control; adaptive software.

Базовым принципом управления качеством изделия, который применяется во многих наиболее развитых предприятиях, является принцип жизненного цикла. Данный принцип позволяет выделить в процессе управления качеством изделия ряд этапов, на которых происходит существенное изменение состояния изделия, начиная от замысла и материализации прототипа до утилизации конечного продукта [1]. С научной точки зрения управление жизненным циклом можно определить как метод управления качеством, направленный на систематизацию процессов, которые переводят объект управления из одного состояния в другое. Данный метод позволяет разрабатывать различные способы управления, отличающиеся структурой этапов жизненного цикла, объектами управления, на которых сфокусировано внимание субъекта управления, и, следовательно, набором критериев управления.

Так, например, для управления жизненным циклом телекоммуникаций в качестве приоритетного объекта управления могут быть выбраны услуги связи, либо телекоммуникационные ресурсы. Для системы образования объектом управления может быть отдельная дисциплина, либо формируемая компетенция. Аналогичным образом можно говорить и об управлении жизненным циклом программного изделия.

В основу предлагаемого способа положена методология управления функциональностью, которая позволяет рассмотреть любое программное изделие как совокупность инвариантной программной части и языка описания функциональности (ЯОФ), предназначенного для адаптации программного изделия к изменениям условий функционирования [2]. В качестве приоритетного объекта управления предлагается выбрать язык описания функциональности, который будет качественно изменяться во времени, что в конечном итоге позволит решить две проблемы: проблему наличия уязвимостей в программном изделии с метауправлением и проблему использования такого изделия конечным пользователем без участия разработчика.

Жизненный цикл программного изделия может быть определен следующей последовательностью этапов:

– первый этап может быть назван «Начальная разработка адаптивного программного обеспечения (АПО)» [3], заключающийся в выборе базового языка описания функциональности, в качестве которого на данном этапе рекомендуется брать интерпретируемый язык общего назначения (ИЯОН);

– на втором этапе «Расширение функциональности АПО» происходит формирование библиотеки ресурсов на ИЯОН, которые содержат типовые структуры данных и алгоритмы, применяемые в различных условиях использования АПО;

– третий этап «Оптимизация», который заключается, во-первых, в выделении из всей совокупности библиотек на ИЯОН прикладных ресурсов (структур данных и алгоритмов) и ресурсов общего назначения, во-вторых, в переносе ресурсов общего назначения на уровень интерпретатора — в контекст интерпретации ЯОФ;

– четвертый этап «Обобщение», заключается в представлении прикладных ресурсов на декларативном проблемно-ориентированном языке сверхвысокого уровня (ДПОЯСУ), полностью заменяющем базовый ИЯОН;

– пятый этап «Визуализация» на котором ДПОЯСУ заменяется на комбинацию языка диаграмм и диалоговых форм с небольшими алгоритмическими вставками, предназначенными для уточнения отдельных прикладных расчетов.

Таким образом, предлагаемый способ должен обеспечить создание человеко-ориентированного адаптируемого программного обеспечения, которое может быть многократно повторно использовано при условии строгого разделения прикладного уровня и уровня общего назначения. Применение данного способа требует разработки объективного набора показателей качества языков описания функциональности.

СПИСОК ЛИТЕРАТУРЫ

1. Косяков А., Свит У. и др. Системная инженерия. Принципы и практика. Пер. с англ. под ред. В. К. Батоврина. - М.: ДМК Пресс, 2017. - 624 с.
2. Шерстюк Ю. М. Основы метауправления функциональностью в информационных системах. – СПб.: СПИИРАН, 2000. – 155 с.
3. Олимпиев А. А. Методика синтеза системы оперативно-технического мониторинга с метауправлением функциональностью. Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII 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, 2018. Т. 2. С. 505-510 с.

УДК 004.056

ДЕЦЕНТРАЛИЗОВАННЫЕ ФИНАНСОВЫЕ СЕРВИСЫ: ОБЩИЙ АЛГОРИТМ АТАКИ

Помогалова Альбина Владимировна[1], Донсков Евгений Андреевич[2], Котенко Игорь Витальевич[2]
[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: a.l.b.i.n.a@bk.ru, radion2002@gmail.com, ivkote@comsec.spb.ru

Аннотация. Блокчейн-сфера децентрализованных финансов предлагает все большее и большее количество разнообразных банковских услуг, которые представляют из себя открытые и прозрачные децентрализованные инструменты. Мгновенные займы, биржевые торги активами и другие инструменты позволяют использовать некогда исключительно централизованные функции в децентрализованной сети. Но подобные инструменты также могут быть подвержены атакам. Атаки на сервисы децентрализованных финансов по-прежнему являются одними из наиболее убыточных. В рамках работы производится анализ существующих сервисов и атак на эти сервисы. В работе разрабатывается общий алгоритм проведения атак на сервисы одного вида.

Ключевые слова: децентрализованные финансы; мгновенные займы; DEX; атаки, блокчейн, Эфириум.

DECENTRALIZED FINANCE SERVICES: GENERAL ATTACK ALGORITHM

Pomogalova Albina[1], Donskov Evgeny[2], Kotenko Igor[2]
[1] The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: a.l.b.i.n.a@bk.ru, radion2002@gmail.com, ivkote@comsec.spb.ru

Abstract. The decentralized finance blockchain offers a growing variety of banking services which are open and transparent decentralized instruments. Flash loans, stock trades and other instruments allow for the use of previously highly centralized functions in a decentralized network. But such instruments can also be attacked. Attacks on decentralized finance services continue to be among the most costly. The paper analyzes existing services and attacks against these services. The paper develops a common algorithm for attacking decentralized finance services of the same type.

Keywords: DeFi; decentralized finance; flash loans; DEX; attacks, blockchain, Ethereum.

Возможность уйти от привычных форм централизованной финансовой среды является одной из самых привлекательных идей для всего человечества. Возможность независимо, быстро, самостоятельно и без привлечения третьей стороны проводить переводы и платежи казалась ранее невозможной. Но

с распространением идей технологии блокчейн это стало реальностью. Более того, сегодняшний прогресс позволяет не только производить оплату услуг, но и дает доступ к процедурам, которые кажутся невозможными без большого количества контролирующих элементов и привлечения посторонних сотрудников. Речь идет о финансовых операциях, которые предполагают кредиты, разнопарные обмены, вклады и даже мгновенные займы. Настоящей революцией на рынке децентрализованных услуг стали децентрализованные финансы (DeFi) [1]. DeFi — это финансовые инструменты, которые представляют из себя сервисы и приложения, созданные на базе блокчейн-платформ. Наиболее популярной платформой для реализации различных подобных инструментов является платформа Ethereum. Центральной задачей DeFi является замена существующих форм централизованных финансов (существующих банков и кредитных организаций) смарт-контрактами с открытым исходным кодом [5]. Преимуществом подобных разработок является открытость исходных данных, что заведомо является более доверительным подходом. Любой участник децентрализованной системы может ознакомиться с логикой работы приложения и изучить его на предмет наличия скрытых угроз, опасных комбинаций кода и других подозрительных, скрытых от глаз элементов.

Подобный подход, безусловно, предполагает революцию в сфере финансов и возможный полный отказ от существующих финансовых институтов. Но открытость исходного кода, которая является гарантией правильных намерений создателя сервиса, может оказать и негативное влияние. Под негативным влиянием подразумевается возможность осуществления ряда атак в случае уязвимостей или нарушенной логики программы. Логические, структурные, синтаксические ошибки провоцируют мгновенные атаки, которые практически невозможно остановить. Единственным способом остановки подобных кибер-атак является аналитика проведенного нападения и выявление строк кода, которые могут быть подвержены атаке, то есть вносят двойственность действий. Элементарным примером подобных атак являются атаки переполнения переменных, которым был подвержен наиболее популярный язык смарт-контрактов Solidity до выпуска обновленной 8-й версии языка [3].

Наиболее популярными и уязвимыми проектами на сегодняшний день являются мгновенные займы и платформы, позволяющие обменивать пары типа токен-Эфир, а также приобретать токены или Эфиры. Так, за 2020 год было проведено более 13 разнообразных атак в DeFi-сфере и сфере децентрализованных бирж с суммарным ущербом более 400 миллионов долларов. А наиболее подверженным атакам местом стали платформы, предоставляющие услуги мгновенных займов.

Основным преимуществом мгновенных займов является возможность вызова смарт-контрактов в рамках проведения одной разрешенной транзакции. При правильном проведении транзакции возможно получить выгоду от обмена взятых в рамках займа средств и последующей мгновенной продажи, а также вернуть размер займа.

Общий алгоритм работы мгновенных кредитов включает в себя следующие действия:

1) Разработка смарт-контракта, включающего в себя необходимую последовательность действий с заемными средствами (обращения к пулам, биржам и т.д.).

2) Функцию заема средств и возврата, а также их вызовы.

3) Проверку смарт-контракта на предмет отсутствия злонамеренных действий относительно заемщика активов.

4) Запуск смарт-контракта, выдачу заемных средств, последовательное выполнение всех строк смарт-контракта, возврат средств заемщику.

В общем случае, алгоритм процедуры выдачи и возврата мгновенного займа включает в себя действия, предусмотренные в рамках смарт-контракта [2]. Так, пользователю выдается заемная сумма, которая находится на счету смарт-контракта до конца прохождения по функциям строк кода смарт-контракта. После завершения действий, описанных в смарт-контракте, производится возврат средств. В случае недостаточного количества средств на смарт-контракте по результату проведенных действий транзакция отменяется.

Таким образом, в рамках работы смарт-контрактов мгновенных займов соблюдается строгая логика, которая требует возврата не меньшего значения, чем то, которое было выдано под заем.

В одной из работ приводятся современные use cases, которые позволяют использовать мгновенные займы для получения выгоды. Также в работе авторы выделяют существующие атаки, которые могут быть произведены с использованием мгновенных займов.

Но наибольшие риски для блокчейн-платформ представляет применение мгновенных займов для взаимодействия с системами с пулами торгуемых пар рассмотренного ранее DeFi сервиса. В ходе исследования атак, с использованием мгновенных займов, авторы работы выделили общий сценарий проведения атаки, которая успешно применяется с февраля 2018 года и до сих пор является одной из самых опасных атак в блокчейн-сфере.

Для выявления общего сценария проведения DeFi атак и обнаружения сходств в рамках работы были проанализированы 3 самые масштабные атаки, нанесшие огромный финансовый ущерб [4]. Для анализа были использованы записи о проведении транзакций, представленные на официальном онлайн-сервисе Etherscan, который был разработан для мониторинга транзакций сети Ethereum, а также официальную информацию от компаний, которым был нанесен ущерб. Это позволило составить подробные схемы действий злоумышленников, которые отражают все действия, предпринятые во время совершения атаки.

Первый этап атаки включает в себя получение средств с использованием сторонних сервисов, что включает в себя мгновенные займы и кредиты, но не ограничивается ими. В данном случае могут быть использованы как мгновенные займы, так и сервисы, которые предполагают залог в виде стейблкоинов. Второй этап подразумевает использование DeFi сервисов, один или более из которых содержат обнаруженную атакующим уязвимость. Атакующий использует эксплойт, настроенный на использование обнаруженной

уязвимости, тем самым проводя манипуляции с DeFi-сервисами с целью получения избыточного количества активов. Следует учесть, что в данной атаке используются DeFi-сервисы категории обменников активов, то есть биржи с комбинациями пулов. Это позволяет добиться резких ценовых перепадов в пулах и использовать уязвимый DeFi-сервис с целью невыгодной для сервиса торговли. Третий, заключительный, этап подразумевает возврат залоговых или заемных активов и выведение оставшихся в ходе манипуляций избыточных средств на сторонние электронные кошельки. Анализ алгоритма атаки позволит выделить общие правила ее проведения и основные зависимости, что будет использовано при разработке механизма анализа уровня безопасности смарт-контрактов.

В рамках представленной работы был проведен анализ децентрализованных финансовых сервисов, выделены категории сервисов. Выполнен сравнительный анализ децентрализованных финансовых сервисов и классических криптовалютных блокчейн-сервисов. Проанализированы и разработаны общие алгоритмы работы децентрализованных финансовых сервисов двух категорий. Выделены уязвимые области сервисов, проанализированы существующие атаки. Исследованы и проанализированы 3 крупнейших атаки в области DeFi сервисов. Выявлены частные особенности атак, а также разработан общий алгоритм проведения атак данной категории. Проведенные исследования показали, что на данный момент наиболее уязвимыми являются DeFi сервисы, которые позволяют продолжать взаимодействие с сервисом в случае невыгодного обмена криптовалютными средствами. Одним из возможных способов предотвращения совершения данного типа атак является проверка смарт-контрактов мгновенных займов на предмет обращения к DeFi сервисам в ходе проведения транзакции займа. В последующих исследованиях предполагается исследовать возможные способы противодействия рассмотренным классам атак с использованием методологии моделирования кибератак [6, 7].

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Gudgeon L., Perez D., Harz D., Livshits B., Gervais A. The Decentralized Financial Crisis // 2020 Crypto Valley Conference on Blockchain Technology (CVCBT), Rotkreuz, Switzerland, 2020, P.1-15, doi: 10.1109/CVCBT50464.2020.00005.
2. Chen W., Wu J., Zheng Z., Chen C., Zhou Y. Market Manipulation of Bitcoin: Evidence from Mining the Mt. Gox Transaction Network // IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, Paris, France, 2019, P.964-972, doi: 10.1109/INFOCOM.2019.8737364.
3. Solidity documentation (2021). Available at: https://docs.soliditylang.org/en/v0.8.1/ (accessed 07 February 2021).
4. Victor F., Hagemann T. Cryptocurrency Pump and Dump Schemes: Quantification and Detection // 2019 International Conference on Data Mining Workshops (ICDMW), Beijing, China, 2019, P. 244-251, doi: 10.1109/ICDMW.2019.00045.
5. Kumar M., Nikhil N., Singh R. Decentralising Finance using Decentralised Blockchain Oracles // 2020 International Conference for Emerging Technology (INCET), Belgaum, India, 2020, P.1-4, doi: 10.1109/INCET49848.2020.9154123.
6. Котенко И.В., Десницкий В.А., Чечулин А.А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд, 2011, № 3, С.68-75.
7. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // SECRYPT 2006. International Conference on Security and Cryptography. Proceedings. Portugal. 7-10 August 2006. P.339-344.

УДК 004.056

ИССЛЕДОВАНИЕ РАСПРЕДЕЛЕНИЯ УЯЗВИМОСТЕЙ СИСТЕМ УПРАВЛЕНИЯ, ИСПОЛЬЗУЕМЫХ НА ОБЪЕКТАХ КРИТИЧЕСКИ ВАЖНОЙ ИНФРАСТРУКТУРЫ

Попова Валерия Олеговна [1], Чечулин Андрей Алексеевич[1,2]

[1] Университет ИТМО

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

[2] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)

14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия

e-mails: lerapopova236@gmail.com, andreych@bk.ru

Аннотация. В работе осуществляется оценка картины распределения уязвимостей систем управления, наиболее часто используемых на объектах критически важной инфраструктуры. Цель исследования - выделить основные тренды в распределении уязвимостей уже совершенных кибератак и предсказать наиболее вероятные уязвимые точки для осуществления новых атак, наиболее критичные уязвимости, что, в свою очередь, поможет снизить риски безопасности как уже существующих, так и проектируемых систем.

Ключевые слова: объекты критически важной инфраструктуры; анализ уязвимостей; открытые базы данных.

INVESTIGATION OF THE VULNERABILITIES DISTRIBUTION IN THE MANAGEMENT SYSTEMS OF CRITICAL INFRASTRUCTURE

Popova Valeria[1], Chechulin Andrei[1,2]

[1] ITMO University

49 Kronverksky Av, St. Petersburg, 197101, Russia

[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)

39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia

e-mails: lerapopova236@gmail.com, andreych@bk.ru

Abstract. The paper assesses the distribution pattern of vulnerabilities of management systems that are most often used at critical infrastructure facilities. The purpose of the study is to identify the main trends in the distribution of

vulnerabilities of already committed cyber-attacks and predict the most likely vulnerabilities for new attacks, the most critical vulnerabilities, which, in turn, will help reduce the security risks of both existing and projected systems.

Keywords*:* critical infrastructure objects; vulnerability analysis; open databases.

Введение. В настоящее время трендом в развитии автоматизированных систем управления на ядерных объектах критически важной инфраструктуры является усложнение структуры и взаимодействия между компонентами. Обеспечение кибербезопасности таких объектов является ключевой задачей на всех этапах эксплуатации. Для снижения риска нарушения безопасности путем осуществления кибератак необходимо получить картину атакующих действий, для чего целесообразно определить уязвимости потенциальных целевых объектов атаки. Для достижения данной цели предлагаем использовать открытые базы уязвимостей, в частности, базу уязвимостей NationalVulnerabilityDatabase (NVD) [1].

Методология исследования.Для достижения целей использованы отрытые базы данных уязвимостей. В частности, национальная база данных уязвимостей NVD. База уязвимостей NVD - американское правительственное хранилище данных уязвимостей, основанное на стандартах правительства США. Данные, содержащиеся в этом хранилище, позволяют автоматизировать управление уязвимостями, оценку безопасности и соответствие требованиям.С целью сравнения и наглядного представления специфики атак на оборудование ядерных объектов критически важной инфраструктуры выбрано оборудование компании Microsoft в качестве исходного образца.

Результаты. В результате проведенного анализа базы данных [2] были получены результаты по распределению кибератак на оборудование, используемое на объектах критически важной инфраструктуры, по временным критериям, по атакуемым типам оборудования, по тяжести последствий атак, по типам нарушения целостности информации, по типу доступа, по критерию получения прав доступа к системе.

Заключение. Интерпретация полученных результатов позволила составить достаточно полную картину по трендам распределения кибератак на объекты критически важной инфраструктуры [3], помогла выявить основные направления атак и уязвимости, используемы злоумышленниками.

Работа выполнена при частичной финансовой поддержке РФФИ (проект 19-29-06099 мк).

СПИСОК ЛИТЕРАТУРЫ

1. Федорченко А.В., Чечулин А.А., Котенко И.В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей // Информационно-управляющие системы, 2014, №5, С.72-79. ISSN 1684-8853.
2. Дружинин Е. Карпов И. Уязвимости компонентов АСУ ТП. Отчет за первое полугодие 2019 года .– Ростелеком Солар.:, 2019. - 32 с.
3. Безопасность АСУ ТП. Итоги 2017 года. – PositiveTechnologies:, 2017. - 12 с.

УДК 004.056

АНАЛИЗ ЗАЩИЩЕННОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ГРАФОВ АТАК

Пучков Владимир Викторович, Котенко Игорь Витальевич
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: puchkov-81@bk.ru, ivkote@comsec.spb.ru

Аннотация. Рассматриваются возможности по использованию графов атак для анализа защищенности киберфизических систем.

Ключевые слова: киберфизическая система; граф атак; анализ защищенности.

ANALYSIS OF THE SECURITY OF CYBER-PHYSICAL SYSTEMS USING ATTACK GRAPHS

Puchkov Vladimir, Kotenko Igor
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: puchkov-81@bk.ru, ivkote@comsec.spb.ru

Abstract. The possibility of using attack graphs to analyze the security of a cyber-physical system is considered.

Keywords: cyberphysical system; attack graph; security analysis.

Введение. В настоящее время киберфизические системы (КФС) становятся основополагающей частью нашей цивилизации. Энергетика, безопасность, промышленность - этот список можно продолжать достаточно долго. И в каждой области КФС находят свое применение, облегчая выполнение поставленных задач. Согласно исследованиям компании ARM, приведенным в [1], число устройств подключенных к Интернету к 2035 году составит порядка 1 трлн. и в дальнейшем будет увеличиваться со скоростью около 20% в год. В связи с глобальным развитием автоматизации, можно сделать вывод, что большинство этих устройств будут иметь все характеристики КФС. Соответственно точный и достоверный анализ безопасности такой системы является необходимостью с момента проектирования и в дальнейшем на всех уровнях ее функционирования.

Методики анализа защищенности КФС на основе графов атак и выбор адекватных защитных мер позволят значительно уменьшить уровень угроз защищаемой системы. Постоянно контролируемые показатели

защищенности, актуальные именно для данной системы, будут своевременно обновляться с учетом поступающей информации о событиях в системе. Такая организация защиты позволит своевременно реагировать на возникающие угрозы.

В настоящей работе производится анализ работ, в которых описываются действующие методики анализа защищенности на основе графов атак. Необходимо отметить, что большинство работ по данной теме были написаны достаточно давно и датируются в основном 2006-2014 годами, и, соответственно, несколько устарели. Также хочется обратить внимание на то, что встречается недостаточно работ именно по анализу защищенности КФС, например, в работе [2] рассматривается безопасность компьютерных систем, в статье [3] авторы сосредоточены на сетевой безопасности, а в источнике [4] графы атак используются для расчета безопасной конфигурации проектируемой сети.

Обзор. На стадии проектирования могут использоваться различные методы и способы анализа защищенности КФС. Это могут быть качественные или количественные методики анализа риска, методики на базе теории нечетких множеств и т.д. Однако большой интерес для качественной оценки рисков и защищенности системы представляют методы, использующие имитацию действий атакующего на основе графов атак, дальнейшую проверку этих действий и выработку наиболее подходящих метрик безопасности защищаемой системы.

Генерация графа атаки - процесс, который включает себя обработку информации об уязвимостях, информацию о приложениях, определение условий достижимости среди сетевых узлов и применение алгоритма построения основного графа.

Граф атак представляет возможные способы, с помощью которых потенциальный злоумышленник может проникнуть в целевую сеть, используя ряд уязвимостей на различных узлах сети и получая новые привилегии на каждом шаге. Другими словами, графы атак используются для проведения анализа защищенности рассматриваемой системы и определения возможности использования злоумышленником уязвимостей в процессе построения сложной многовекторной атаки [4].

После успешного использования уязвимости на хосте злоумышленник получает на нем дополнительные привилегии и либо продолжает атаковать следующие хосты с исходного, либо пытается повысить свои привилегии на этом хосте, используя полученные дополнительные уязвимости. Однако необходимо понимать, что наличие уязвимости не всегда будет условием успешной атаки. Для определения успешности возможной атаки вводится такое понятие, как вероятность успешной атаки. Данный показатель рассчитывается в зависимости от квалификации атакующего, сложности рассматриваемой системы и сложности использования уязвимости.

Ниже приведем основные виды графов атак.

Полный граф. Включает в себя все пути, которые может использовать атакующий для компрометации сети. Однако происходит экспоненциальный рост сложности графа в процессе роста сложности сети.

Предиктивный граф. В процессе построения новый узел добавляется в случае, если ни один предок данного узла еще не использовал ту же уязвимость, что и новый узел. Этот граф строится гораздо быстрее полного графа. Нужно отметить, что наряду с достоинствами этот граф все еще имеет лишние структуры.

Граф со множеством предусловий. Он состоит из трех видов узлов: состояние, предусловие, уязвимость. Отличается скоростью построения. Его можно преобразовать в полный или предиктивный граф. Однако его недостатком является недостаточная наглядность.

Для генерации графа атак обычно необходимо иметь набор начальных привилегий. Конечные узлы возможного графа атаки являются целевыми привилегиями (их злоумышленник стремится получить в конце). Можно выделить полный граф атаки (в нем выделяются все возможные пути атаки от начальных привилегий до привилегий цели) и частичный граф (в нем показывается часть этих возможных путей).

Граф атаки может быть динамическим. В этом случае его узлы и ребра могут обновляться при установке новых продуктов или удалении уже существующих продуктов на целевых хостах сети. В этом случае новые уязвимости могут добавляться к хостам или уже существующие уязвимости могут удаляться. Иногда граф атаки в качестве узлов может использовать информационные активы. Использование такого актива может привести к некоторым привилегиям, полученным на хосте или любом другом хосте, который косвенно доступен через этот хост. В качестве примера для такого информационного ресурса можно указать файлы cookie.

В процессе эксплуатации КФС используются как активные, так и пассивные методики анализа уязвимости.

Применение графов атак дает возможность объединить преимущества обоих методик, чем значительно повышается эффективность анализа защищенности [6].

В работах [7] авторы предлагают реализацию анализа защищенности за счет построения общего графа атак, который будет моделировать действия, атакующего с учетом параметров защищаемой сети, а также целей и уровня знаний и нахождения нарушителя. Это позволит выполнить оценку защищенности как от внешних, так и внутренних злоумышленников.

Заключение. Графы атак могут использоваться для анализа безопасности КФС как в автономном режиме, так и в режиме онлайн. В случае автономной работы, не вмешиваясь в работу целевой сети они могут использоваться для определения оптимальных положений брандмауэров и систем обнаружения вторжений, вычисления показателей оценки безопасности сети [8, 9]. В том случае, если сбор информации из целевой сети происходит в режиме, близком к реальному времени, графы атак могут быть использованы для анализа заражения, корреляции журналов [10, 11] и анализа оценки ситуации безопасности для целевой системы.

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Перри Л. Архитектура Интернета Вещей. М.: ДМК, 2019. С. 21–38, 205–208, 354–384Ronzhin A. Trends in Development of UAV-UGV Cooperation Approaches in Precision Agriculture // Interactive Collaborative Robotics. – 2018. – С. 213.
2. Котенко И.В., Полубелова О.В., Саенко И.Б., Чечулин А.А. Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности, Т.8, № 2, 2012. С.100-108.
3. Nmap, Nmap security scanner, <http://nmap.org/>; 2015. Noel S, Robertson E, Jajodia S. Correlating intrusion events and building attack scenarios through attack graph distances / ACSAC. IEEE Computer Society; 2004. P. 350–9.
4. Pamula J., Jajodia S., Ammann P., Swarup V. A weakest-adversary security metric for network configuration security analysis // Proceedings of the 2Nd ACM workshop on quality of protection, QoP '06. New York, NY, USA: ACM; 2006. doi:10.1145/1179494.1179502.
5. Kaynar K. A taxonomy for attack graph generation and usage in network security // Turkish Advanced Research Center (GT-ARC), TU Berlin, Ernst Reuter Platz 7, 10587 Berlin, Germany. ARTICLE IN PRESS journal of information security and applications 2016.
6. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // SECRYPT 2006. International Conference on Security and Cryptography. Proceedings. Portugal. 7-10 August 2006. P.339-344.
7. Котенко И.В., Десницкий В.А., Чечулин А.А. Исследование технологии проектирования безопасных встроенных систем в проекте Европейского сообщества SecFutur // Защита информации. Инсайд, 2011, № 3, С.68-75.
8. LeMay E., Ford M., Keefe K., Sanders W., Muehrcke C. Model-based security metrics using adversary view security evaluation (advise) // 2011 eighth international conference on Quantitative evaluation of systems (QEST), 2011. p.191–200. doi:10.1109/QEST.2011.34.
9. Wang L., Albanese M., Jajodia S. Attack graph and network hardening // Network hardening, Springer Briefs in computer science. Springer International Publishing; 2014, P.15–22.
10. Kotenko I, Doynikova E. Security assessment of computer networks based on attack graphs and security events. In: Mahendra M, Neuhold E, Tjoa A, You I, editors. Lecture notes in computer science, vol. 8407. Information and communication technology. Springer Berlin Heidelberg; 2014. P. 462–71.
11. Roschke S., Cheng F., Meinel C. A new alert correlation algorithm based on attack graph // Proceedings of the 4th international conference on computational intelligence in security for information systems, CISIS'11. Berlin, Heidelberg: Springer-Verlag, 2011. P.58–67.

УДК 004.056.5

ПОДХОДЫ К УСТРАНЕНИЮ НЕОПРЕДЕЛЕННОСТИ ВХОДНОЙ ИНФОРМАЦИИ БЕЗОПАСНОСТИ В ЗАДАЧАХ АНАЛИЗА ЗАЩИЩЕННОСТИ СИСТЕМ ИНДУСТРИАЛЬНОГО ИНТЕРНЕТА ВЕЩЕЙ

Федорченко Елена Владимировна, Паращук Игорь Борисович
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: doynikova@comsec.spb.ru, shchuk@rambler.ru

Аннотация. Рассмотрены некоторые виды нестохастической неопределенности входной информации безопасности, которая имеет место в задачах анализа защищенности систем индустриального Интернета вещей в различных условиях обстановки. Предложены общие подходы к оценке показателей защищенности систем такого класса в условиях неоднозначности (нечеткости) и недостаточности (неполноты и противоречивости) исходных данных. Эти подходы ориентированы на применение методов теории нечетких множеств, нейросетевых методов и позволяют повысить достоверность и оперативность анализа защищенности систем индустриального Интернета вещей в различных условиях функционирования.

Ключевые слова: индустриальный Интернет вещей; неопределенность; анализ; защищенность; показатель; нечеткость; противоречивость.

APPROACHES TO ELIMINATING THE UNCERTAINTY OF SECURITY INPUT INFORMATION IN THE TASKS OF ANALYZING THE SECURITY OF INDUSTRIAL INTERNET OF THINGS SYSTEMS

Fedorchenko Elena, Parashchuk Igor
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: doynikova@comsec.spb.ru, shchuk@rambler.ru

Abstract. Some types of non-stochastic uncertainty of security input information, which occurs in the problems of analyzing the security of industrial Internet of Things systems in various environmental conditions, are considered. General approaches to assessing the security indicators of systems of this class in the conditions of ambiguity (vagueness) and insufficiency (incompleteness and inconsistency) of the source data are proposed. These approaches are focused on the application of methods of the theory of fuzzy sets, neural network methods and allow to increase the reliability and efficiency of the analysis of the security of industrial Internet of Things systems in various operating conditions.

Keywords: industrial Internet of Things; uncertainty; analysis; security; indicator; fuzziness; inconsistency.

Введение. Системы индустриального Интернета вещей (ИИВ) являются важным направлением развития мировой информационно-телекоммуникационной инфраструктуры. Данные системы представляют собой комплексные программно-аппаратные промышленные системы, обеспечивающие эффективное взаимодействие объектов (машин, устройств, механизмов), компьютеров и человека. Они обеспечивают интеллектуальные производственные процессы с использованием новейших методов анализа данных для получения новых качественных результатов индустриальных операций [1]. Разнообразие и сложность компонентов ИИВ обуславливает существование проблем разработки методов и средств анализа их защищенности [2, 3].

Подобные проблемы решаются путем научных исследований и практических разработок в рамках частных подзадач: формирования множества объектов и метрик анализа защищенности ИИВ; анализа журналов событий объектов ИИВ и существующих средств мониторинга защищенности ИИВ; идентификации источников и значений параметров входной информации безопасности; синтеза множества иерархически взаимосвязанных метрик безопасности (показателей защищенности), позволяющих оценивать защищенность ИИВ; анализа онтологий метрик безопасности ИИВ в интересах оценки защищенности системы.

Важной задачей продолжает оставаться разработка методов и средств достоверного и оперативного анализа защищенности систем ИИВ. К информации безопасности, являющейся исходными данными для анализа защищенности систем ИИВ, относят входную информацию об объектах коммуникации, об уязвимостях, об инцидентах безопасности, контрмерах, конфигурациях, политиках безопасности и т.д. [3].

Известно, что в классической постановке анализ защищенности систем ИИВ осуществляется в условиях детерминированности, вероятности и неопределенности значений параметров подобной входной информации безопасности, при этом детерминированные условия реально встречаются редко. Вероятностные условия более реальны, они характеризуются тем, что каждому параметру входной информации безопасности соответствует вполне определенное распределение вероятностей его состояния на множестве возможных состояний. В неопределенных условиях, наиболее характерных для систем ИИВ, показатели их защищенности могут иметь случайный характер, но в отличие от вероятностных условий, закон их распределения неизвестен [4].

Специалистам в области оценки информационной безопасности сложных систем различного назначения очевидна актуальность задачи разработки алгоритмов анализа защищенности систем ИИВ, учитывающих неопределенность исходных данных – входной информации безопасности, неопределенность параметров текущего состояния защищенности систем такого класса, вызванные различного вида воздействиями и другие виды неопределенности. Исследование подходов к анализу защищенности систем, исследование видов и характера неопределенности, имеющей место при таком анализе, показывают, что на современном этапе недостаточно развиты алгоритмы анализа в условиях нестохастической неопределенности, а именно, неоднозначности (нечеткости) и недостаточности (неполноты и противоречивости) исходной информации для анализа защищенности систем ИИВ.

Выход из этой ситуации нам видится в использовании «нечетких» и «противоречивых» оценок защищенности. При этом «нечеткие» оценки защищенности принимают значения в рамках множества лингвистических переменных, описывающих уровни (значения) показателей защищенности: плохая – удовлетворительная – хорошая – отличная защищенность. Степень соответствия тому или иному значению лингвистических переменных определяется в рамках методов теории нечетких множеств на основе функций принадлежности и нечетких отношений [5-7].

Приведенные качественные оценки защищенности называют «нечеткими». Основная идея «нечеткого» анализа заключается в том, что вместо определенных понятий, выражающих классы (множества) оценок защищенности с жестко заданными границами, вводятся понятия (например, плохая – удовлетворительная – хорошая – отличная защищенность), объемы которых расплывчаты в следующем смысле: имеются оценки показателей защищенности, которые попадают под данное понятие и являются элементами «жесткой» части его объема; оценки показателей защищенности, которые полностью не попадают под понятие, и результаты анализа, которые подпадают под понятие с определенной степенью [5, 7].

Помимо этого, «нечеткий» подход к решению задачи многокритериального анализа защищенности и выбора защитных мер заключается в выражении общей цели функционирования подсистемы безопасности системы ИИВ в виде иерархии подцелей. Здесь на нижнем уровне иерархии находятся частные цели, связываемые с элементарными критериями, которые позволяют оценить объекты из заданного множества. При этом для анализа защищенности и выбора защитных мер осуществляется операция свертки над нечеткими множествами, объединяющими частные цели. В итоге получим нечеткие оценки защищенности.

Вторым ключевым аспектом нестохастической неопределенности является недостаточность (неполнота, противоречивость) исходных данных, которая может быть решена на базе «противоречивых» оценок защищенности. Для решения таких задач нашли свое успешное применение методы теории искусственных нейронных сетей [8]. Такой подход использует экстраполирующие нейронные сети, являющиеся разновидностью известных моделей ассоциативной памяти. Предлагаемый подход расширяет возможности существующих искусственных нейронных сетей, используемых в интересах поддержки принятия решений по контролю за системами ИИВ, позволяя принимать обоснованные решения по анализу защищенности.

Заключение. Таким образом, проведен анализ особенностей, уровней и характера неопределенности, влияющей на анализ защищенности систем ИИВ в различных условиях функционирования. Предпринята попытка сформулировать общие подходы к оценке показателей защищенности систем такого класса в условиях нестохастической неопределенности, а именно, неоднозначности (нечеткости) и недостаточности (неполноты и противоречивости) исходных данных – входной информации безопасности. Использование данных подходов создает предпосылки для повышения достоверности и оперативности анализа защищенности систем ИИВ в различных условиях обстановки.

Исследования проводятся при финансовой поддержке РФФИ (проект 19-07-01246) в СПб ФИЦ РАН (СПИИРАН).

СПИСОК ЛИТЕРАТУРЫ

1. Страшун Ю.П. Технические средства автоматизации и управления на основе IIoT/IoT. Учебное пособие. М.: Лань, 2020. – 76 с.
2. European Union Agency for Cybersecurity (ENISA). Good practices for Security of Internet of Things in the context of Smart Manufacturing. 2018. – P. 11.
3. Дойникова Е.В. Классификация и анализ целей кибератак в системах Индустриального Интернета вещей. // Информационная безопасность

регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2019 г.: Материалы конференции. / СПОИСУ. СПб.: 2019. 596 с., С. 116-117.
4. Бушуев С.Н., Осадчий А.И., Фролов В.М. Теоретические основы создания информационно-технических систем. – СПб.: ВАС, 1998. – 404 с.
5. Паращук И.Б., Бобрик И.П. Нечеткие множества в задачах анализа сетей связи. – СПб.: ВУС, 2001. – 80 с.
6. Kotenko I., Parashchuk I. Decomposition and Formulation of System of Features of Harmful Information Based on Fuzzy Relationships // 2019 International Russian Automation Conference (RusAutoCon), Sochi, Russia, / IEEE Xplore Digital Library: Browse Conferences (2019). Vol. 8867588, 2019. pp. 1-5.
7. Авраменко В.С., Бобрешов-Шишов Д.И., Беденков В.Н., Маликов А.В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная конференция. Т.3. – СПб.: СПБГУТ, 2017. С.13-18.
8. Паращук И.Б., Иванов Ю.Н., Романенко П.Г. Нейросетевые методы в задачах моделирования и анализа эффективности функционирования сетей связи. / Учебно-методическое пособие. – СПб.: ВАС, 2010. – 103 с.

УДК 004.056

СИСТЕМА ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ОТ КИБЕР АТАК И ВЫБОРА ЗАЩИТНЫХ МЕР С ИСПОЛЬЗОВАНИЕМ СЕМАНТИЧЕСКОЙ МОДЕЛИ ДАННЫХ И МЕТРИК

Федорченко Елена Владимировна, Федорченко Андрей Владимирович, Новикова Евгения Сергеевна, Браницкий Александр Александрович, Мелешко Алексей Викторович, Пучков Владимир Викторович
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: {doynikova, fedorchenko, novikova, branitskiy, meleshko}@comsec.spb.ru, puchkov-81@bk.ru

Аннотация. В докладе предлагается система оценивания защищенности от кибер атак и выбора защитных мер. Она представляет собой программное средство, позволяющее сформировать семантическую модель метрик и данных для анализируемой системы с использованием обобщенной модели путем сбора и обработки условно статических данных об анализируемой системе, расширить ее путем определения новых концептов и сущностей онтологии путем сбора и анализа динамических данных, и использующее ее для оценивания защищенности и выбора контрмер путем вывода и вычисления ряда метрик. Лежащая в основе программного средства семантическая модель обеспечивает прозрачность и объяснимость формируемых оценок и решений по реагированию. Программное средство использует методы обработки больших данных при анализе динамических данных. Применимость программного средства для заявленных целей протестирована на примере компонентов индустриального Интернета вещей.

Ключевые слова: программное средство; оценивание защищенности; кибер атака; защитные меры; семантическая модель; метрики; данные.

SYSTEM FOR SECURITY ASSESSMENT AND COUNERMEASURE SELECTION USING SEMANTIC MODEL OF DATA AND METRICS

Fedorchenko Elena, Fedorchenko Andrey, Novikova Evgenia, Branitskiy Alexander, Meleshko Alexey, Puchkov Vladimir
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: {doynikova, fedorchenko, novikova, branitskiy, meleshko}@comsec.spb.ru, puchkov-81@bk.ru

Abstract. The research proposes a system for assessing the security against cyber-attacks and for selecting the security measures. It is a software tool that allows generating a semantic model of metrics and data for the analyzed system using a generalized model by collecting and processing conditionally static data about the analyzed system, extending it by defining new concepts and entities of ontology by collecting and analyzing dynamic data, and uses it to assess security and select countermeasures by deriving and calculating a number of metrics. The semantic model underlying the software tool provides transparency and explainability of the obtaines assessments and response decisions. The tool uses big data processing techniques to analyze dynamic data. The applicability of the software tool for the stated purposes is tested on the example of the components of the industrial Internet of things.

Keywords: software; security assessment; cyber-attack; countermeasures; semantic model; metrics; data.

Введение. В настоящее время системы мониторинга защищенности от кибер атак собирают большие объемы данных, которые можно использовать в целях повышения защищенности информационных систем и своевременного выбора и применения защитных мер. Для этого необходимо разрабатывать методы, методики и программные инструменты обработки и анализа таких данных с заявленными целями. В данной работе описывается разработанное программное средство, учитывающее связи между данными и метриками защищенности при выполнении оценивания защищенности и выбора защитных мер за счет формирования семантической модели метрик и данных.

Система оценивания защищенности от кибер атак и выбора защитных мер. Разработанное программное средство реализовано на языке Python. В качестве входных данных используется обобщенная семантическая модель метрик и данных, реализованная с использованием языка OWL, а также условно статические данные об известных конфигурациях анализируемой системы, программном и аппаратном обеспечении, уязвимостях, атаках и защитных мерах, и динамические данные о событиях, происходящих в системе. Программное средство использует методы обработки больших данных при анализе динамических данных о событиях.

Архитектура разработанного программного средства включает компонент сбора и предобработки условно статических данных, компонент сбора и предобработки динамических данных, компонент формирования семантической модели метрик и данных для анализируемой системы на основе условно статических данных, компонент расширения семантической модели на основе динамических данных, компонент оценивания защищенности, компонент выбора защитных мер и базу данных, содержащую результаты работы компонентов [1].

Компонент оценивания защищенности реализует методику оценивания защищенности на основе семантической модели метрик и данных [2]. Обобщенная семантическая модель объединяет полный набор метрик от первичных до интегральных, их связи между собой и с объектами предметной области. Итоговая модель для анализируемой системы может включать не полный набор первичных метрик, в зависимости от которого в рамках методики выбирается предобученная модель (классификатор), используемая для вычисления интегральных метрик. Компонент выбора защитных мер реализует методику выбора защитных мер путем логического вывода на основе семантической модели метрик и данных с использованием связей между объектами анализируемой системы и их уязвимостями/возможными атаками и применимыми и доступными защитными мерами [3].

В процессе работы программное средство вначале собирает статическую информацию из открытых источников, а также информацию, добавляемую экспертами, и на ее основе заполняет обобщенную онтологию для получения онтологии, объединяющей данные и метрики (первичные) для анализируемой системы. На следующем этапе динамические данные обрабатываются для определения и уточнения объектов системы, в том числе программного и аппаратного обеспечения и связей между ним, и расширения онтологии. Далее, сформированная семантическая модель используется при оценивании защищенности для вывода и вычисления интегральных метрик защищенности в зависимости от доступных первичных метрик с использованием предобученных классификаторов. На последнем этапе, семантическая модель используется для выбора защитных мер для повышения защищенности анализируемой системы.

Применимость программного средства для заявленных целей протестирована на примере компонентов индустриального Интернета вещей.

Заключение. В докладе предложена и рассмотрена система оценивания защищенности и выбора защитных мер, реализованная в виде программного средства, использующего в процессе работы семантическую модель метрик и данных. Отличительной особенностью предлагаемой системы является прозрачность и объяснимость результатов. Дальнейших исследования будут направлены на теоретическую и экспериментальную оценку программного средства и лежащих в его основе методик.

Работа выполнена при финансовой поддержке РФФИ (проект 19-07-01246 А).

СПИСОК ЛИТЕРАТУРЫ

1. Федорченко Е.В., Федорченко А.В., Быстров И.С. Архитектура системы оценивания защищенности от кибер атак и выбора защитных мер с использованием семантической модели данных и метрик // X Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании" (АПИНО-2021)». Санкт-Петербург, 24-25 февраля 2021 г. Сборник научных статей. 2021.
2. Дойникова Е.В., Федорченко А.В., Котенко И.В., Новикова Е.С. Методика оценивания защищенности на основе семантической модели метрик и данных // Вопросы кибербезопасности. 2021. N 1(41). С. 29-40. DOI: 10.21681/2311-3456-2021-1-29-40.
3. Дойникова Е.В., Федорченко А.В., Гайфулина Д.А. Методика выбора мер противодействия кибератакам с использованием онтологии метрик безопасности // XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020 г., часть 1., С.137-138.

УДК 004.056

АНАЛИЗ РАСШИРЕННОЙ МОДЕЛИ «CYBER KILL CHAIN» ДЛЯ АТРИБУЦИИ НАРУШИТЕЛЕЙ КИБЕРБЕЗОПАСНОСТИ ПРИ РЕАЛИЗАЦИИ ЦЕЛЕВЫХ АТАК НА ОБЪЕКТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Хмыров Семен Сергеевич, Котенко Игорь Витальевич
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: khmyrov.s.s@gmail.com, ivkote1@mail.ru

Аннотация. Атрибуция кибернарушителя является многоцелевой задачей. В работе выполнен анализ расширенной модели Cyber Kill Chain для атрибуции нарушителей кибербезопасности при реализации целевых атак на объекты критической инфраструктуры.

Ключевые слова: целевые атаки; критическая инфраструктура; атрибуция кибернарушителя; кибербезопасность КИИ; Cyber Kill Chain.

ANALYSIS OF THE EXTENDED «CYBER KILL CHAIN» MODEL FOR ATTRIBUTING CYBER SECURITY OFFENDERS UNDER IMPLEMENTATION OF TARGETED ATTACKS AGAINST CRITICAL INFRASTRUCTURE OBJECTS

Khmyrov Semyon, Kotenko Igor
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: khmyrov.s.s@gmail.com, ivkote1@mail.ru

Abstract. Attributing a cyber-intruder is a multi-purpose task. The paper analyzes an extended Cyber Kill Chain model for attribution of cybersecurity violators when implementing targeted attacks against critical infrastructure facilities.

Keywords: targeted attacks; critical infrastructure; attribution of a cyber-intruder; cybersecurity of CII; Cyber Kill Chain.

Введение. Развитие механизмов обнаружения и предупреждения информационных угроз и ликвидация последствий их проявления, вызванных информационно-техническим воздействием (ИТВ) на объекты критической информационной инфраструктуры (КИИ), является одной из приоритетных национальных задач при повышении защищенности и устойчивости функционирования КИИ [1, 2]. К данным механизмам напрямую относится атрибуция нарушителей кибербезопасности, т.е. процесс идентификации происхождения и источника кибератаки с целью установления злоумышленника или группы злоумышленников [3, 4].

К наиболее характерному типу ИТВ относится – целевая кибератака или развитая устойчивая угроза (APT) [5]. APT - это сложная, многоуровневая атака, выполняемая преимущественно на информационно-телекоммуникационную инфраструктуру военных и государственных объектов [6]. Данные объекты в большинстве случаев ведущими государствами мира относятся к КИИ [7]. Как правило, кибернарушитель обладает значительными ресурсами, которые позволяют ему создавать возможности для достижения целей посредством различных векторов нападения [8, 9].

Цель работы анализ модели Cyber Kill Chain и формирование набора атрибутов кибернарушителя.

Для атрибуции кибернарушителя при реализации целевых атак на объекты КИИ, необходимо расследовать несколько инцидентов, сопоставить факты и осуществить анализ специфики и индивидуальных манер кибернарушителя. В ходе APT выполняется структурированная последовательность шагов, цепочка действий. Применение модели Cyber Kill Chain позволяет последовательно исследовать APT [10].

Модель Cyber Kill Chain. Базовая модель [11, 12] включает в себя (предполагает) семь стадий, необходимых для достижения поставленной цели, представленных ниже.

Шаг 1. Разведка. Осуществляется выбор и сбор информации о атакуемой цели. Устанавливается организационная структура, применяемые информационные технологии, средства обеспечения информационной безопасности. Полученные данные выступают в роли базы знаний для проектирования следующего шага.

Шаг 2. Вооружение. Определение способа компрометации целевого объекта. Использование существующего или разработка собственного уникального вредоносного программного обеспечения (ПО), эксплойта.

Шаг 3. Доставка. Внедрение, распространение применяемого решения для компрометации целевого объекта.

Шаг 4. Заражение. Активация вредоносного решения на скомпрометированном целевом объекте.

Шаг 5. Инсталляция. Развертывание полноценных сервисов, модулей для дальнейшей эксплуатации и закрепления в скомпрометированной информационной инфраструктуре.

Шаг 6. Получение управления. Администрирование вредоносного решения, его обновление, получение нового функционала, реализация полного спектра команд для достижения поставленных целей.

Шаг 7. Выполнение действий. Уничтожение, шифрование или кража данных. Достижение иных поставленных целей [13]. Каждый из элементов включает описание систематического процесса на данном этапе и применение наиболее популярных векторов атаки для достижения цели. Также в модели существуют индикаторы и жизненные циклы индикатора. С учетом постоянно растущих векторов атак и инструментария кибернарушителя, число шагов может быть увеличено.

Для повышения эффективности анализа APT и результата атрибуции, базовую модель можно расширить, добавив стадии: «шифрование»; «запутывание»; «уничтожение следов». В докладе рассматриваются элементы данной расширенной модели, включая возможность использования злоумышленником различных автоматизированных средств, в том числе онтологических [14].

Исследуя данные шаги, эксперты и аналитики смогут понять фазы APT, источники сбора данных, векторы атаки, применяемые методики кибернарушителями, используемый инструментарий, сформировать профиль кибернарушителя, метрики для своевременного определения цепочки атак и определить возможность атрибуции.

Полученные в ходе анализа каждого жизненного цикла кибератаки данные, в дальнейшем могут применяться для формирования датасета профилей APT. Шаг 1 (разведка), подразумевает изучение злоумышленником веб-сайтов, рассылку писем, работу с базами – данных на специализированных ресурсах даркнета, социальную инженерию. На основе этого можно определить следующий набор атрибутов: IP адрес, URL страницы, заголовок страницы, реферер страницы, браузер (тип, версия), операционная система (тип, версия), устройство, часовой пояс, язык, HTTP запросы, страна, город, провайдер, разрешение экрана, глубина цвета, mail, server, domain и т.п. Таким образом, можно выявить активность относительно целевого объекта, определить степень риска (возможность будущей атаки) и попытаться совершить атрибуцию ведущего разведку (его причастность к APT).

Также можно разработать меры защиты и противодействия на каждом шаге реализации APT. Практическим примером является поэтапный анализ кибератак Stuxnet и WannaCry с дальнейшей атрибуцией и выработкой контрмер [15, 16]. Для повышения уровня защищённости целевого объекта в [17] предлагается использовать матрицу дополнительных контрмер на каждом шаге цепочки атаки. Цель данной

матрицы - усиление защитных мер, направленных на нейтрализацию кибернарушителя в более ранней стадии цепочки вторжения, снижение возможного ущерба, минимизация временных и финансовых затрат после атаки. Матрица позволяет организовать эшелонированную оборону для своевременного обнаружения, усложнения, обмана или нейтрализации угрозы на каждой из семи фаз Cyber Kill Chain модели.

Заключение. Реализация модели Cyber Kill Chain в процессе атрибуции, позволит организовать более эффективный подход к идентификации кибернарушителя, выработать эффективные меры по сдерживанию, выявлению, нейтрализации и сокращению возможного ущерба в ходе целевой атаки. Стоит отметить перспективность применения данной модели в интеллектуальных системах безопасности [18].

Работа выполнена при финансовой поддержке Гранта РНФ № 21-71-20078 в СПб ФИЦ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. Скрыль С.В. и др. Актуальные вопросы проблематики оценки угроз компьютерных атак на информационные ресурсы значимых объектов критической информационной инфраструктуры. Безопасность информационных технологий, Том 28, 2021, № 1 С. 84–94.
2. Стратегия национальной безопасности Российской Федерации [Текст] // Указ Президента Российской Федерации от 31.12.2015 N 683 [Электронный ресурс]. URL: http://www.consultant.ru/document/ (дата обращения: 25.06.2021).
3. Christian R. Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace. 2019, Springer, Cham, 2019. 424 p.
4. Энциклопедия «Касперского». Атрибуция кибератаки [Электронный ресурс]. URL: https://encyclopedia.kaspersky.ru/glossary/cyber-attribution/ (дата обращения: 25.06.2021).
5. Забегалин Е. В. К вопросу об определении термина «информационно-техническое воздействие» // Системы управления, связи и безопасности. 2018. № 2. С. 121–150. URL: http://sccs.intelgr.com/archive/2018-02/08-Zabegalin.pdf (дата обращения 25.06.2021).
6. Steffens T. Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage. Springer, Berlin, 2020. 205 p.
7. Kotenko I., Stepashkin M. Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages of Computer Network Life Cycle // Lecture Notes in Computer Science, Springer-Verlag, V.3685. 2005. P. 311-324.
8. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1 // Труды СПИИРАН. 2016. Вып. 4 (47). С. 5-27.
9. Clark R., Hakim S. Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. Springer, Cham, 2017. 290 p.
10. Тюрин М.А., Грамс В.А., Мельников Н.А. The Cyber Kill Chain Model // В сборнике: Сборник статей XIX Международного научно-исследовательского конкурса, 2021. С. 48-50.
11. The Cyber Kill Chain [Электронный ресурс]. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (дата обращения 23.06.2021).
12. Kotenko I., Stepashkin M. Network Security Evaluation based on Simulation of Malefactor's Behavior // SECRYPT 2006. International Conference on Security and Cryptography. Proceedings. Portugal. 7-10 August 2006. P.339-344.
13. Лукацкий А.В. Убийственная цепочка или что такое Kill Chain. Securitylab [Электронный ресурс]. URL: https://www.securitylab.ru/blog/personal/Business_without_danger/320009.php (дата обращения 27.06.2021).
14. Котенко И. В., Полубелова О.В., Саенко И.Б., Чечулин А.А. Применение онтологий и логического вывода для управления информацией и событиями безопасности // Системы высокой доступности, Т.8, № 2, 2012. С.100-108.
15. Саранский А.В., Новиков В. И., Братишко Н. М., Казанцева В. А. Поэтапный разбор кибератаки WannaCry при помощи модели жизненного цикла Cyber-Kill Chain // В сборнике: Инновационные технологии в науке и образовании. Сборник статей XIV Международной научно-практической конференции. 2019. С. 32-34.
16. Colbert E., Kott A. Cyber-security of SCADA and Other Industrial Control Systems, Springer, Cham, 2016. 355 p.
17. Hutchins E., Cloppert M., Amin R. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains // Leading Issues in Information Warfare & Security Research, 2011. 14 p.
18. Котенко И.В., Саенко И.Б., Чечулин А.А. [и др.] // Интеллектуальные сервисы защиты информации в критических инфраструктурах. БХВ-Петербург, 2019. 400 С.

УДК 004.65

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ SQL-ИНЪЕКЦИЙ

Якушев Денис Игоревич, Вайберт Наталия Антоновна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: d.i.ya@yandex.ru, tasha.vaybert@mail.ru

Аннотация. Рассматривается вопрос защиты информации от SQL-инъекций, выявляются основные причины появления таких уязвимостей, а также сами методы защиты от подобного типа атак.

Ключевые слова: защита; SQL-инъекция; база данных.

METHODS FOR PROTECTING INFORMATION FROM SQL-INJECTIONS

Yakushev Denis, Vaybert Natalia
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: d.i.ya@yandex.ru, tasha.vaybert@mail.ru

Abstract. The issue of protecting information from SQL injections is considered, the main reasons for the appearance of such vulnerabilities are identified, as well as the methods of protection against this type of attacks themselves.

Keywords: protection; SQL-injection; database.

На сегодняшний день многие организации, компании, государственные службы, в том числе и МВД России используют в своей деятельности базы данных и различные веб-приложения. По статистике Positive

Technologies, каждое четвертое веб-приложение подвержено критически опасной уязвимости «Внедрение операторов SQL». В результате использования SQL-инъекций в базу данных злоумышленникам удалось получить доступ к клиентским данным (включая имена, адреса и телефоны), доменным именам, FTP-паролям, сведениям о банковском счете (без данных кредитных карт) [1].

SQL-инъекция – это метод (как и другие механизмы веб-атак) для атаки на приложения, управляемые данными [2]. Злоумышленник использует преимущество плохо отфильтрованных или неправильно экранированных символов, встроенных в операторы SQL, при разборе переменных данных из пользовательского ввода. Он вставляет произвольные данные, чаще всего запрос к базе данных, в строку, которая в конечном итоге выполняется базой данных через веб-приложение.

Целью работы является анализ эффективности наиболее распространенных средств защиты от SQL-инъекций.

Поставленная цель требует решения следующих задач:

– изучение особенностей внедрения операторов SQL (SQL-инъекции);
– исследование методов обнаружения аномалий в SQL-запросах к базам данных;
– изучение методов защиты от исследуемого типа атак.

Объектом исследования выступают методы защиты информации от SQL-инъекций.

Предметом работы выступают SQL-запросы, базы данных.

Основными причинами появления уязвимости типа SQL-инъекции являются:

динамическое построение SQL-запросов;

– некорректная обработка исключений;
– некорректная обработка специальных символов;
– некорректная обработка типов данных;
– небезопасная конфигурация СУБД [3].

В дальнейшем необходимо рассмотреть основные классификацию методов защиты от SQL-инъекций:

– методы защиты, основанные на изменении кода веб-приложения;
– методы защиты без изменения кода веб-приложения.

Первый тип реализуется следующими мерами:

– экранирование специальных символов. Использование функции, экранирующей специальные символы строки, и тем самым изменяя синтаксис SQL-запроса и уменьшая вероятность проведения атаки типа SQL-инъекции;

– явное преобразование типов полей ввода. Примером может служить функция языка PHP CAST («Varchar» AS INT), преобразующая строковый тип в числовой;

– подготавливаемые запросы. Подготавливаемые запросы или параметризованные запросы используются для повышения эффективности, когда один запрос выполняется многократно, а также для повышения безопасности баз данных [4].

Второй тип защиты реализуется посредством использования специальных межсетевых экранов для SQL-серверов, такие как GreenSQL [4].

Таким образом, были выявлены основные причины появления SQL-инъекций, а также методы защиты от подобного рода атак, которые позволяют свести возможность проведения таких атак злоумышленниками к минимуму, что значительно усиливает свойства безопасности информации, циркулирующей в информационной системе.

СПИСОК ЛИТЕРАТУРЫ

1. Positive research. «Актуальные киберугрозы IV квартал 2017 года.» [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-Q4-rus.pdf (дата обращения: 01.08.2021 г.);
2. Учебник по SQL-инъекциям [Электронный ресурс]. Режим доступа: http://kodesource.top/sql/sql-injection/sql-injection.php (дата обращения: 01.08.2021 г.);
3. SQL-инъекции – распространённый метод взлома веб-приложений и сайтов [Электронный ресурс]. Режим доступа: https://web-creator.ru/articles/sql_injection (дата обращения: 01.08.2021 г.);
4. Соколин Д.Д., Тимохович А.С. Методы комплексного обеспечения безопасности SQL-сервера от атак типа SQL-инъекции. // Academy. 2017. 3 (18). С. 7-9.

УДК 004

МЕТОД АВТОМАТИЗАЦИИ ПОИСКА САЙТОВ DARKNET

Якушев Денис Игоревич, Мочалова Валерия Олеговна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: d.i.ya@yandex.ru, lera.rusanova.2017@mail.ru

Аннотация. В статье рассматривается возможность получения правоохранительными органами используемых адресов в Даркнет.

Ключевые слова: правоохранительными органы; Даркнет.

A METHOD FOR AUTOMATING THE SEARCH FOR DARKNET SITES

Yakushev Denis, Mochalova Valeria
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: d.i.ya@yandex.ru, lera.rusanova.2017@mail.ru

Abstract. The article considers the possibility of obtaining the addresses used by law enforcement agencies in the Darknet.

Keywords: law enforcement agencies; Darknet.

Объектом исследования является оперативно-розыскная информация.

Предметом исследования - метод автоматизации поиска сайтов в Darknet.

Цель работы: повышение эффективности предотвращения, выявления и расследования преступлений в области информационных технологий, посредством поиска адресов сайтов Darknet.

Исходя из цели можно выделить следующие задачи:

Анализ преступлений, которые происходят в области информационных технологий

Анализ существующего методов предотвращения, выявления и расследования преступлений в области информационных технологий

Разработка метода повышения эффективности предотвращения, выявления и расследования преступлений в области информационных технологий, посредством поиска адресов сайтов Darknet.

Методы, используемые в ходе достижения задач, являются анализ и синтез, а также применение программных решений к решению поставленной задачи.

Термин Darknet или "Тёмная паутина" в общем понимании обозначает совокупность веб-сайтов, видимых публично, но при этом имеющих скрытый IP-адрес сервера, на котором они размещаются [1].

По сути, Darknet это частная сеть, в которой соединения устанавливаются только между доверенными пирами, иногда именующимися как «друзья», и чаще всего с использованием нестандартных протоколов и портов. Darknet отличается от других распределенных одноранговых сетей, так как файлообмен происходит анонимно (вследствие того, что IP-адреса ресурсов недоступны публично), и, следовательно, пользователи могут общаться без особых опасений и государственного вмешательства [2].

Можно встретить сравнение Darknet и технологий 2p2-обмена применяемых, к примеру, для распространения торрентов. Так, наиболее распространенные на сегодняшний день файлообменники, например, Bittorrent, на самом деле не является Darknet, поскольку пользователи могут связываться с кем угодно в сети. Почти все известные Darknet децентрализованы и, следовательно, считаются одноранговыми. Так же, многие сайты Darknet требуют установки специального программного обеспечения для получения доступа к сети. Практически все сайты, находящиеся в Тёмной паутине, скрывают свою принадлежность, используя инструмент шифрования Tor. Важно сказать, что не все сайты Тёмной паутины используют Tor [3].

Рассмотрим случай, который произошёл 28 сентября 2020 года о похищении семилетнего мальчика. В поисках ребенка приняли участие представители силовых органов, МЧС, военные и добровольцы. Ребенка искали с помощью собак, беспилотников и даже вертолетов. Однако все было безрезультатно. Найти ребенка удалось благодаря данным, переданным Интерполом, который также был подключен к розыску. Как оказалось, преступник вел переписку в Darknet через браузер Tor. Благодаря этим данным удалось установить местоположение похитителя, который находился в соседней деревне [4].

Таким образом, адреса сайтов в Darknet имеют большое значение для розыска, однако не могут быть получены с помощью поисковых систем. Для установления используемых адресов в домене. onion предлагается фильтрация интернет-трафика. Поисковый запрос может быть сформулирован с помощью регулярных выражений. Все искомые адреса имеют общую структуру: http://(…).onion, где (…) название ресурса, состоящее из латинских букв и цифр. Отсюда следует что все адреса в общем виде могут быть записаны с помощью регулярных выражений. Что позволит осуществлять поиск в потоках данных.

Практическое решение поставленной задачи позволит правоохранительным органам получить доступ к используемым сайтам Darknet, что предоставит возможность правоохранительным органам получать оперативно-значимую информацию.

СПИСОК ЛИТЕРАТУРЫ

1. Латур Б. Об интеробъективности. / Пер. с англ. А. Смирнова; под научн. ред. В.С. Вахштайна // Социология вещей: сб. ст. / Под ред. В.С. Вахштайна. - М: Издательский дом «Территория будущего», 2006. - С. 169-199.
2. Мэтт Иган. На темной стороне интернета: что такое Dark Web и Deep Web? URL: https://www.dgl.ru/articles/na-temnoy-storone-interneta-chto-takoe-dark-web-i-deep-web_11677.html.
3. [Электронный ресурс] URL: https://securelist.ru/skrytye-resursy-seti-tor-ti [aya-gavan-dlya-kiberprtstupnikol/15621/(Дата обращения: 15.09.2021).
4. [Электронный ресурс] URL: https://www.if24.ru/v-rossii-cherez-darknet-nashli-pohishhennogo-malchika/(Дата обращения: 15.09.2021).

СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

УДК 003.26

СТРОЕНИЕ КОНЕЧНЫХ НЕКОММУТАТИВНЫХ АЛГЕБР С МНОЖЕСТВОМ ГЛОБАЛЬНЫХ ОДНОСТОРОННИХ ЕДИНИЦ И СИНТЕЗ КРИПТОСХЕМ

Костина Анна Александровна[1], Мирин Анатолий Юрьевич[1], Молдовян Дмитрий Николаевич[2]
[1] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: anna-kostina1805@mail.ru, mirin@cobra.ru, mdn.spectr@mail.ru

Аннотация. Обсуждается строение конечных алгебр с множеством глобальных односторонних единиц как носителей криптосхем с открытым ключом. Показано, что с каждой глобальной единицей связано гомоморфное отображение алгебры и множество векторов, образующих подалгебру. Наличие такого гомоморфизма может быть эффективно использовано при анализе криптосхем на алгебрах указанного типа путем сведения к анализу криптосхем на алгебрах меньшей размерности.

Ключевые слова: конечные алгебры; некоммутативные алгебры; криптосхемы с открытым ключом; алгортмы цифровой подписи.

STRUCTURE OF NON-COMMUTATIVE ALGEBRAS WITH A SET OF GLOBAL SINGLE-SIDED UNITS AND DESIGN OF CRYPTOSCHEMES

Kostina Anna[1], Mirin Anatoliy[1], Moldovyan Dmitriy[2]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[2] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: anna-kostina1805@mail.ru, mirin@cobra.ru, mdn.spectr@mail.ru

Abstract. The structure of finite algebras with a set of global single-sided units as carriers of the public-key cryptoschemes is discussed. It is shown that with each global unit, a homomorphic mapping of algebra and a subset of vectors forming a subalgebra are connected. The presence of such a homomorphism can be effectively used in the analysis of cryptoschemes on the algebras of the specified type by reduction to the analysis of a cryptoscheme on algebras of a smaller dimension.

Keywords: finite algebras; non-commutative algebras; public-key cryptoschemes; digital signature algorithms.

Конечные некоммутативные ассоциативные алгебры (КНАА) представляют интерес в качестве алгебраических носителей постквантовых протоколов открытого согласования ключа [1] и электронной цифровой подписи [2, 3]. Среди КНАА выделяются алгебры, содержащие большое множество глобальных односторонних единиц. Возникает вопрос об использовании особенностей КНАА такого типа при разработке криптосхем с открытым ключом.

В данном сообщении рассматривается строение КНАА, содержащих большое множеств глобальных односторонних (левосторонних или правосторонних) единиц и его использование при криптоанализе двухключевых криптосхем на КНАА уазанного типа.

При исследовании строения было использовано наличие гомоморфизмов алгебры, связанных с глобальными односторонними единицами. Каждая из последних задает уникальное гомоморфное отображение алгебры в подалгебру с глобальной двухсторонней единицей. Каждая из единиц задает уникальную подалгебру, к которой она является глобальной двухсторнней единицей. Каждый из локально обратимых элементов алгебры содержится в уникальной подалгебре. Все подалгебры изоморфны между собой. Для определения порядка подалгебр выполняется подсчет локально обратимых элементов алгебры и полученное значение делится на число глобальных односторонних единиц. С глобальной правосторонней (левосторонней) единицей связано гомоморфное отображение алгебры в подалгебру, включающую эту единицу. Данный гомоморфизм задается умножением слева (справа) всех векторов на эту единицу и позволяет свести анализ стойкости криптосхем на основе КНАА с множеством глобальных односторонних единиц к анализу соответствующих криптосхем на основе алгебр меньшей размерности, содержащих глобальную двухстороннюю единицу.

Изучены заданные над простым полем $GF(p)$ четырехмерные и шестимерные КНАА, в которых операция ассоциативного умножения задана по различным таблицам умножения базисных векторов. В первом случае число глобальных односторонних единиц равно квадрату простого числа p и всегда имеют место гомоморфизмы в двухмерные подалгебры. Во втором случае число глобальных односторонних единиц равно квадрату, кубу или четвертой степени числа p и имеют место гомоморфизмы в четырехмерные, трехмерные или двухмерные подалгебры, соответственно.

Основным результатом выполненного исследования является то, что при заданном уровне стойкости криптосхемы на КНАА изученного типа всегда будут существенно уступать по вычислительной эффективности аналогичным криптосхемам, построенным на КНАА с глобальной односторонней единицей. Таким образом, способов построения алгоритмов электронной цифровой подписи на основе вычислительной трудности скрытой задачи дискретного логарифмирования [1] следует проводить в направлении использования КНАА с глобальной двухсторонней единицей.

СПИСОК ЛИТЕРАТУРЫ

1. Moldovyan N.A., Moldovyan A.A. Finite Non-commutative Associative Algebras as Carriers of Hidden Discrete Logarithm Problem // Вестник ЮУрГУ. Серия “Математическое моделирование и программирование”. 2019. Т. 12. № 1. С. 66−81. DOI: 10.14529/mmp190106.
2. Молдовян Н.А., Абросимов И.К. Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23−32.
3. Moldovyan D.N., Moldovyan A.A., Moldovyan N.A. A new design of the signature schemes based on the hidden discrete logarithm problem // Quasigroups and Related Systems. 2021. Vol. 29. No. 1. P. 97-106.

УДК 003.26

ПСЕВДОВЕРОЯТНОСТНОЕ ШИФРОВАНИЕ КАК МЕХАНИЗМ ЗАЩИТЫ ИНФОРМАЦИИ

Костина Анна Александровна[1], Молдовян Александр Андреевич[2], Фахрутдинов Роман Шафкатович[1]
[1] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: anna-kostina1805@mail.ru, maa1305@yandex.ru, fahr@cobra.ru

Аннотация. Рассмотрены вопросы применения псевдовероятностного шифрования как базового преобразования данных для построения новых механизмов защиты информации от несанкционированного доступа. Одной из новых возможностей, предоставляемых данным типом шифрования, является возможность реализации механизмов навязывания ложной информации.

Ключевые слова: псевдовероятностное шифрование; отрицаемое шифрование; симметричные криптосистемы; блочные шифры.

PSEUDOPROBABILISTIC ENCRYPTION AS A MECHANISM FOR THE INFRMATION PROTECTION

Kostina Anna[1], Moldovyan Alexandr[2], Fahrutdinov Roman[1]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[2] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: anna-kostina1805@mail.ru, maa1305@yandex.ru, fahr@cobra.ru

Abstract. The use of pseudoprobabilistic encryption is considered as a basic data transformation to build new information protection mechanisms from unauthorized access. One of the new features provided by this type of encryption is the ability to implement the mechanisms of imposing false information.

Keywords: pseudo-probabilistic encryption; deniable encryption; symmetric cryptosystems; bloc ciphers.

Псевдовероятностное шифрование представляет собой специальный случай отрицаемого шифрования с разделяемым секретным ключом. Данный тип криптографического преобразования данных ориентирован на использование в средствах защиты информации от несанкционированного доступа. Он реализуется как процесс шифрования, вычислительно неотличимый по криптограмме от вероятностного шифрования, и представляет собой совместное преобразование двух независимых сообщений на двух ключах, секретном и фиктивном. При этом расшифровывание полученного шифртекста выполняется с использованием одного и того же алгоритма. Известны общие способы построения блочных [1] и поточных [2-4] алгоритмов псевдовероятностного шифрования. В случае блочного шифрования любой известный алгоритм блочного шифрования может быть использован как базовое преобразование при построении блочного псевдовероятностного шифра. Это дает основание рассматривать два новых режима использования блочных шифров – режимы вероятностного и псевдовероятностного шифрования. В настоящем сообщении обсуждаются аспекты реализации специальных механизмов защиты информации, использующих особенности псевдовероятностных алгоритмов шифрования.

Благодаря тому, что криптограмма, генерируемая алгоритмом псевдовероятностного шифрования, вычислительно неотличима от шифртекста, получаемого в ходе вероятностного шифрования, имеет место ситуация, когда потенциальный криптоаналитик, выполнив дешифрование перехваченной криптограммы, не уверен, что он получил истинное секретное сообщение. Это создает дополнительные трудности для потенциального нарушителя, который знает, что для защиты информации используется механизм псевдовероятностного шифрования. В модели нарушителя, который не знает, что применяется псевдовероятностное шифрование, имеется возможность навязывания ему ложной информации, что представляет значительный интерес в специальных приложениях средств защиты информации в информационно-телекоммуникационных системах. Применяя секретный и фиктивный ключи различного размера, может быть обеспечена надежность защиты секретного сообщения и возможность для нарушителя раскрыть фиктивное сообщение, выполнив перебор по ключевому пространству. При этом задавая соответствующий размер фиктивного ключа можно регулировать вычислительную сложность указанного способа криптоанализа, обеспечивая возможность расшифровать криптограмму нарушителями, обладающими вычислительными ресурсами различного уровня. Задавая трудоемкость взлома, близкую к возможностям вычислительных ресурсов нарушителя, потенциально создается мотивировка доверия к раскрытому фиктивному сообщению как полученному в ходе криптоанализа.

Аналогичная ситуация возникает в случаях, когда принимается модель нарушителя имеющего возможность получения ключей шифрования методами, отличными от криптоанализа (покупка и хищение ключей). При этом могут использоваться фиктивные ключи большого размера.

Реализация новых механизмов защиты информации на основе псевдовероятностного шифрования предполагает учет конкретного их приложения. Общим моментом является то, что при использовании стойких алгоритмов шифрования, на основе которых строятся алгоритмы псевдовероятностного шифрования, перед криптоаналитиком, раскрывшим фиктивное сообщение, возникает дилемма: он выполнил поставленную перед ним задачу или следует продолжить криптоанализ до раскрытия еще одного сообщения, которое и окажется истинным секретным сообщением. При этом, во втором случае может оказаться, что применялось вероятностное шифрование и раскрытие второго сообщения окажется теоретически невыполнимой задачей.

Механизм псевдовероятностного шифрования может быть расширен на следующие случаи: 1) совместное шифрование трех и более сообщений на независимых ключах; 2) рандомизация псевдовероятностного шифрования; 3) дополнительное применение процедур сжатия одного или всех шифруемых сообщений. Для последних случаев появляются дополнительные возможности по реализации новых механизмов защиты информации.

СПИСОК ЛИТЕРАТУРЫ

1. Moldovyan N.A., Moldovyan A.A., Duc Tam Nguyen, Nam Hai Nguyen, Cong Manh Tran,Hieu Minh Nguyen Pseudo-probabilistic block ciphers and their randomization // J. Ambient Intelligence and Humanized Computing. 2019. Vol. 10. P. 1977-1984. DOI: 10.1007/s12652-018-0791-6
2. Молдовян Н.А., Баширов З.С., Солнышкин Ж.А. Протокол поточного отрицаемого шифрования с разделяемым ключом // Вопросы защиты информации. – 2015. – № 3. – С. 27-31.
3. Костина А.А., Молдовян Д.Н., Молдовян Н.А. Методические аспекты псевдовероятностного шифрования // Современное образование: содержание, технологии, качество. – 2019. – Т. 1. – С. 336-338.
4. Молдовян А.А., Молдовян Н.А., Березин А.Н., Шаповалов П.И. // Международная конференция по мягким вычислениям и измерениям. 2017. – Т. 1. – С. 27-30.

УДК 004.056

ОБНАРУЖЕНИЕ АНОМАЛИЙ В СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ ПУТЕМ АНАЛИЗА ЭНЕРГОПОТРЕБЛЕНИЯ

Крундышев Василий Михайлович, Калинин Максим Олегович
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: vmk@ibks.spbstu.ru, max@ibks.spbstu.ru

Аннотация. В статье рассмотрен подход к обнаружению кибератак на устройства Интернета вещей на основе анализа энергопотребления. Представлен метод обнаружения аномалий с использованием прогнозирования на основе временных рядов.

Ключевые слова: анализ энергопотребления; временные ряды; интернет вещей; прогнозирование; ARMA; IoT.

ANOMALY DETECTION IN THE INTERNET OF THINGS BY ANALYSIS OF ENERGY CONSUMPTION

Krundyshev Vasiliy, Kalinin Maxim
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mails: vmk@ibks.spbstu.ru, max@ibks.spbstu.ru

Abstract. The paper discusses an approach to detecting cyberattacks on IoT devices based on energy consumption analysis. A method for detecting anomalies using time series forecasting is presented.

Keywords: energy consumption analysis; time series; internet of things; forecasting; ARMA; IoT.

Введение. Развитие технологий беспроводных сетей 4/5G, диджитализация производств, а также повсеместное внедрение устройств Интернета вещей привели к тому, что у киберпреступников появились новые цели [1]. Если раньше задача обеспечения безопасности заключалась в поддержании целостности, доступности и конфиденциальности данных, то теперь под угрозой объекты не цифрового, а реального мира: беспилотные автомобили, умные заводы, городская инфраструктура [2, 3]. Основной проблемой безопасности Интернета вещей является отсутствие средств защиты у большинства конечных устройств. Производители оборудования зачастую не уделяют должного внимания вопросу обеспечения безопасности. Взломав и взяв под контроль один узел сети, у злоумышленника уже появляются огромные возможности по реализации различных атак. Под воздействием таких атак, как «отказ в обслуживании», «атака грубой силы» и т.д. у устройств Интернета вещей увеличивается энергопотребление [4]. Для обнаружения таких атак предлагается метод, основанный на прогнозировании энергопотребления с использованием временных рядов.

Временной ряд – это совокупность статистических данных, собранных в разные моменты времени, о значении каких-либо параметров исследуемого процесса. Значения временного ряда получаются путем записи значения определенного параметра исследуемого процесса через одинаковые периоды времени. В данном случае значением параметра будет являться параметры энергопотребления. Временные ряды могут быть стационарными и нестационарными.

Разработанный метод обнаружения аномалий на основе анализа энергопотребления состоит из следующих этапов:

1) сбор данных сервером со всех контролируемых устройств сети Интернета вещей;

2) построение модели ARMA для прогноза энергопотребления для каждого устройства;

3) сопоставление фактических и данных прогноза, вычисление отклонений;

4) при возникновении множественных аномалий энергопотребления выявление предположительного нарушителя или точку входа нарушителя.

В локальной системе есть n устройств, $n \epsilon \mathbb{N}$. Они образуют множество $D = \{\mathrm{d}_1, \mathrm{d}_2, \dots, \mathrm{d}_n\}$ – множество устройств локальной сети. Этим устройствам соответствует информация об энергопотреблении e_i и прогноз для устройства f_i, где i, где $i = 1,2, \dots, n$.

На первом этапе система собирает данные e_i от устройства d_i и размешает их на центральном сервере. При подключении нового устройства требуется несколько дней собирать данные, чтобы прогноз был точный.

На втором этапе строится модель ARMA для определённого устройства d_i, вычисляется прогноз f_i. И система дальше собирает информацию e_i.

По истечении времени прогноза проверяется ошибка прогноза, и делается вывод о нормальном или аномальном энергопотреблении. Строится множество устройств с аномалиями $D_A = \{d_j\}$ и без них $D_H = \{d_k\}$, где $j, k = 1,2, \dots, n$ и для любых $j, k: j \neq k$. Если таких аномалий несколько, то система определяет, где находится нарушитель путем вычисления веса устройств, который устанавливается в зависимости от количества узлов-соседей с аномальным энергопотреблением.

Для функционирования системы предлагается использовать централизованную архитектуру сети Интернета вещей, где собранные данные обрабатываются на выделенном сервере. Узел нарушителя определяется на основе матрицы смежности, характеризующей взаимодействие узлов сети.

В результате экспериментальных исследований была определена конфигурация модели ARMA, а именно SARMA(2,0,2)(1,0,2)[24]. При использовании данной конфигурации коэффициент ошибки составляет 10%, что свидетельствует о высокой точности прогнозирования.

Исследование выполнено в рамках стипендии Президента РФ для поддержки молодых ученых и аспирантов (СП-2714.2021.5).

СПИСОК ЛИТЕРАТУРЫ

1. Овасапян Т. Д., Москвин Д. А. Выявление внутренних нарушителей в VANET-сетях с использованием нейронных сетей. материалы IV межрегиональной научно-практической конференции. Севастопольский государственный университет; науч. ред. Б.В. Соколов. 2018. – С. 239-240.
2. Дахнович А. Д., Москвин Д. А., Зегжда Д. П. Применение принципа «безопасности через незнание» в промышленном Интернете Вещей. Проблемы информационной безопасности. Компьютерные системы. №1. 2021. – С. 131-137.
3. Rossi B. et al. Anomaly detection in smart grid data: An experience report //2016 ieee international conference on systems, man, and cybernetics (smc). – IEEE, 2016. – P. 2313-2318.
4. Zegzhda D., Pavlenko E., Shtyrkina A. Cybersecurity and Control Sustainability in Digital Economy and Advanced Production. The Economics of Digital Transformation: Approaching Non-stable and Uncertain Digitalized Production Systems. 2020. – P. 173.

УДК 004.93'1

АКТУАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ НЕЙРОСЕТЕВЫХ АЛГОРИТМОВ В СИСТЕМАХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Ложников Павел Сергеевич
Омский Государственный Технический Университет
Мира пр., 11, Омск, 644050, Россия
e-mail: lozhnikov@mail.ru

Аннотация. Рассматриваются возможные атаки на алгоритмы искусственного интеллекта в виде манипуляций с моделями, обучающими и входными данными, направленные на извлечение модели, обучающих данных и знаний. Предлагается использовать «защищенное исполнение» искусственного интеллекта, где вместо весовых коэффициентов классических нейронов используются корреляционные, которые анализируют связи между признаками вместо значений признаков в задачах классификации образов.

Ключевые слова: атаки на искусственный интеллект; информационная безопасность; защищенный искусственный интеллект; корреляционные нейроны.

TOPICAL ISSUES OF NEURAL NETWORK ALGORITHM PROTECTION IN ARTIFICIAL INTELLIGENCE SYSTEMS

Lozhnikov Pavel
Omsk State Technical University
11 Mira Av, Omsk, 644050, Russia
e-mail: lozhnikov@mail.ru

Abstract. Possible attacks on artificial intelligence algorithms in the form of manipulations with models, training and input data, aimed at extracting the model, training data and knowledge, are considered. It is proposed to use the "protected execution" of artificial intelligence, where instead of the weighting coefficients of classical neurons, correlation ones are used, which analyze the connections between the features instead of the feature values in the problems of image classification.

Keywords: attacks on artificial intelligence; information security; protected artificial intelligence; correlation neurons.

Искусственный интеллект (ИИ) становятся существенным интеллектуальным активом компаний, другими словами – нематериальным ресурсом, обладающим свойством уникальности и исключительности, способным приносить значительные экономические выгоды. По мере роста потребления продуктов и услуг, созданных на основе ИИ, необходимо предпринимать защитные меры, чтобы обезопасить не только потребителей услуг, но и сами алгоритмы ИИ от злоупотребления, атак и нарушения работоспособности.

Вводится понятие «защищенное исполнение» ИИ. Это такое исполнение ИИ, обеспечивающее невозможность совершения любым неавторизованным лицом или субъектом доступа таких действий как, анализ операций, совершаемых ИИ, управление ИИ, извлечение знаний ИИ.

В ответственных приложениях ИИ должен выполняться в защищенном исполнении.

Учитывая то, что ИИ в перспективе будет все больше и больше приносить прибыли компаниям, он становится объектом потенциальных компьютерных атак. Если приложения и алгоритмы ИИ выполнены в незащищенном исполнении, то злоумышленники гипотетически могут провести следующие виды атак:

1. *Манипуляции с моделями.* Частным случаем являются атаки «на решающий бит» (атаки «одного бита»). Например, если на выходе нейронной сети располагается функция SoftMax, то достаточно поменять два ее выхода местами, чтобы заменить одно управляющее воздействие на другое. Другая ситуация возникает, если хакер напрямую подключится к объекту управления или к каналу передачи данных с возможностью изменять сигналы на выходе ИИ. В этом случае он сможет имитировать определенные управляющие воздействия и изменять одну команду на другую.

2. *Манипуляции с обучающими данными*. Целью таких манипуляций может быть создание вредоносного экземпляра ИИ, который будет выполнять функции, заложенные злоумышленником. Подмену экземпляра ИИ можно зафиксировать при сравнении контрольных сумм параметров и знаний ИИ.

3. Манипуляции с входными данными. К данной категории можно отнести «состязательные» атаки (спуфинг), при которых хакер подает на вход ИИ фальсифицированные или перехваченные данные с целью получения на выходе ИИ желаемых управляющих воздействий. Обычно для защиты от такого рода атак обучающую выборку пытаются расширить с учетом всех возможных вариаций входных данных, что не всегда возможно на практике.

4. *Извлечение модели и/или обучающих данных (атаки «ключ под ковриком»)*. В памяти ИИ могут храниться конфиденциальные или персональные данные. Чтобы защитить эти данные от угрозы нарушения конфиденциальности, параметры решающих правил (например, таблицы весовых коэффициентов и связей нейронов) принято шифровать на некотором криптографическом ключе [1].

5. *Гибридные атаки.* Эта категория атак может также быть связана с определенными манипулятивными воздействиями. Примером является атака «извлечения знаний» из нейронной сети с множеством выходов.

Чтобы указанные угрозы можно было устранить (или снизить до минимально возможного уровня) ИИ должен работать, как преобразователь входных воздействий (поступающей информации) в длинный криптографический ключ или пароль, который можно ассоциировать с определенным управляющим воздействием.

Параметры обученного ИИ необходимо хранить в специальном виде, защищенном от извлечения «знаний», даже при отсутствии стороннего шифрования. Для этого нужно перейти от весовых коэффициентов классических нейронов к параметрам корреляционных нейронов. Корреляционные нейроны – это новый класс нейронов, анализирующих корреляционные связи между признаками вместо значений признаков в задачах классификации образов; они обучаются с учителем в автоматическом режиме [2].

На кафедре комплексной защиты информации Омского государственного технического университета разработаны модели корреляционных нейронов и алгоритмы их обучения, проведено аналитико-синтетическое исследование научных работ, а также международных и национальных стандартов, касающихся проблем безопасности искусственного интеллекта и методов их решения. Разработан проект третьего национального стандарта «Искусственный интеллект в защищенном исполнении», который затрагивает пока только задачи классификации [3].

СПИСОК ЛИТЕРАТУРЫ

1. Lozhnikov, P. S. Generation of a biometrically activated digital signature based on hybrid neural network algorithms / P. S. Lozhnikov, A. E. Sulavko // Journal of Physics: Conference Series, Omsk, 27–28 февраля 2018 года. – Omsk: Institute of Physics Publishing, 2018. – P. 012047. – DOI 10.1088/1742-6596/1050/1/012047.
2. Защищенный режим исполнения искусственного интеллекта на базе автоматически обучаемых сетей автокорреляционных нейронов: отчет о НИР. ОмГТУ. Рук. Сулавко А.Е. – Омск. – 101 С. – Исполн.: Ложников П.С., Самотуга А.Е., Магазев А.А., Данилова О.Т. URL:
3. https://www.researchgate.net/publication/351904440_ZASISENNYJ_REZIM_ISPOLNENIA_ISKUSSTVENNOGO_INTELLEKTA_NA_BAZE_AVTOMATICESKI_OBUCAEMYH_SETEJ_AVTOKORRELACIONNYH_NEJRONOV (дата обращения: 30.08.2021)
4. Иванов А.И., Сулавко А.Е. Проект третьего национального стандарта россии по быстрому автоматическому обучению больших сетей корреляционных нейронов на малых обучающих выборках биометрических данных // Вопросы кибербезопасности. - 2021. - №3. - С. 84-93. DOI:10.21681/2311-3456-2021-3-84-93.

УДК 004.056

ПОСТРОЕНИЕ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ НАСТРОЙКИ ПАРАМЕТРОВ БЕЗОПАСНОСТИ WSN-СЕТЕЙ

Овасапян Тигран Джаникович, Таразевич Мария Сергеевна, Москвин Дмитрий Андреевич
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: otd@ibks.spbstu.ru, tarazevich.home@gmail.com, moskvin@ibks.spbstu.ru

Аннотация. В рамках работы предложена система поддержки принятия решений (СППР) для настройки параметров безопасности беспроводных сенсорных сетей (WSN). Проведен анализ принципов развертывания WSN-сетей, особенностей их работы, проблем безопасности. Разработана СППР, позволяющая подбирать параметры для беспроводных сенсорных сетей. Были собраны, проанализированы и систематизированы экспертные знания в области безопасности WSN-сетей. Разработан блок моделирования предметной области и ситуаций, который позволяет пользователю вводить параметры сети и получать соответствующие рекомендации для принятия управленческих решений безопасности.

Ключевые слова: беспроводные сенсорные сети; WSN-сети; система поддержки принятия решений; сетевые атаки.

BUILDING A DECISION SUPPORT SYSTEM FOR CONFIGURATION OF SECURITY PARAMETERS FOR WSN-NETWORKS

Ovasapyan Tigran, Tarazevich Maria, Moskvin Dmitry
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mails: otd@ibks.spbstu.ru, tarazevich.home@gmail.com, moskvin@ibks.spbstu.ru

Abstract. The paper proposes a decision support system (DSS) for configuring the security parameters of wireless sensor networks (WSN). The analysis of the principles of deployment of WSN-networks, the peculiarities of their work, security problems is carried out. Developed a DSS, which allows person to select parameters for a wireless sensor network. For this purpose, expert knowledge in the field of wireless sensor networks security was collected, analyzed and systematized. A modeling block of the subject area and situations was developed, which allows the user to enter the network parameters and obtain relevant recommendations for making security management decisions.

Keywords: Wireless Sensor Networks; WSN; decision support system; network attacks.

Активное развитие в области исследований беспроводных сенсорных сетей (Wireless Sensor Networks, WSN) пришлось на начало 21 века. Беспроводные сенсорные сети приобрели значительную популярность благодаря своей универсальности в решении многих задач в различных областях применения и имеют потенциал для изменения нашей жизни [1, 2]. Эта технология используется в широком спектре отраслей, например, в структурном и экологическом мониторинге, промышленности, военном деле, медицине и сельском хозяйстве, при создании систем умного города и, в частности, умного транспорта.

В настоящее время для WSN-сетей не существует комплексного подхода к обеспечению безопасности. Можно утверждать, что ни одна общая схема безопасности не будет подходить для всех беспроводных сенсорных сетей. В данной работе было разработано решение – система поддержки принятия решений с учетом прикладных и технических архитектур и требований безопасности в WSN.

На начальном этапе работы были выделены целевые области применения технологии, первичные параметры беспроводных сенсорных сетей, которые указываются заказчиком (область применения, тип внешней среды, способ развертывания, количество узлов, категория передаваемой информации и др.).

Исследованы типовые угрозы в беспроводных сенсорных сетях [3], а также актуальные методы защиты. Проанализирована классификация по уровням модели OSI актуальных для WSN-сетей атак, которая систематизирует основные методы защиты и меры противодействия от рассмотренных атак [4].

После анализа был разработан прототип системы поддержки принятия решений, который позволяет заказчику принимать корректные обоснованные решения.

Физические модели сетей формируются в результате работы алгоритмов выбора топологии и технических средств узлов, расчета количества кластеров сети, представленных в виде нечетких моделей – наборов нечетких фактов и правил. Задача проектирования безопасной WSN-сети сводится к построению формализаций на основе декомпозиции общей задачи проектирования. В процессе разработки первых двух блоков (начальной подготовки и формализации экспертных знаний) было собрано множество данных для анализа и сформирована база знаний. Блок анализа и рекомендаций состоит из формализованных экспертных знаний в области методов обеспечения безопасности. WSN-сети были разделены на категории по размерности, областям применения, передаваемой информации, топологий. Заключающие два блока (анализа и рекомендаций, моделирования предметной области) отвечают за определение системы ключевых показателей и составление финального решения для заданных заказчиком параметров.

Из-за физического ограничения ресурсов беспроводных сенсорных узлов энергоэффективность является одним из основных ограничений при расчете оптимальной топологии беспроводных сенсорных сетей (БСС) [5]. Была разработана модель, осуществляющая подбор наиболее энергоэффективного разделения сети ячеистой топологии на кластеры на основе функции искажения скорости и модели энергопотребления в соответствии со схемой передачи данных в WSN.

На основе ранее разработанных формализаций экспертных знаний было разработано программное средство, в которое выдает рекомендации по построению безопасной сети и наиболее энергоэффективному разделению сети на отдельные кластеры в случае необходимости.

Для оценки эффективности разработанной системы проводилось моделирование WSN-сети в симуляторе TRMSim-WSN. Для примера использовалась распределенная промышленная сеть, развернутая в контролируемой среде, состоящая из 1000 узлов – 90% легитимны, 10% скомпрометированы. Скомпрометированные узлы реализовывали атаку выброса пакетов. После внесения изменений с учетом рекомендаций разработанной СППР процент потерянных пакетов в ходе моделирования снизился на 30%, а время работы сети увеличилось.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №19-37-90027\19.

СПИСОК ЛИТЕРАТУРЫ

1. Kandris D. et al. Applications of wireless sensor networks: an up-to-date survey //Applied System Innovation. – 2020. – Т. 3. – №. 1. – С. 14.
2. Krundyshev V., Kalinin M. The Security Risk Analysis Methodology for Smart Network Environments //2020 International Russian Automation Conference (RusAutoCon). – IEEE, 2020. – С. 437-442.
3. Pathan A. S. K., Lee H. W., Hong C. S. Security in wireless sensor networks: issues and challenges //2006 8th International Conference Advanced Communication Technology. – IEEE, 2006. – Т. 2. – С. 6 pp.-1048.
4. Boubiche D. E. et al. Cybersecurity issues in wireless sensor networks: current challenges and solutions //Wireless Personal Communications. – 2020. – С.
5. Yang M., He J., Zhang Y. Calculating the number of cluster heads based on the rate-distortion function in wireless sensor networks //The Scientific World Journal. – 2014. – Т. 2014.

УДК 004.032.6+.056.52

МЕТОДЫ ВИЗУАЛИЗАЦИИ ВЕКТОРОВ ДВИЖЕНИЯ СЖАТОГО ВИДЕОПОТОКА ДЛЯ ОЦЕНКИ ВОЗМОЖНОСТЕЙ ЕГО ИДЕНТИФИКАЦИИ

Фахрутдинов Роман Шафкатович, Мирин Анатолий Юрьевич
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: fahr@cobra.ru, mirin@cobra.ru

Аннотация. Рассмотрены методы визуализации векторов движения сжатого видеопотока для оценки возможности использования данных при решении задачи идентификации видеопоследовательности.

Ключевые слова: сравнение видеопоследовательностей; определение степени сходства видеоматериалов; визуализация векторов движения.

COMPRESSED VIDEO STREAM MOTION VECTORS VISUALIZATION METHODS TO ESTIMATING THE POSSIBILITIES ITS IDENTIFICATION

Fahrutdinov Roman, Mirin Anatoliy
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: fahr@cobra.ru, mirin@cobra.ru

Abstract. Compressed video stream motion vectors visualization methods considered to estimate the possibility solving the problem of identifying a video sequence.

Keywords: video sequence comparison; similarity of video sequences; visualization of motion vectors.

В настоящее время наблюдается взрывной рост количества видеоинформации, которая доступна пользователям через сеть Интернет. Пользователи самостоятельно создают видеоконтент, обмениваются им, совершают видеозвонки, используя видеохостинги, социальные сети, мессенджеры и другие видеосервисы.

Однако проблема идентификации видеопоследовательностей является нерешённой. Простые методы идентификации, такие, как использование метаданных (имена файлов или служебной информации в структуре видеопотока) или «водяные знаки» (специальные метки в видеоданных), недостаточно устойчивы для однозначной идентификации и могут быть изменены путём простого переименования или перекодирования видеопоследовательности (с изменением геометрии, добавлением «зерна» или использованием специальных видеофильтров).

Отсутствие возможностей по идентификации создаёт проблемы при контроле копирования видеоконтента [1], приводит к затратам видеохостингов на хранение дублирующих видеозаписей, усложняет контроль за распространением запрещённого (местным законодательством) контента [2], делает невозможным контроль просмотра с учётом возрастных норм и т.д.

Возможным способом идентификации является использование параметров самого видеопотока для его идентификации. Такими параметрами являются, например, гистограммы изменения яркости в зависимости от кадра изображения, соотношения динамичных и статических сцен, расстояния между ними, траектория движения объектов внутри кадра [3] и т.д. Одним из таких параметров являются вектора движения [4], которые описывают (в целом) динамику движения частей изображения между кадрами в процессе просмотра.

Использование векторов движения содержит ещё один дополнительный аспект, повышающий привлекательность его использования. Вектора движения могут быть извлечены из видеопотока без полного декодирования. Тем самым снижаются требования к производительности при получении идентификационных наборов данных. Т.к. видеопоследовательности имеют сравнительно большой размер (по сравнению с текстом и звуком), то это является существенным основанием для изучения использования такой возможности для идентификации.

Для оценки использования векторов движения видеопотока в качестве основы построения идентификаторов видео, необходимо предложить способы их визуализации (представления векторов движения видеопотока в виде графика приемлемой размерности). Видеопоток при этом, может иметь продолжительность более 1 часа видео (несколько десятков тысяч кадров).

В качестве вариантов решения этой задачи, предлагается рассмотреть к использованию возможные варианты визуализации векторов движения:

- график зависимости средних длин векторов в кадре от номера кадра;
- график зависимости общей длины векторов в кадре от номера кадра;
- гистограмма зависимости направления движения в кадре от номера блока.

Для последнего метода рассматривается возможность использования в визуализации помимо натурального следования номеров блоков в кадре (0, 1, 2, 3 …), способы ZigZag-сканирования блоков в кадре, а также прямого и обратного следования блоков по спирали.

СПИСОК ЛИТЕРАТУРЫ

1. Arun Hampapur, Rudolf M. Bolle. Comparison of Distance Measures for Video Copy Detection, IBM Research Report, RC 22056 (W0105-007) 14 May 2001, https://dominoweb.draco.res.ibm.com/reports/RC22056.pdf
2. Министерство юстиции Российской Федерации, официальный сайт, https://minjust.gov.ru/ru/extremist-materials/
3. R.Roopalakshmi, G.Ram Mohana Reddy. A Novel CBCD Approach Using MPEG-7 Motion Activity Descriptors. 2011 IEEE International Symposium on Multimedia, 5-7 Dec. 2011, P. 179-184
4. Kasım Taşdemir, A. Enis Çetin. Content-based video copy detection based on motion vectors estimated using a lower frame rate. Springer-Verlag London 2014, Issue date: September 2014, P. 1049–1057

УДК 003.26

УДВОЕНИЕ ПРОВЕРОЧНОГО УРАВНЕНИЯ КАК СПОСОБ ПОСТРОЕНИЯ АЛГОРИТМОВ ЦИФРОВОЙ ПОДПИСИ, ОСНОВАННЫХ НА СКРЫТОЙ ЗАДАЧЕ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ

Фахрутдинов Роман Шафкатович[1], Мирин Анатолий Юрьевич[1], Молдовян Николай Андреевич[2]

[1] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия

[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: fahr@cobra.ru, mirin@cobra.ru, nmold@mail.ru

Аннотация. Удвоение проверочного уравнения обсуждается как способ построения алгоритмов цифровой подписи, основанных на скрытой задаче дискретного логарифмирования. Способ может быть реализован с использованием одной или двух независимых конечных ассоциативных алгебр как носителей криптосхемы. В качестве последних могут использоваться коммутативные и некоммутативные алгебры. При использовании

коммутативных алгебр представляют интерес алгебры, мультипликативная группа которых обладает многомерной цикличностью.

Ключевые слова: конечные алгебры; ассоциативные алгебры; криптосхемы с открытым ключом; алгоритмы цифровой подписи.

DOUBLING OF THE VERIFICATION EQUATION AS A DESIGN METHOD OF THE SIGNATURE ALGORITHMS BASED ON THE HIDDEN DISCRETE LOGARITHM PROBLEM

Fahrutdinov Roman[1], Mirin Anatoliy[1], Moldovyan Nikolay[2]

[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia

[2] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia

e-mails: fahr@cobra.ru, mirin@cobra.ru, nmold@mail.ru

Abstract. Doubling the verification equation is discussed as a way of constructing digital signature algorithms based on a hidden discrete logarithm problem. The method can be implemented using one or two independent finite associative algebras as carriers of the cryptoscheme. Commutative and non-commutative algebras can be used as the carriers. When using commutative algebras, algebras whose multiplicative group has multidimensional cyclicity are of interest.

Keywords: finite algebras; associatrive algebras; public-key cryptoschemes; digital signature algorithms.

Одно из направлений разработки постквантовых схем электронной цифровой подписи (ЭЦП) связано с использованием вычислительной трудности скрытой задачи дискретного логарифмирования (СЗДЛ) [1, 2]. При построении алгоритмов ЭЦП данного типа задаются специальные конструктивные критерии, направленные на предотвращение возможности прямолинейного применения квантового вычислителя для нахождения значения дискретного логарифма x. Один из критериев формулируется как требование того, что построение периодических функций по известным параметрам алгоритма приводит к получению периодов, длины которых не зависят от значения x. Для реализации схем ЭЦП, удовлетворяющих данному критерию, предложено использование скрытой группы, обладающей двухмерной цикличностью, и новый конструктивный прием – удвоение проверочного уравнения [3]. В настоящем сообщении, упомянутый прием рассматривается как более общий способ построения алгоритмов ЭЦП, основанных на СЗДЛ.

Способ построения алгоритмов ЭЦП, включающий удвоение проверочного уравнения, требует использования двух независимых открытых ключей, образующих единый открытый ключ пользователя. Тем не менее, интерес к данному способу определяется тем, что он потенциально позволяет разработать достаточно практичные постквантовые схемы ЭЦП, основанные на СЗДЛ. Необходимость удвоения проверочного уравнения возникает из-за того, что один из элементов подписи используется как множитель в проверочном уравнении и может быть использован как подгоночный параметр в алгоритмах подделки подписи. При удвоении проверочного уравнения, данный элемент подписи должен удовлетворять независимым проверочным уравнениям, что потенциально предотвращает атаки данного типа на схему подписи. Однако, следует учитывать, что прием удвоения проверочного уравнения и открытого ключа не решает автоматически данную проблему подделки подписи. Требуется соответствующим образом составить проверочные уравнения, используемые в процедуре проверки ЭЦП, и использовать согласованные с ними процедуры формирования удвоенного открытого ключа. После этого целесообразно рассмотреть атаку по подделке подписи для каждого из проверочных уравнений с целью выявления возможных случаев, когда подгонка по одному из уравнений всегда будет обеспечивать и подгонку по второму уравнению.

При соблюдении отмеченных требований к построению схем ЭЦП с удвоенным поверочным уравнением, рассматриваемый способ может быть использован как общий метод построения алгоритмов ЭЦП. Он существенно расширяет класс алгоритмов, основанных на вычислительной трудности СЗДЛ, и даёт возможность использования в качестве алгебраического носителя не только некоммутативных, но и коммутативных конечных ассоциативных алгебр. При использовании последних представляют интерес алгебры, мультипликативная группа которых обладает многомерной цикличностью (к ним относятся конечные группы с двумя и более образующими, обладающих одним значением порядка). Также в рамках одной схемы ЭЦП могут использоваться различные алгебры, в том числе коммутативные и некоммутативные. При разработке схем подписи данного типа весьма важно иметь данные по структуре используемых алгебр. В частности, по строению некоммутативных алгебр как множества коммутативных подалгебр и строению последних.

СПИСОК ЛИТЕРАТУРЫ

1. Moldovyan N.A., Moldovyan A.A. Finite Non-commutative Associative Algebras as Carriers of Hidden Discrete Logarithm Problem // Вестник ЮУрГУ. Серия “Математическое моделирование и программирование”. 2019. Т. 12. № 1. С. 66−81. DOI: 10.14529/mmp190106.
2. Молдовян Н.А., Абросимов И.К. Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23–32.
3. Moldovyan N.A., Moldovyan A.A. Candidate for practical post-quantum signature scheme. Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2020. Т. 16. Вып. 4. С. 455–461. https://doi.org/10.21638/11701/spbu10.2020.410.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

УДК 004.652.4

ПОДХОД К ОБНАРУЖЕНИЮ ВРЕДОНОСНЫХ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Аль-Барри Мазен Хамед, Саенко Игорь Борисович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: mazenb51@gmail.com, ibsaen@mail.ru

Аннотация. В настоящее время центры обработки данных приобретают все большую популярность при работе большинства типов учреждений, так как они надежно сохраняют и пересылают данные между пользователями и устройствами хранения. Учитывая важность данных, содержащихся в центрах обработки данных, вопросы обеспечения их безопасности приобретают большую значимость для противодействия потенциальным внешним и внутренним угрозам. В статье рассмотрен подход к обнаружению аномального поведения пользователей центров обработки данных, основанный на применении искусственных нейронных сетей, включенных в состав аналитического блока, который можно размещать на одном из узлов локальной вычислительной сети. Экспериментальная оценка показала, что возможно применение этого аналитического блока как вспомогательного средства для выявления аномалий в журналах транзакций центра обработки данных.

Ключевые слова: центр обработки данных; аномалий; классификатор; искусственная нейронная сеть; система защиты информации.

AN APPROACH TO DETECT HARMFUL ACTIONS BY USERS OF DATA CENTERS

Al-Barri Mazen, Saenko 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: mazenb51@gmail.com, ibsaen@mail.ru

Abstract. Nowadays, data centers are becoming increasingly popular with most types of institutions because they securely store and transfer data between users and storage devices. Given the importance of data contained in data centers, issues of ensuring their security become more important in countering potential external and internal threats. The paper discusses an approach to detecting anomalous behavior of users of data centers, based on the use of artificial neural networks included in the analytical unit, which can be placed on one of the nodes of the local computer network. Experimental evaluation has shown that it is possible to use this analytic unit as an aid to identifying anomalies in the data center transaction logs.

Keywords: data center; anomalies; classifier; artificial neural network; information security system.

Введение. Вопросы обнаружения аномального поведения пользователей в автоматизированных системах управления актуальны на протяжении последних десятилетий. В настоящее время, после появления распределенных облачных сервисов и их широкого распространения, важность роли центров обработки данных (ЦОД) возросла, и поэтому проблемы безопасности, связанные с ними, неуклонно возрастают. ЦОД играют важную роль в системах управления различного назначения. Они составляют информационно-техническую основу облачной инфраструктуры, так как поддерживают хранилище разнородной информации, которая используется пользователями в собственных интересах [1].

По этой причине ЦОД являются объектами, на которые в первую очередь нацеливаются нарушители безопасности в целях получения информации или нарушения работы центров. При этом они могут быть как внутренними, так и внешними нарушителями [2].

При построении систем защиты информации ЦОД могут использоваться различные методы поиска аномалий, обладающие той или иной степенью эффективности. Однако эти аномалии обычно обнаруживаются в сетевом трафике. Но аномалии сетевого трафика не отражают неправильное, ненормальное поведение пользователя ЦОД при работе с базами данных. Эти действия можно обнаружить только путем анализа регистрационных журналов базы данных. Такой анализ, направленный на выявление аномального поведения пользователей ЦОД, в настоящее время либо не проводится, либо проводится не в полном объеме.

Особенность БД как объекта компьютерной атаки заключается в том, что атака реализуется через изменение SQL запросов [3]. В то же время измененные запросы к БД могут создаваться доверенными пользователями. Выявить такие нарушения чрезвычайно сложно. Однако, учитывая, что практически во всех СУБД на ЦОД ведутся регистрационные журналы, в которых фиксируются все действия пользователей, представляется возможным разработать способ обнаружения аномальных SQL запросов и, тем самым, выявить среди пользователей ЦОД потенциального нарушителя информационной безопасности, если проводить анализ регистрационных журналов с помощью методов машинного обучения. На этом основана идея предлагаемого подхода, рассматриваемого в докладе.

Для реализации предложенного подхода к обнаружению аномалий в действиях пользователей ЦОД целесообразно разместить на узле вычислительной сети ЦОД аналитический блок с возможностью получения данных из журнала транзакций БД в режиме времени, приближенном к реальному.

Аналитический блок должен иметь в своем составе:

- модуль преобразования исходных данных;
- модуль, содержащий искусственные нейронные сети;
- модуль интерпретации полученных результатов.

Как правило, журнал транзакций хранится в виде одного или нескольких постоянно обновляемых файлов. В журнале, в текстовом виде содержится информация о событиях базы данных и о пользовательских запросах. По умолчанию в запись журнала включена следующая информация:

- дата запроса;
- время запроса;
- источник запроса;
- информация о событии (запросе).

Предлагаемый подход включает следующие этапы:

1) определение перечня типов аномалий, которые возможны в SQL запросах;

2) формирование и предварительная обработка набора данных для анализа на предмет определения аномалий;

3) формирование обучающей выборки и обучение с их помощью выбранных классификаторов;

4) использование обученных классификаторов для непосредственного выявления аномальных SQL запросов.

На первом этапе представляется необходимым разработать модель представления аномалий. Эта модель должна представлять множество возможных атак на БД и демонстрировать, каким образом эти атаки отображаются на записи регистрационного журнала.

На втором этапе следует предложить с максимальной полнотой дополнительные признаки, которые следует включить в набор данных, формируемый исходя из записей регистрационного журнала и играющий роль обучающей выборки. Таковыми признаками могут быть средние значения, дисперсии, частоты появления в наборе данных запросов определенного типа и прочие признаки.

На третьем и четвертом этапах применяются различные классификаторы, основанные на тех или иных методах машинного обучения. В перечень анализируемых методов включены следующие классификаторы: метод главных компонентов, машина опорных векторов, метод k-ближайших соседей, линейная регрессия, двухслойный персептрон, дерево решений. Эти классификаторы являются наиболее распространенными в практике обнаружения аномалий [4]. Каждому из них свойственны свои достоинства и недостатки. Анализ их возможностей показал, что наибольшей целесообразностью применения в предлагаемом подходе обладают машина опорных векторов и дерево решений.

Заключение. В статье рассмотрен подход к обнаружению аномального поведения пользователей ДЦ на основе применения искусственных нейронных сетей, включенных в состав специализированного программно реализованного аналитического блока, размещенного на одном из узлов локальной вычислительной сети ДЦ.

По итогам анализа полученных результатов возможно применение аналитического блока в текущем виде как вспомогательного средства для выявления разного рода аномалий, в том числе аномалий в журналах транзакций баз данных ЦОД.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко, И.В. Перспективные системы хранения данных для мониторинга и управления безопасностью информации / И.В. Котенко, И.Б. Саенко, О.В. Полубелова // Труды СПИИРАН. – 2013. – Вып. 2 (25). – С.113-134.
2. Kant, K. Security considerations in data center configuration management / K. Kant, M. Le, S. Jajodia // Proceedings of the 2011 4th Symposium on Configuration Analytics and Automation (SAFECONFIG). – 2011. – Pp. 1–9.
3. Mousa, A. Database Security Threats and Challenges / A. Mousa, M. Karabatak, T. Mustafa // 2020 8th International Symposium on Digital Forensics and Security (ISDFS). – 2020. – Pp. 1-5.
4. Браницкий, А.А. Методика многоаспектной оценки и категоризации вредоносных информационных объектов в сети Интернет / А.А. Браницкий, И.Б. Саенко // Труды учебных заведений связи. – 2019. – Т. 5, № 3. – С. 58-65.

УДК 004.056

ПОДХОДЫ К ЗАЩИЩЕННОМУ ПОСТРОЕНИЮ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

Ащеулов Сергей Викторович, Горденко Артем Дмитревич, Колосовский Никита Эдуардович, Шинкарев Семен Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: se_men82@mail.ru, colos.nikita@gmail.com

Аннотация. В публикации приведен тщательный и детальный анализ результатов и подходов к защищенному построению распределенных вычислительных систем специального назначения, так же рассмотрены перспективность и актуальность различных направлений по обеспечению достоверности и безопасности информации на первичной сети общего пользования взаимоувязанной сети связи России.

Ключевые слова: распределенные вычислительные системы; защита информации; сети ограниченного пользования; криптография.

APPROACHES TO SECURE CONSTRUCTION OF DISTRIBUTION COMPUTING SYSTEMS

Asheulov Sergei, Gordenko Artem, Kolosovskiy Nikita, Shinkarev Semen
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: se_men82@mail.ru, colos.nikita@gmail.com

Abstract. In publication contains a thorough and detailed analysis of the results and approaches to the secure construction of distributed computing systems for special purposes to ensure the reliability and security of information on the primary public network.

Keywords: distributed computing system; protection of information; cryptography; restricted networks.

Введение. Современный подход к построению информационно-вычислительных систем предполагает преобразование информации любого вида и любой природы к единому формату и транспортирование ее в целях коллективного использования посредством глобальной информационно-вычислительной сети. Эта сеть будет являться основой для построения перспективной системы связи как вида войск, так и вооруженных сил в целом.

Перспективная интегральная цифровая система связи (ИЦСС) должна создаваться на основе преимущественного использования цифровой техники связи, интеграции в едином устройстве функций уплотнения, коммутации и засекречивания, создания универсальных (интегральных) оконечных средств пользователя, сокращения количества отдельных транспортных сетей и слияния их в конечном итоге в единую цифровую сеть интегрального обслуживания.

Конечной целью такой интеграции должно явиться предоставление пользователю множества услуг при использовании единых систем передачи и коммутации, объединения и автоматизации систем эксплуатационно-технического обслуживания и управления.

При разработке системы защиты информации перспективной ИЦСС, необходимо учитывать состояние и перспективы развития первичной сети общего пользования взаимоувязанной сети связи (ВСС) России, так как именно с ней взаимодействуют все первичные сети ограниченного пользования, к которым и относится первичная сеть МО РФ.

Учитывая специфику построения сети связи МО РФ, наибольшее внимание уделяется вопросам безопасности передачи информации между элементами сети. При этом все потенциально возможные нарушения безопасности информации в сетях делятся на два вида: пассивные и активные.

В качестве практического приема политики безопасности рассмотрим услуги ее предоставления.

1. Идентификация – процедура определения законности объекта для данной информационной системы.

2. Аутентификация – процедура определения того, является ли данный объект именно таким, каким он себя представляет, или, для систем передачи, подтверждение подлинности защищаемой информации и обнаружения попыток ее подделать, то есть противостояние активным атакам.

3. Предоставление полномочий (авторизация) – определение сферы действий объекта и доступных ему ресурсов информационной системы.

4. Обеспечение конфиденциальности данных.

5. Обеспечение целостности данных.

Защищенность информации – это ее свойство быть известной только идентифицированным, аутотентифицированным и авторизованным субъектам информационной системы (пользователям, процессам, программам и средствам, реализующим эти программы). Для всех остальных эта информация должна быть неизвестна.

Процедура доступа субъекта к объекту определяется как совокупность реализации следующих механизмов политики безопасности, а именно: идентификации, аутентификации, авторизации.

Анализ более чем трех тысяч нарушений информационной безопасности показал, что самым распространенным является нарушение полномочий или несанкционированный доступ.

Одним из наиболее перспективных и актуальных направлений обеспечения достоверности и безопасности информации является концепция пролонгированной безопасности.

Гарантия пролонгированной безопасности важна для центров сертификации, а также для ряда криптографических приложений в тех случаях, когда восстановление режима безопасного взаимодействия сопряжено с дополнительными трудностями (например, организация секретного канала для связи с удаленными космическими станциями). Механизм пролонгированной безопасности позволяет минимизировать угрозу долговременной атаки. Пролонгированная безопасность построена на принципах распределенности и периодического обновления исходной информации.

В связи с этим возникает необходимость разработки математических методов, алгоритмов и нейросетевых средств надежной и безопасной обработки информации в распределенных вычислительных системах и, что в свою очередь, включает в себя разработку математических основ порогового доступа и блуждающих ключей в распределенных вычислительных сетях.

Одной из задач, связанных с обработкой и хранением данных, является защита информации от раскрытия и изменения. Предлагаемые новые криптоалгоритмы для шифрования данных, не дают гарантированной стойкости шифра, учитывая современное развитие вычислительной техники. Концепция, применяемая сегодня для защиты информации предполагает преобразование ее к другому виду посредством некоторых ключей (секретного или открытого и закрытого).

Для того чтобы завладеть информацией, хранящейся в современной вычислительной системе, необходимо похитить зашифрованные данные и ключ, а при наличии большой вычислительной мощности достаточно знания закрытой информации.

Следовательно, чтобы снизить вероятность раскрытия данных, необходимо увеличивать стойкость шифра или улучшать механизмы хранения ключей и данных. В первом случае подразумевается увеличение длины ключа или усложнение алгоритма вычисления, что приводит к большим аппаратным и временным затратам. Второй подход предполагает различные методы защиты от проникновения, такие как межсетевые экраны, многоуровневые системы доступа, смарт-карты, использование в качестве ключа отпечатка пальца, голоса пользователя вычислительной системы.

Перспективным направлением современной криптографии в технологии хранения ключей являются пороговые системы доступа, когда ключ хранится не в одном месте, а его части, называемые "тенями", распределены между элементами вычислительной системы. Чтобы получить ключ, противник должен "вскрыть" необходимое количество объектов сети, для получения всех теней ключа. Разделение ключа не принесет ожидаемого эффекта, если противник использует атаку методом перебора паролей, когда при криптоанализе в качестве пароля используются значения из словаря часто используемых паролей или значения генерируются из всех возможных символов для ввода пароля.

Для повышения надёжности хранения ключа предлагается распределить между элементами системы не ключ, а сами данные, то есть реализовать следующую схему. Если в эту схему включить шифрование полученных частей данных, то можно существенно понизить вероятность их раскрытия.

Задача состоит в нахождении оптимального преобразования данных для их разделения на тени. Простая разбивка файла данных может дать ожидаемый результат, т. к. по фрагментам данных восстановить весь файл (это особенно актуально для текстовых файлов и изображений). Что немаловажно, при потере одной из теней, весь документ восстановить будет проблематично, и избежать этого можно только дублированием. Дублирование, в свою очередь, делает уязвимым конечное шифрование ключей, т. к. наличие одного фрагмента данных, зашифрованного разными ключами, существенно упрощает криптоанализ.

Нестандартный выход из этой ситуации предоставляет Китайская теорема об остатках, которая лежит в основе системы остаточных классов (СОК).

Разделение информации между объектами вычислительной системы ещё малоизученный, но многообещающий подход к обеспечению безопасности информации. Интересен для рассмотрения вопрос разделения исходных данных между n объектами системы, таким образом, что любые из пользователей ($к \leq n$) могли бы получить исходную информацию. Это не только сделает удобнее использование этой системы, но и благодаря свойствам арифметики СОК контролировать правильность "теней" и избегать подмены или изменения защищаемой информации.

СПИСОК ЛИТЕРАТУРЫ

1. Пожидаев С.В., Горденко Д.В. Криптография как защита электронного документооборота. // В сборнике: Время науки. Сборник научных трудов I Международной научно-практической конференции. 2019. С. 35-41.
2. Юрданов Д.В., Горденко Д.В., Горденко Н.В., Петлина Е.М., Павлюк Д.Н. К вопросу применения системы остаточных классов в современных устройствах цифровой обработки сигналов. // Фундаментальные исследования. 2016. № 2-2. С. 318-322.
3. Горденко Д.В., Горденко Н.В. Естественная избыточность в системе остаточных классов. // В сборнике: Студенческая наука для развития информационного общества. Сборник материалов III Всероссийской научно-технической конференции. 2015. С. 126-129.
4. Резеньков Д.Н., Горденко Д.В., Минкина Т.В., Брыкалова А.А. Обнаружение и коррекция ошибок в системе остаточных классов систематическими кодами. // Вестник СевКавГТИ. 2015. № 4 (23). С. 172-175.
5. Горденко Д.В., Павлюк Д.Н., Шапошников Е.В., Кондрашов А.В., Горбачев А.В. Обнаружение ошибок с самоконтролем в модулярной арифметике. // Вестник СевКавГТИ. 2015. № 1(20). С. 202-207.

УДК 004.054

ОРГАНИЗАЦИЯ ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОКОММУНИКАЦИОННЫМИ СЕТЯМИ

Ащеулов Сергей Викторович, Деев Александр Владимирович, Зверев Александр Львович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: zal16@mail.ru

Аннотация. Описаны проблемные вопросы, требующие внимания при решении задачи организации процессов управления инфокоммуникационными сетями. Даны функции автоматизированных систем управления инфокоммуникационными сетями. Приводятся основные преимущества органов управления при внедрении сетевого управления.

Ключевые слова: инфокоммуникационные сети; автоматизированные системы управления; управление; планирование связи.

ORGANIZATION OF MANAGEMENT PROCESSES INFOCOMMUNICATION NETWORKS

Ascheulov Sergey, Deev Alexander, Zverev Alexander
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: zal16@mail.ru

Abstract. The problematic issues that require attention when solving the problem of organizing management processes of infocommunication networks are described. The functions of automated control systems for infocommunication networks are given. The main advantages of the controls in the implementation of network control are given.

Keywords: infocommunication networks; automated control systems; control; communication planning.

Введение. Управление современными инфокоммуникационными сетями **(**ИКС) требует применения соответствующих программно-аппаратных платформ, которые обеспечивают необходимый уровень качества предоставляемой услуги связи в любое время и с минимальными эксплуатационными затратами. Кроме того, для решения поставленной задачи целесообразно создавать специальную сеть управления, обеспечивающую управление ИКС путем организации взаимосвязи с компонентами различных систем связи на основе единых интерфейсов и протоколов [1].

Наметившиеся в последние годы тенденции конвергенции услуг и сетей, выдвигают на первое место задачи более высоких уровней управления. Их успешное решение возможно только при использовании комплексов специализированного программного обеспечения, включающего прикладные системы управления сетями и услугами ИКС. При этом предполагается широкое применение специальной архитектуры и технических решений для достижения управляемости различных типов телекоммуникационного оборудования и систем связи в составе ИКС.

Основная задача управления при этом – это обеспечение функционирования ИКС с заданными показателями эффективности при внешних и внутренних воздействиях. В общем случае процесс управления включает следующие этапы: получение информации о состоянии ИКС, анализ полученной информации, выработка решения и исполнение решения, т.е. осуществление управляющих воздействий. Системы управления ИКС состоят из программно-аппаратных средств, оперативного и административного персонала, обеспечивающих управление, и относятся к классу автоматизированных систем управления (АСУ) [2, 3].

Основные функции АСУ ИКС:

– контроль за качеством прохождения информации по управлению;

– контроль за состоянием телекоммуникационных сетей в составе ИКС;

– управление функционированием телекоммуникационных сетей ИКС в соответствии с условиями обстановки.

Важной задачей при создании АСУ ИКС является рациональное распределение функций управления между персоналом органов управления и аппаратно-программными средствами. Неоднородность систем управления приводит к прерыванию в информационных потоках, замедлению процессов выработки управляющих команд и повышению вероятности возникновения ошибок.

Необходимо отметить, что при внедрении современного комплекса сетевого управления, даже при наличии устаревшего оборудования, орган управления ИКС получает следующие преимущества:

– повышается качество услуг связи и обслуживания ИКС;

– оперативно обнаруживаются и устраняются неисправности;

– снижаются эксплуатационные расходы и появляются дополнительные возможности за счет качественно новых услуг, что создает предпосылки для дальнейшего расширения модернизации сетей ИКС;

– орган управления ИКС может контролировать других пользователей, пользующихся той же сетью связи;

– орган управления ИКС может контролировать техническое состояние и работоспособность как отдельных узлов, так и всей ИКС в целом;

– орган управления получает возможность контролировать абонентские линии и управлять потоками вызовов, анализировать трафик, а также принимать обоснованные решения по вопросу номенклатуры услуг и обслуживания сетей ИКС.

Создаваемые АСУ ИКС в той или иной мере должны учитывать иерархию организационных уровней управления, существующую для ЕСЭ РФ на ближайшую и отдаленную перспективу.

Весь комплекс задач управления ИКС в целом условно разделяется на задачи технологического управления (управление средствами связи), оперативно-технического управления (учет, контроль, анализ, поддержание требуемых параметров и характеристик телекоммуникационных сетей ИКС и услуг, предоставляемых ей) и задачи организационного управления (задачи планирования) [4].

Одной из важнейших задач, которую необходимо решать при организации технологического управления оборудованием ИКС, является задача оперативного мониторинга состояния ее элементов и, в первую очередь, мониторинг коммутационного оборудования. Решение задач мониторинга состояния коммутационного оборудования ИКС обычно осуществляется по схеме «менеджер-агент» с применением стандартных протоколов управления, среди которых могут быть использованы протоколы CMIP или SNMP [5].

Задачи планирования при управлении ИКС тесно связаны с задачами планирования связи вообще, которые наряду с задачами оперативно-технического управления являются наиболее важными при управлении, представляют собой процесс постановки целей, которые требуется достичь, и разработки программы их достижения, оформленной в виде совокупности документов по связи, основным из которых является план связи. Содержанием процесса планирования является распределение ресурсов ИКС и определение порядка их использования. Сущность и содержание планирования связи определяется ее целевым предназначением, характером функционирования и принципами применения в той или иной оперативной обстановке.

Вместе с тем, изменение соотношения между функциями и задачами оперативно-технического и организационного управления зависит не только от структурных изменений, но и от специфических особенностей ИКС как объекта управления. Так в области оперативно-технического управления ИКС эти особенности требуют реализации значительной доли функций управления технологическими средствами без вмешательства сотрудников органов управления и оперативно-технического персонала в процессы восстановления в реальном масштабе времени. Это означает необходимость введения в состав каждого элемента ИКС (средства, комплекса связи) доли автоматов, обеспечивающих наблюдаемость состояний этих элементов, а также более широкого использования средств принятия решений и исполнительных элементов по восстановлению их работоспособности на основе встроенных средств автоматизации. В области организационного управления требуемое качество управления ИКС с учетом указанных особенностей должно быть обеспечено при создании и функционировании унифицированных типовых комплексов средств управления (КСУ) АСУ ИКС на основе новых информационных технологий, которые обеспечат возможность повышения уровня творческого решения задач в области организационного управления при участии сотрудников органов управления связью в процессе управления.

Заключение. Выполнение целей, поставленных перед системой управления ИКС, в конечном итоге, должно гарантировать функционирование ИКС в целом и отдельных сетей, входящих в ее состав, с требуемой эффективностью. Управление ИКС будем считать эффективным, если оно обеспечивает требуемую (заданную) эффективность функционирования самой ИКС в условиях воздействия на нее и систему управления сетью различных естественных и преднамеренных дестабилизирующих факторов (в т.ч. программно-аппаратных атак).

СПИСОК ЛИТЕРАТУРЫ

1. Вентцель Е.С. Исследование операций – М.: сов. Радио, 1977.
2. Анфилатов В.С., Емельянов А.А., Кукушкин А.А. Системный анализ в управлении – М. Финансы и статистика, 2002.
3. Буренин А.Н., Легков К.Е. Модели организации информационной управляющей сети для систем управления современными инфокоммуникационными сетями // Наукоемкие технологии в космических исследованиях Земли. 2012.
4. Легков К.Е. К вопросу организации процессов управления инфокоммуникационными сетями специального назначения // Наукоемкие технологии в космических исследованиях Земли. 2014.
5. Гребешков А.Ю. Стандарты и технологии управления сетями связи. М.: Эко-Тренд. 2003. 288 с.

УДК 004.7

ПЕРСПЕКТИВЫ РАЗВИТИЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Бабич Борис Иванович, Зубакин Владимир Валентинович, Троцко Алиса Викторовна, Шинкарев Семен Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: se_men82@mail.ru

Аннотация. В настоящее время состояние инфотелекоммуникационных сетей показывает, что возможности традиционных технологий практически исчерпаны. Одним из вариантов развития инфотелекоммуникационных сетей является переход на концепцию программно-конфигурируемых сетей. Программно-конфигурируемый подход предлагает разделить уровень управления и уровень передачи данных путем переноса функций управления на отдельное устройство (контроллер).

Ключевые слова: сеть передачи данных; управление; задачи; свойства.

PROSPECTS FOR THE DEVELOPMENT OF DATA TRANSMISSION NETWORKS

Babich Boris, Zubakin Vladimir, Trocko Alisa, Shinkarev Semen
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: se_men82@mail.ru

Abstract. Nowadays the state of infotelecommunications networks shows that the capabilities of traditional networks have been exhausted. One of the development options of infotelecommunications networks is the transition to the concept of software-configurable networks. Software-configurable approach proposes to divide the level of control and the level of data transfer by the way of transferring the control function to a separate device(controller).

Keywords: data transmission network; management; tasks; features.

Введение. Современное состояние и тенденции развития компьютерных сетей показали, что потенциал роста производительности, пропускной способности сетей на основе традиционных технологий практически исчерпан. Это связано с ростом затрат времени на маршрутизацию, с трудностями в конфигурации сети и управления потоками в ней, особенно с учётом новых потребностей в политиках качества сервиса для высокоскоростных глобальных сетей и сетей центров обработки данных, с ростом потребности виртуализации сетей, т.е. отображения нескольких логически изолированных сетей с независимыми политиками качества обслуживания на общий набор сетевых ресурсов.

Одна из важнейших задач построения и развития сетей передачи данных связана с использованием принципиально новых сетевых технологий, связанных с рациональным построением сети передачи данных, включающих целый комплекс новых задач научного и практического характера, к которым следует отнести обоснование методики, разработку и совершенствование алгоритмов синтеза структуры сетей.

В сетях передачи данных можно выделить 4 основных уровня управления так, что каждый последующий включает в себя предыдущие.

1. Поддержание в рабочем (исправном) состоянии отдельных технических средства, когда ОУ являются отдельные устройства, каналы, передатчики, приемники, блоки каналообразующей и коммутационной аппаратуры, устройства питания и т.п. Целью управления в данном случае является поддержание в норме (регулирования) отдельных параметров аппаратуры (напряжений, уровней сигналов, усиления частоты уровня шумов, контактного давления и т.п.) и содержание отдельных устройств в исправности.

2. Управление доставкой сообщений по адресу (в сети с коммутацией каналов установлением соединения), когда объектами управления являются коммутационные системы узлов коммутации каналов и сообщений. Здесь основной целью управления будут выбор пути (путей), создание тракта передачи в соответствии с адресом и удовлетворение дополнительных требований по приоритету времени доставки, выделению каналов соответствующего качества и т.п., в соответствии с заданным алгоритмом.

3. Управление распределением каналов и регулирование потоков сообщений, когда объектами управления являются системы кроссирования, а основной целью - распределение и перераспределение каналов между вторичными сетями, создание пучков прямых каналов и выработка алгоритмов выбора путей для обеспечения удовлетворения требований доставки сообщений при изменениях сети или потоков. В некоторых случаях на этом уровне может приниматься решение об ограничении приема заявок определенного приоритета или от определенных пользователей. Реализация принятых решений может осуществляться на уровне управления доставкой сообщений.

4. Управление сетью в целом как технико-экономической системой являвшейся частью народного хозяйства и включающей как технические средства доставки информации, так и людские коллективы обслуживающий эти средства. Целью этого управления являются не только поддержание функционирования сети и материально-техническое обеспечение этого функционирования, но и планирование развития сети, создание тарифов и законодательных актов пользования сетью, а также регулирование отношений с пользователями.

Одним вариантов развития сетей передачи данных является переход на концепцию программно-конфигурируемых сетей, в основе которой лежит два принципа:

– перенос слоя управления из сетевых устройств (маршрутизаторов и коммутаторов) в центральное внешнее устройство – контроллер сети;

– унификация механизма продвижения и интерфейса между механизмом продвижения и контроллером.

Целью программно-конфигурируемых сетей является обеспечение гибкой, дифференциальной обработки трафика.

Необходимое свойство, которым должна обладать система программно-конфигурируемых сетей, - это отсутствие зависимости программного обеспечения контроллера от производителя коммутаторов. Чтобы контроллер мог управлять коммутаторами от разных производителей однотипно, они должны строго соответствовать так называемой стандартной абстрактной модели коммутатора. Модель описывает формат таблицы продвижения и определяет набор действий, которые коммутатор может выполнить над пакетом: передать на определенный порт, отбросить, изменить значение определенного поля заголовка и т.п. Кроме того, остается еще одно важное условие универсальности приложения программно-конфигурируемых сетей – должен

существовать единый стандарт на программный интерфейс API, предоставляемый ОС контроллера приложениям.

Еще одним новым направлением обеспечения программируемости сетей наряду с рассмотренной концепцией программно-конфигурируемых сетей является концепция виртуализация сетевых функций (NFV).

Эта концепция состоит в том, что функции сетевых устройств – маршрутизаторов, коммутаторов, файерволов и др. – реализуется не на аппаратной специализированной платформы, а программным путем в серверах общего назначения.

Можно считать подход виртуализации сетевых функций развитием популярной концепции виртуальных машин, согласно которой, за счет слоя виртуализации – гипервизора – на основе физических ресурсов одного компьютера создается несколько виртуальных машин со своей собственной ОС и приложениями. В виртуальном мире концепции создаются программные единицы, эмулирующие не только физический компьютер, но и физические сетевые устройства, в результате чего программным путем создается виртуальная сеть, функционально аналогичная реальной сети.

К ключевым преимуществам виртуализации сетевых функций относятся следующие: меньше места для размещения сетевого оборудования; снижение энергопотребления; сокращение затрат на обслуживание сети; простая и быстрая модернизация сети.

Виртуализация сетевых функций — это часть изменений, которые происходят в работе и взаимодействии сетевого программного и аппаратного обеспечения. В сочетании с сетями передачи данных технология виртуализации сетевых функций создает среду с разнообразными возможностями автоматизации и программирования. Кроме того, виртуализация сетевых функций позволяет разворачивать более клиентоориентированные сетевые инфраструктуры, динамично адаптирующиеся к потребностям и требованиям клиентов, что позволит решать множество задач по перераспределению потоков на сети, восстановление сети, повышения качества обслуживания и много другое. При этом для каждой задачи должны быть четко сформулированы требования, определены параметры и критерии. Где в случае необходимости сеть передачи данных будет перестраиваться в требуемый момент времени для решения конкретной задачи.

Заключение. Таким образом, одним из вариантов развития инфотелекоммуникационных сетей является переход на концепцию программно-конфигурируемых сетей. Программно-конфигурируемый подход, в свою очередь, предлагает разделить уровень управления и уровень передачи данных путем переноса функций управления на отдельное устройство.

СПИСОК ЛИТЕРАТУРЫ

1. Чуднов А.М., Кирик Д.И., Курашев З.В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений/ Радиотехнические и телекоммуникационные системы. - 2017. -№2. с.41-49.
2. Маркин В. Г., Рыжкова А. Г. Протоколы маршрутизации в мобильных самоорганизующихся сетях // Теория и техника радиосвязи, 2013, №4, с.48-56. Siachalou S. Efficient QoS routing.// The International Journal of Computer and Telecommunications Networking. 2003. vol. 43. iss. 3. p. 351-367.
3. Чуднов А. М., Курашев З. В. Принципы формирования маршрутных таблиц на основе оптимизации распределения потоков в сети передачи данных. // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9, № 6 с. 46–51.
4. Паращук И.Б. Саенко И.Б. Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конференции. Севастополь, 22-26 сентября 2020 г. / Севастопольский государственный университет, науч. ред. Б.В. Соколов. – Севастополь: СевГУ, Том2, 2020. – 179 с., С. 243-249.

УДК 004.056.5

ОЦЕНКА ВЛИЯНИЯ АТАК НА БЕСПРОВОДНЫЕ СЕТИ СЕМЕЙСТВА СТАНДАРТОВ IEEE 802.11

Бабков Иван Николаевич, Абраменко Георгий Тимофеевич, Коновалова Виктория Вадимовна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: ib9809@mail.ru, georgabramenko@gmail.com, konovalova.viktoriya.99@mail.ru

Аннотация. В докладе обосновывается актуальность оценки влияния атак на беспроводные сети семейства стандартов IEEE 802.11. Рассматриваются особенности стандартов, влияющих на безопасность функционирования сетей. Проводится оценка влияния атак на беспроводные сети.

Ключевые слова: IEEE 802.11; Wi-Fi; безопасность беспроводных сетей; evil twin; dos; arp-spoofing.

ASSESSING THE IMPACT OF ATTACKS ON WIRELESS NETWORKS OF THE IEEE 802.11 FAMILY OF STANDARDS

Babkov Ivan, Abramenko Georgii, Konovalova Viktoria
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: ib9809@mail.ru, georgabramenko@gmail.com, konovalova.viktoriya.99@mail.ru

Abstract. The report substantiates the relevance of assessing the impact of attacks on wireless networks of the IEEE 802.11 family of standards. The features of the standards that affect the security of the functioning of networks are considered. The impact of attacks on wireless networks is being assessed.

Keywords: IEEE 802.11; Wi-Fi; wireless security; evil twin; dos; arp-spoofing.

Альтернативой проводного решения для построения локальных сетей в настоящее время являются беспроводные сети, использующие вместо кабелей — радиоэфир. В подавляющем большинстве случаев подобные сети формируются как беспроводные локальные сети, базирующиеся на стандартах IEEE 802.11. Технологии беспроводных локальных вычислительных сетей (Wireless Local Area Network – WLAN) развиваются с каждым днём и стали необходимой частью жизни общества. WLAN раскрывают новые способности для их пользователей – прежде всего мобильность терминалов и простоту изменения конфигурации сети. Даже крупные организации создадут свои сети с возможностью беспроводного подключения, в рамках концепции BYOD (Bring Your Own Device) [1]. Концепция подразумевает, что каждый сотрудник может принести и использовать своё собственное мобильное устройство для работы, а также использовать проводную или беспроводную сеть.

Не только в компаниях, но и в повседневной жизни люди сталкиваются с беспроводными сетями повсюду. Однако при использовании таких сетей необходимо учитывать проблему их слабой защищенности. Так, например, согласно данным исследований Positive Technologies, 7 из 8 корпоративных беспроводных сетей были доступны за пределами контролируемой зоны, что потенциально позволяет проводить атаки [2].

Стандарты IEEE 802.11 для сетей WLAN были разработаны в 1997 г. по инициативе IEEE (Institute of Electrical and Electronics Engineers) с целью создания беспроводного расширения для стандартов локальных вычислительных сетей (ЛВС) 802 серии. Стандарт описывает физический и MAC – уровень (подуровень управления доступом к среде) беспроводных ЛВС. Важнейшим структурным блоком сетей IEEE 802.11 является базовая зона обслуживания – набор станций, которые могут связываться друг с другом, но при этом остаются под контролем одной из них, выполняющей координирующие функции. Расширенная зона обслуживания формируется с помощью точек доступа (обеспечивает взаимодействие беспроводных клиентов с проводной инфраструктурой сети), соединенных разделительной системой. Также, IEEE 802.11 допускает перемещение устройств из одной зоны точки доступа в зону другой (роуминг), тем самым обеспечивая мобильность.

Несмотря на все достоинства вышеописанного стандарта, проблема незащищенности беспроводных сетей имеет особый характер, так для передачи данных используется радиоканал, а средой передачи является воздушное пространство. В пределах радиуса действия сетевого оборудования возможно узнать имя беспроводной сети (SSID) и MAC адрес обнаруженного устройства, что позволяет даже низкоквалифицированному нарушителю совершать атаки, используя готовые инструменты операционных систем из семейства UNIX.

Актуальность защиты беспроводных сетей в будущем будет увеличиваться все больше и больше, поэтому необходимо исследовать работу как контроллерных, так и не контроллерных точек доступа во время атак и предлагать адекватные механизмы защиты. Обычно такие исследования работы точек доступа во время атак проходят в рамках сертификаций или аудита по информационной безопасности и имеют ограниченный доступ к конкретным результатам. Поэтому существует необходимость в создании специальной среды для исследования работ точек во время атак, где не будет затронута ничья конфиденциальность.

Исследование работы точек доступа можно выполнить с помощью пентеста. Основная цель пентеста — подтвердить или опровергнуть риски несанкционированного доступа к защищаемой информации с помощью найденных уязвимостей. А главный принцип выполнения — обеспечить необходимую доказательность путем применения техник, методов и инструментария, используемых злоумышленниками. Зачастую злоумышленник проникает во внутреннюю сеть атакуемой компании, используя внешние объекты в качестве опорной платформы для развития и расширения поверхности атаки. Большинство компаний не готовы отразить такие нападения. Тестирование на проникновение помогает предприятию выстроить эффективные процессы обеспечения безопасности.

В связи с вышеизложенным, была поставлена цель оценки влияния атак на точки доступа беспроводной сети. В качестве объекта исследования были выбраны точки доступа компании Ubiquiti Networks (UN) [3].

Поставленная цель определяет следующий круг задач:

- Организовать лабораторный стенд для исследования влияния атак;
- Рассмотреть модель угроз;
- Выбрать актуальные атаки;
- Исследовать работу точек доступа во время атак;
- Предложить рекомендации по защите от выбранных атак.

Для исследования уязвимостей точек доступа были выбраны следующие актуальные деструктивные атаки на Wi-Fi сети:

- DoS (отказ в обслуживании), создается множество пакетов, которые тем или иным способом выводят из строя или замедляют работу точки доступа, что может привести к замедлению работы участка или всей сети.
- Evil Twin (с англ. «злой двойник») подразумевает создание и использование мошеннической точки доступа с идентичными параметрами. Созданная паразитная точка доступа может забирать клиентов у существующей легитимной точки доступа [4].
- ARP-Spoofing (с англ. «подмена ARP»), нарушитель осуществляет инъекцию пакетом, в результате чего изменяется запись в таблице ARP и перенаправляется весь трафик с точки доступа через нарушителя [5].

Основными критериями выбора для исследования данных атак являлись их широкая распространенность [6], а также соответствие угрозам, приведенным в банке данных угроз ФСТЭК России [7, 8].

Приведены рекомендации по защите точек доступа беспроводной сети от исследованных деструктивных атак [9, 10].

Выводы. В целях проведения исследований был смоделирован лабораторный стенд. Исследована и проведена оценка влияния выбранных актуальных атак на точки доступа. Лабораторный стенд возможно использовать в будущем для исследования влияния других атак на выбранное оборудование. Также, в рамках организованного стенда можно осуществлять лабораторные работы по дисциплине «Безопасность беспроводных сетей». Разработанный лабораторный стенд позволяет исследовать влияние атак на оборудование и методы защиты на участке или всей локальной сети. Стенд может быть организован как удаленно, так и локально, что позволит познакомиться с настройкой контрольных и не контроллерных точек доступа [11-13].

СПИСОК ЛИТЕРАТУРЫ

1. Красов, А. В., Рогова А. Н. Риски при реализации технологии BYOD в организациях и решения для их минимизации. Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. Т. 1. С. 506–510.
2. Positive Technologies. Уязвимости корпоративных информационных систем. [Электронный ресурс] URL: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019/?sphrase_id=88725 (дата обращения 3.06.2021).
3. Tadviser. Оборудование для беспроводных сетей (WLAN) мировой рынок [Электронный ресурс] URL: https://www.tadviser.ru/a/265124 (дата обращения 3.06.2021).
4. Ковцур М. М., Симанов М. С. Анализ особенностей организации авторизации пользователей в сетях коллективного доступа стандарта IEEE 802.11. Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 4. С. 537–541.
5. Инструменты Kali Linux. Атака на Wi-Fi [Электронный ресурс] URL: https://www.kali.tools/?tag=атака-на-wi-fi (дата обращения 5.06.2021).
6. Ковцур М. М., Киструга А. Ю., Ворошнин Г. Е., Федорова А. Э. Исследование атак authentication failure и Arp inject и методов их обнаружения в сетях семейства IEEE 802.11 // Информационные технологии и телекоммуникации. 2021. Т. 9. № 1. С. 87–98.
7. БДУ ФСТЭК России. УБИ.140 [Электронный ресурс] URL: https://bdu.fstec.ru/threat/ubi.140 (дата обращения 7.06.2021).
8. БДУ ФСТЭК России. УБИ.126 [Электронный ресурс] URL: https://bdu.fstec.ru/threat/ubi.126 (дата обращения 7.06.2021).
9. Козлов В. А., Рындюк В. А., Воробьев Г. А., Чернышев А. Б. Модели и методы защиты от атак "man in the Middle" (MITM). Современные фундаментальные и прикладные исследования. 2017. № 1(24). С. 27–35.
10. Зуев И. П., Карельский П. В., Ковцур М. М., Юркин Д. В. Разработка методики проведения испытаний IPS модулей. Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020): IX Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2020. Т.1. С. 492–496.
11. Бабков И. Н., Абраменко Г. Т., Храмцов Д. О., Оганесян А. Г. Оценка воздействия различных атак на точки беспроводного доступа Ubiquiti networks. Заметки ученого. 2021. Т.1 № 4. С. 67–70.
12. Александрова Е.С., Иванов Г.Н., Ковцур М.М. Анализ механизмов защиты Wi-Fi сетей. // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). С 47-51.
13. Петров В.А., Ковцур М.М., Киструга А..Ю. Исследование методов дальнометрии в беспроводных сетях. // REDS: Телекоммуникационные устройства и системы. С 42-49.

УДК 004.056.5

КЛАССИФИКАЦИЯ И РАНЖИРОВАНИЕ ПО ИНФОРМАТИВНОЙ ЗНАЧИМОСТИ ТРЕБОВАНИЙ К ПОКАЗАТЕЛЯМ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ

Башкирцев Андрей Сергеевич, Паращук Игорь Борисович, Беляев Сергей Валерьевич, Боголепов Григорий Сергеевич

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

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

e-mails: ab098@yandex.ru, shchuk@rambler.ru, goshaceh@mail.ru, bogolepov@inbox.ru

Аннотация. Предложен подход к классификации и ранжированию современных требований к защищенности автоматизированных систем управления телекоммуникационными сетями. Подход основан на анализе относительной информативности этих требований и опирается на процедуры и алгоритмы оценки их информативности по критерию минимума величины энтропии. Результаты решения данной задачи позволят повысить адекватность и достоверность описания тех существенных свойств подсистем защиты информации, которые определяют их качество.

Ключевые слова: ранжирование; классификация; показатель; автоматизированная система управления; требования; защищенность; телекоммуникационная сеть; информативность.

CLASSIFICATION AND RANKING BY INFORMATIVE SIGNIFICANCE OF REQUIREMENTS FOR SECURITY INDICATORS OF AUTOMATED TELECOMMUNICATIONS NETWORK MANAGEMENT SYSTEMS

Bashkirtsev Andrey, Parashchuk Igor, Belyaev Sergey, Bogolepov Grigory

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

3 Tikhoretsky Av, St. Petersburg, 194064, Russia

e-mails: ab098@yandex.ru, shchuk@rambler.ru, goshaceh@mail.ru, bogolepov@inbox.ru

Abstract. An approach to the classification and ranking of modern requirements for the security of automated control systems of telecommunications networks is proposed. The approach is based on the analysis of the relative

informativeness of these requirements and relies on procedures and algorithms for evaluating their informativeness by the criterion of the minimum entropy value. The results of solving this problem will increase the adequacy and reliability of the description of the essential properties of information security subsystems that determine their quality.

Keywords: ranking; classification; indicator; automated control system; requirements; security; telecommunications network; informative significance.

Введение. Автоматизированные системы управления (АСУ) должны обеспечивать достижение целей создания, развития и функционирования сложных управляемых телекоммуникационных сетей (ТКС), причем надежность и адаптивность АСУ должны быть достаточными для достижения установленных целей функционирования ТКС в заданном диапазоне изменений условий применения. Помимо этого, в АСУ ТКС должны быть предусмотрены контроль правильности выполнения автоматизируемых функций и диагностирование с указанием места, вида и причины возникновения нарушений правильности функционирования автоматизированной системы [1-3].

Данные системы управления должны в автоматизированном режиме выполнять: сбор, обработку и анализ информации (сигналов, сообщений, документов и т.п.) о состоянии ТКС; выработку управляющих воздействий (программ, планов и т.п.); передачу управляющих воздействий (сигналов, указаний, документов) на исполнение и ее контроль; реализацию и контроль выполнения управляющих воздействий, а также обмен информацией (документами, сообщениями и т.п.) с взаимосвязанными автоматизированными системами [4].

Важным элементом системы требований к АСУ ТКС являются требования по защищенности информации, циркулирующей в системах такого класса. Защищенность АСУ ТКС достигается путем разработки и применения совокупности организационных и технических мер, направленных на нейтрализацию угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования управляемой ТКС, на локализацию и минимизацию последствий от возможной реализации угроз безопасности информации, восстановление штатного режима функционирования АСУ в случае реализации угроз безопасности информации [5].

При формулировке состава и физической сущности показателей защищенности (ПЗ) АСУ ТКС с учетом потенциальных угроз безопасности информации, должны быть приняты во внимание структурно-функциональные характеристики АСУ ТКС, а также иные особенности ее построения и функционирования.

Показатели защищенности АСУ ТКС в полной мере определяются качеством проектирования и построения подсистемы, призванной осуществлять защиту АСУ ТКС. При этом в состав ПЗ АСУ ТКС должны быть включены показатели, физически характеризующие и численно аттестующие: типы субъектов доступа; методы управления доступом; меры защиты информации; виды и типы средств защиты информации; структура подсистемы защиты АСУ ТКС с учетом класса защищенности и др. [6, 7].

Своевременной и важной, на наш взгляд, является задача разработки методического аппарата, обеспечивающего определение требуемой номенклатуры и объема требований к ПЗ АСУ ТКС, а также учитывающего особенности эксплуатации подсистемы защиты АСУ ТКС и разработки ее элементов.

В основу формулировки этой задачи положен вопрос – существует ли возможность построения на имеющемся множестве показателей защищенности сколько-нибудь разумной и полезной системы их отношений с состоянием защищенности АСУ ТКС. При этом известно, что построение таких отношений возможно на основе формулировки соответствующих моделей, которые ориентированы на традиционные задачи классификации. Примером одного из современных подходов к решению задач классификации и ранжирования является подход, в основе которого реализуются механизмы ранжирования по информативной значимости. Ранжирование требований к ПЗ АСУ ТКС по информативной значимости позволяет снять неопределенность наблюдаемого состояния защищенности системы управления, которая количественно характеризуется энтропией этого состояния [8-10].

Если предположить, что вектор требований полностью определяет сущность защищенности АСУ ТКС, то, используя описанное в работах [9, 10] свойство, заключающиеся в том, что энтропия совокупности независимых величин равна сумме энтропии этих величин, можно перейти к определению информативной значимости требований к ПЗ АСУ ТКС – формулировке и заданию требований к защищенности, причем важнейшим требованием является то, которое обладает максимальным количеством информативности.

Второй, не менее важный аспект определения информативной значимости требований к ПЗ АСУ ТКС – требования можно выбирать по критерию минимума величины энтропии. Чем меньше дисперсия требований, тем плотнее распределение и тем больше вероятность того, что требования принадлежат к одному классу, характеризующему определенное состояния защищенности АСУ ТКС.

Заключение. Таким образом, рассмотрен комплекс современных требований к защищенности автоматизированных систем управления телекоммуникационными сетями. Проведен анализ общих требований к показателям защищенности, выполнение которых призвано обеспечить своевременное и устойчивое управление защитой информации, циркулирующей в системах контроля и мониторинга телекоммуникационных сетей в современных условиях. На основе оценок относительной информативности требований к безопасности информации могут быть сформированы требования к показателям защищенности АСУ ТКС, причем с учетом их адаптации при изменении внешних условий функционирования.

Тем самым может быть решена задача определения объема и номенклатуры требований к показателям защищенности АСУ ТКС. Эта задача может и должна быть сформулирована и решена, как задача

многокритериального ранжирования по информативности исходной совокупности требований, описывающих защищенность АСУ. Помимо этого, результаты решения данной задачи, по мнению авторов, позволят повысить адекватность и достоверность описания тех существенных свойств подсистем защиты информации, которые, в целом, и определяют их качество.

СПИСОК ЛИТЕРАТУРЫ

1. Межгосударственный стандарт ГОСТ 34.003-90 Автоматизированные системы. Термины и определения. – М.: Стандартинформ, 1992. –14 с.
2. Межгосударственный стандарт ГОСТ 24.104-85 Единая система стандартов автоматизированных систем управления. Автоматизированные системы управления. Общие требования. – М.: Стандартинформ, 1985. – 23 с.
3. Ермолаева В.В., Калашников Д.А. Автоматизированные системы управления // Молодой ученый. №11. 2016. С. 166-168.
4. Паращук И.Б., Башкирцев А.С., Ногин С.Б. Динамическая оптимизация параметров контроля в интересах управления связью между различными информационно-аналитическими и вычислительными системами // Естественные и технические науки. №4 (94), 2016. С. 24-28.
5. Приказ ФСТЭК России от 14 марта 2014 года №31. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. (с изменениями на 9 августа 2018 года). – М.: ФСТЭК. 2014. – 28 с.
6. Башкирцев А.С., Митрофанов Е.А., Паращук И.Б. Автоматизированные системы управления телекоммуникационными сетями: обзор и анализ современных требований // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020 г.: Материалы конференции. Часть 1. \ СПОИСУ. – СПб.: 2020. – 393 с., С. 63-65.
7. Башкирцев А.С., Митрофанов Е.А., Паращук И.Б. Анализ требований к автоматизированным системам управления телекоммуникационными сетями. // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 8. – СПб.: СПОИСУ, 2020. – 474 с. С. 91-95.
8. Корлякова М.О., Твердохлеб Н.О. Анализ подходов к определению информативности признаков // Научная сессия МИФИ-2006. Т.3 Интеллектуальные системы и технологии, – М.: МИФИ, 2006. С. 146-147.
9. Федоров В.К., Сергеев Н.П., Кондрашин А.А. Контроль и испытание в проектировании и производстве радиоэлектронных средств. – М.: Техносфера, 2005. – 563 с.
10. Гаскаров Д.В., Голинкевич Т.А., Мозгалевский А.В. Прогнозирование технического состояния и надежности аппаратуры. – М.: Советское радио, 1974. – 224 с.

УДК 004.054

ПОВЫШЕНИЕ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Бондарев Виктор Юрьевич, Титов Владимир Степанович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: bondarev82@mail.ru, titov@mail.ru

Аннотация. Статья посвящена вопросу повышения устойчивости функционирования автоматизированных систем управления. Определены основные проблемные вопросы и представлены направления повышения устойчивости функционирования современных автоматизированных систем управления.

Ключевые слова: автоматизированная система управления; устойчивость; требования к устойчивости сети передачи данных; реализация требований к повышению устойчивости функционирования автоматизированных систем управления.

IMPROVING THE STABILITY OF THE FUNCTIONING OF AUTOMATED CONTROL SYSTEMS

Bondarev Viktor, Titov 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: bondarev82@mail.ru, titov@mail.ru

Abstract. The article is devoted to the issue of increasing the stability of the functioning of automated control systems. The main problematic issues are identified and the directions of increasing the stability of the functioning of modern automated control systems are presented.

Keywords: automated control system; stability; requirements for the stability of the data transmission network; implementation of requirements for improving the stability of the functioning of automated control systems.

Введение. Анализ существующих информационных систем показал, что взаимодействие определяет существование, структурную организацию и свойства всякой информационной системы. Взаимодействие – свойство, присущее не только материи в целом, но и всем ее состояниям и проявлениям, отдельным вещам, явлениям, процессам, их сторонам и свойствам. Первым необходимым условием для взаимодействия двух (или более) систем является их одновременное существование. Под одновременностью существования будем понимать такой промежуток времени функционирования систем, в течение которого воздействие хотя бы одной из них повлияет на результативность другой при выполнении конкретной задачи. Причем это влияние может быть непосредственным, и опосредованным, когда эффективность системы может существенно возрасти. Во-вторых, необходимым условием для взаимодействия является наличие у рассматриваемых систем определенных свойств, которые позволили бы им осуществлять соответствующее воздействие друг на друга.

Свойство устойчивости является фундаментальным свойством любой информационной системы. Данное свойство интуитивно может быть определено как некоторое постоянство, неизменность определенной структуры (статическая устойчивость) и поведения системы (динамическая устойчивость). Применительно к информационным системам определение устойчивости было дано выдающимся русским математиком Ляпуновым А.М.:

«Устойчивость – это способность системы функционировать в состояниях близких к равновесному, в условиях постоянных внешних и внутренних возмущающих воздействий». Устойчивость автоматизированных систем Взаимодействие неизбежно приводит к внешним и внутренним воздействиям для информационных систем, которые обязательно как следствие потребуют усиление такого свойства системы как устойчивость.

Различают активную и пассивную форму устойчивости. Активная форма устойчивости (надежность, отказоустойчивость, живучесть и пр.) присуща сложным системам, поведение которых основано на акте решения. Здесь акт решения определяется как выбор альтернатив, стремление системы достигнуть предпочтительное для нее состояние – целенаправленное поведение, а это состояние – ее целью. Пассивная форма (прочность, сбалансированность, гомеостазис) присуща простым системам, не способным к акту решения. Так как штатный режим функционирования информационных систем, как правило, далек от равновесного, центральным элементом в данном случае является понятие структурно-функциональной устойчивости. При этом внешние и внутренние информационно- технические воздействия постоянно изменяют само равновесное состояние информационной автоматизированной системы. Соответственно мерой близости позволяющей решать изменяется ли поведение системы и как существенно под действием возмущения, здесь является множество выполняемых функций при взаимодействии.

Развитию теории устойчивости автоматизированных систем были посвящены исследования целого ряда отечественных ученых. Однако теория устойчивости в этих работах развивались лишь только с точки зрения уязвимости структуры автоматизированных систем без явного учета уязвимости поведения системы в условиях априорной неопределенности информационно-технических воздействий (в условиях взаимодействия).

Основой поддержания работоспособности автоматизированных систем в условиях информационно-технических воздействий относятся:

– недостаточная устойчивость функционирования автоматизированных систем;

– рост сложности структуры и поведения аппаратно-программных средств;

– трудность выявления количественных закономерностей, позволяющих исследовать устойчивость функционирования в условиях взаимодействия.

В первом случае сложностью является недостаточная устойчивость функционирования автоматизированной системы, которая часто оказывается ниже требуемой. Во многих случаях аппаратно-программные средства не в состоянии полностью выполнить свои функции по множеству причин. Среди этих причин:

– несогласованность реальных параметров вычислительных процессов и данных в спецификациях системного и прикладного программного обеспечения;

– переоценка современного уровня развития технологии программирования;

– переоценка возможностей современных методов и средств защиты информации, отказоустойчивости вычислительных систем (ВС) и надежности программного обеспечения (ПО).

Незнание или игнорирование названных причин приводит к снижению эффективности функционирования автоматизированных систем.

Во втором случае сложностью является территориальный и поведенческий рост структуры информационной системы. К особенностям структуры автоматизированной системы относится следующее. Современные информационные системы, как правило, представляют собой территориально распределенные системы, состоящие из множества ЛВС клиентсерверной архитектуры. При этом защищенность и устойчивость функционирования аппаратных и программных средств автоматизированных систем в ряде случаев не обеспечены. Более 70% инструментальных средств разработки прикладного ПО являются зарубежными, менее 20% обладают соответствующими лицензиями производителя.

В противоположность экспериментальным методам, дающим возможность изучать единичный вычислительный процесс автоматизированных систем, методы аналитической верификации алгоритмов позволяют рассматривать наиболее общие свойства вычислительного процесса, характерные для класса процессов автоматизированной системы в целом. Однако названные подходы обладают существенными недостатками. Недостатком экспериментальных методов является невозможность распространить результаты, полученные в данном эксперименте, на другой вычислительный процесс, отличающийся от изученного. Недостатком методов аналитической верификации алгоритмов ПО является трудность перехода от класса не является собственным свойством исследуемых задач. В действительности влияние отдельных факторов внешней и внутренней среды автоматизированной системы, представленных различными величинами, проявляется не порознь, а совместно. Теория подобия позволяет сформулировать необходимые и достаточные условия изоморфности двух моделей разрешенного поведения автоматизированных систем в условиях информационно-технических воздействий, описываемых системами однородных степенных многочленов (позиномов). Как следствие, становится возможным: - производить аналитическую верификацию вычислительных процессов автоматизированной системы и проверять условия изоморфности; - численно определять коэффициенты некоторого представления модели вычислительных процессов автоматизированной системы для достижения

условий изоморфности. А это позволяет контролировать семантическую корректность вычислительных процессов, обнаруживать аномалии вычислительных процессов и восстанавливать параметры вычислительных процессов автоматизированной системы, существенно влияющие на устойчивость поведения системы.

Заключение Поддержания работоспособности автоматизированных систем в условиях взаимодействия (информационно-технических воздействий) является важной технической проблемой и требует своего разрешения. Проблемная ситуация состоит в противоречии между необходимостью поддержания работоспособности взаимодействующей автоматизированной системы в условиях информационно-технических воздействий и недостаточной проработкой моделей и методов обнаружения и парирования информационно-технических воздействий злоумышленника. Оценка практической применимости известных моделей и методов поддержания работоспособности автоматизированных систем (N-кратное резервирование; инверсионное программирование; введение различной структурной и функциональной избыточности; перераспределение операций, структур и ресурсов вычислительных систем; восстановление работоспособности элементов; реализация различных защитных функций и пр.) свидетельствует об их ограниченной ценности и показывает, что в настоящее время повышение (сохранение) устойчивости функционирования автоматизированных систем сдерживается отсутствием адекватных математических моделей разрешенного функционирования автоматизированных систем в условиях взаимодействия (информационно- технических воздействий).

СПИСОК ЛИТЕРАТУРЫ

1. Афанасьев Ю.И. Теория взаимодействия. Анализ в условиях синхронизации процесса // Образовательные ресурсы и технологии. 2014.
2. Калинин В.Н., Резников Б.А., Варакин Е.И. Теория систем и оптимального управления. Л.: Изд-во ВКА, 1979. Ч. 1.
3. Калинин В. Н., Резников Б.А., Варакин Е.И. Теория систем и оптимального управления. – Л.: Изд-во ВКА, 1987. Ч. 2.
4. Парфенова М.Я., Руденко Ю.С. Механизм интеграции образования, науки и производства с применением подхода диссимметрии // Образовательные ресурсы и технологии. 2013.
5. Кубова В.И., Кубова Р.М. Обучающая модель исследования работы сердца как импульсной системы // Образовательные ресурсы и технологии. 2013.

УДК 004.7: 621.39

АЛГОРИТМ ГИБКОЙ МАРШРУТИЗАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ БПЛА

Волков Вадим Вагифвич, Дмитренко Михаил Евгеньевич, Попов Андрей Иванович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: AdPopovAI@yandex.ru

Аннотация. Рой беспилотных летательных аппаратов (БПЛА) требует передачи данных, связанных с задачей передачи данных, по сети. Ресурсные ограничения и динамический характер роя создают проблемы при разработке протоколов маршрутизации БПЛА. Большинство традиционных схем произвольной маршрутизации не интеллектуальны и не могут адаптироваться к динамической природе сетей БПЛА. С другой стороны, некоторые схемы маршрутизации на основе искусственного интеллекта (ИИ) могут потреблять значительные вычислительные ресурсы в беспилотных летательных аппаратах. Предлагается адаптивный протокол маршрутизации, а именно маршрутизация роя на основе скелетов (*SSR*), который использует интеллектуальный алгоритм онлайн-обучения и особенности топологии управляемого полетом БПЛА для распределения трафика по оптимальным маршрутам.

Ключевые слова: беспилотный летательный аппарат; рой; геометрическая адресация; адаптивная маршрутизация; скелет; каркас; маршрутизация роя.

COMPLEX ROUTING ALGORITHM IN PACKET MOBILE DATA NETWORKS

Volkov Vadim, Dmitrenko Mihail, Popov Andrey
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: AdPopovAI@yandex.ru

Abstract. A swarm of unmanned aerial vehicles (UAVs) requires the transmission of data related to a data transmission task over a network. Resource constraints and the dynamic nature of the swarm create problems when developing UAV routing protocols. Most traditional random routing schemes are not intelligent and cannot adapt to the dynamic nature of UAV networks. On the other hand, some artificial intelligence (AI) - based routing schemes can consume significant computing resources in unmanned aerial vehicles. An adaptive routing protocol is proposed, namely skeleton-based swarm routing (SSR), which uses an intelligent online learning algorithm and features of the UAV's flight-controlled topology to distribute traffic along optimal routes.

Keywords: unmanned aerial vehicle; swarm; geometric addressing; adaptive routing; skeleton; wireframe; swarm routing.

Введение. Сети связи, состоящие из беспилотных летательных аппаратов (БПЛА), были развернуты в различных гражданских, коммерческих и военных целях, таких как борьба со стихийными бедствиями, пограничное наблюдение, поисково-спасательные операции, доставка грузов и т. д. В таких сетях часто

требуется передавать данные (например, видео наблюдения высокого разрешения) между БПЛА или на станцию управления. Таким образом, установление надежных сквозных маршрутов между беспилотными летательными аппаратами имеет решающее значение для многих применений, требующих высокого качества обслуживания (*QoS*).

Для эффективной координации и совместной работы БПЛА обычно взаимодействуют специальным образом и образуют летающую специальную сеть (*FANET*). Подмножество БПЛА может соединиться со станцией управления. Исходя из степени координации между БПЛА, Фанеты (*FANETs*) могут иметь различную архитектуру применения. Например, архитектура взаимодействия роя.

В данной статье разработана интеллектуальная, высокопроизводительная схема маршрутизации, которая адаптируется к динамике формирования Роя. В целом предложенная схема распределена и может быть использована для улучшения различных показателей *QoS* (таких как пропускная способность, задержка, балансировка нагрузки и т. д.), а также времени жизни сети. Он использует структуру роя (формирование) для уменьшения сложности интеллектуальной маршрутизации. Многие существующие схемы маршрутизации обычно ищут кратчайший путь и не могут адаптироваться к динамике сети. С другой стороны, централизованные решения и схемы маршрутизации, которые полагаются на частое обновление информации о состоянии канала для построения базы данных топологии, вносят высокую сложность и накладные расходы, что не подходит для ограниченных ресурсами роевых сетей.

Схема маршрутизации использует специальную систему геометрической адресации для определения ролей и расположения различных узлов на основе структуры роя, чтобы уменьшить накладные расходы на маршрутизацию и задержку. Фактически, управляемые миссией роевые сети, которые следуют за определенной формацией, могут быть представлены каркасом, называемым скелетом. Здесь скелет относится к основной структуре роя, которая состоит из нескольких относительно стабильных узлов, называемых костями. Узлы, расположенные во внешней области роя, обычно имеют более высокую мобильность, чем узлы ядра/внутренней области. Что касается модели адресации узлов, то здесь термин “геометрический” предпочтительнее термина “географический”, поскольку географические координаты узлов могут быть недоступны. Обратите внимание, что геометрический адрес представляет область, в которой находится узел.

Предлагаемый протокол маршрутизации является гибридным:

геометрическая переадресация: пакеты пересылаются в область, которую, как ожидается, достигнет узел, на основе «жадной» схемы переадресации.

Реактивный поиск: локальный поиск проводится для определения местоположения пункта назначения.

Предполагается, что форма построения БПЛА плавно меняется в зависимости от требований миссии. Мы называем такой процесс морфингом роя, подобно концепции морфинга изображения/полигона в области компьютерного зрения.

В частности, предлагается распределенная схема онлайн-маршрутизации на основе динамического программирования, называемая маршрутизацией роя на основе скелетов (*skeleton-based swarm routing (SSR)*), которая использует листовой канал маршрутизации для передачи пакетов через узлы, которые испытывают меньшую нагрузку трафика (следовательно, имеют меньшую вероятность перегруженности) и, следовательно, улучшают качество обслуживания. Предложенная схема маршрутизации является гибкой и может быть использована для улучшения других сетевых показателей, таких как срок службы сети, когда требования к *QoS* не являются жесткими.

Геометрическая адресация на основе скелета роя: новая геометрическая модель адресации разработана на основе структуры скелета роя, которая представляет приблизительное местоположение БПЛА. Стратегия образования морфинга реализуется для того, чтобы направить узел в положение с минимальным воздействием на его геометрический адрес, когда вся сеть изменяет формацию.

Адаптивная маршрутизация труб: листовидная маршрутизационная труба строится в соответствии с моделью адресации. Труба служит основным каркасом схемы маршрутизации и может адаптироваться к изменениям каркасной структуры сети.

Оптимизация маршрута на основе динамического программирования: предложен новый распределенный, недорогой, интеллектуальный протокол маршрутизации для достижения высокой пропускной способности и сбалансированной по нагрузке передачи данных внутри канала.

Ресурсы Узла.

Поскольку данные *GPS* могут быть недоступны в некоторых узлах, предлагаемая схема не опирается на точную информацию о географическом местоположении. Чтобы оставаться в правильном относительном положении, узлы оценивают угол и расстояние своих соседей с помощью недорогого оборудования, такого, как компас и датчики. Межузловое расстояние также может быть оценено с помощью *RSS*-методов. Узлы имеют ограниченную мощность и вычислительные ресурсы и поэтому не способны выполнять сложные алгоритмы. Здесь используются простые всенаправленные антенны и синхронизируются временные часы узлов.

Узлы роя летают в 2D-среде. Предполагается, что одним из узлов является лидер роя, который предварительно выбран и зафиксирован. Лидер может получить доступ к более крупным ресурсам. Однако для того, чтобы сделать схему применимой к сетям с ограниченными ресурсами, предполагается, что только лидер имеет доступ к командам миссии. Лидер может сам принять решение о топологии роя или получить команду от другого объекта, например, от станции управления.

Информация о новой структуре может быть представлена как основная информация о скелете, такая как длина и угол наклона костей, и передается лидером на близлежащие костные узлы. Рой действует распределенным образом, и каждый узел направляет свой дочерний узел в правильное положение (стратегия управления формированием родитель-ребенок). Таким образом, отпадает необходимость в географической информации (например, данных GPS) и траектории движения всех узлов роя. Это снижает сложность алгоритма управления формированием, особенно в больших роях, и улучшает масштабируемость и гибкость сети.

Предполагается, что БПЛА движутся со скоростью 10~50 м/с. В роевых сетях, управляемых миссией, БПЛА сотрудничают друг с другом для выполнения миссии. Однако формирование, управляемое миссией, не означает, что все узлы имеют заранее определенную траекторию и все местоположения заранее известны и точны. Узлы все еще могут свободно перемещаться в своей близости, но им необходимо поддерживать общую топологию, и поэтому следует сохранить приблизительный “каркас” роя. Когда поступает новая команда Миссии Роя, узлы могут двигаться вместе к целевой области или локально, чтобы правильно заполнить область. Они также могут переехать, чтобы помочь с установлением маршрута. Следовательно, динамика сети может быть описана моделью прогнозирования топологии.

Заключение. В дополнение к общей таблице соседей, которая записывает информацию о соседях 1-го прыжка (например, их идентификаторы, расстояния и т. д.), Каждый узел также поддерживает таблицу геоадресаций, содержащую идентификаторы всех узлов и их геоадресы, а также отметку времени обновления геоадреса. Таблица геоадресаций распределяется по всей сети (лидером) при построении формирования роя и может обновляться при значительных изменениях в рое (например, после каждого морфинга формы). Между тем, каждый узел может также обновить геоадрес, извлеченный из заголовка пакета, если соответствующая временная метка новее, чем сохраненная в таблице. Узлы также поддерживают таблицу маршрутизации для одного или нескольких назначений, которая включает узлы ретрансляции следующего перехода (называемые потенциальными перенаправителями или *PF*) и стоимость пути до пункта назначения, инициируемого каждым *PF*.

СПИСОК ЛИТЕРАТУРЫ

1. Чуднов А.М., Кирик Д.И., Курашев З.В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений/ Радиотехнические и телекоммуникационные системы. - 2017. -№2. с.41-49.
2. Крюкова Е.С. Модель функционирования электронной библиотеки для анализа ее качества и информационной безопасности//Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2020. № 9-10 (147-148). С. 16-22.
3. Овсянников С.Н., Панин Р.С., Калюка В.И. Принципы обеспечения информационной безопасности в сетях беспроводного абонентского доступа//Региональная информатика и информационная безопасность. 2017. С. 147-149.
4. Gerald R. Ash Dynamic routing in communication networks.. McGraw-Hill, 1998 . – 746 p.

УДК 004.621.397

МАРШРУТИЗАЦИЯ ПАКЕТОВ В НЕОДНОРОДНОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ

Волков Вадим Вагифович, Дмитренко Михаил Евгеньевич, Попов Андрей Иванович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: AdPopovAI@yandex.ru

Аннотация. Изучается задача управления маршрутизацией пакетов в сети передачи данных, использующей в качестве фрагментов пакетные сети радиосвязи с автоматически управляемыми режимами функционирования радиосредств. Основным отличием постановок задач от традиционных задач является необходимость учета в этом случае возможности назначения (переназначения) маршрутов, которые могут быть реализованы при работе радиосредств в различных режимах, определяющих как корреспондирующее направление передачи данных, так и техническую скорость обмена информацией в данном направлении. Разработана методика оптимизации управления маршрутизацией пакетов данных, предложен алгоритм нахождения оптимального распределения потоков по показателю вероятности своевременной доставки сообщений и приведен пример, иллюстрирующий его работу. Приведена оценка выигрыша, обеспечиваемого за счет комплексной оптимизации системы маршрутных таблиц в увязке с назначением режимов работы радиосредств.

Ключевые слова: система передачи данных; пакетная сеть радиосвязи; гибкая сетевая топология; распределение потоков; маршрутизация; матрицы тяготения.

COMPLEX ROUTING ALGORITHM IN PACKET MOBILE DATA NETWORKS

Volkov Vadim, Dmitrenko Mihail, Popov Andrey
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: AdPopovAI@yandex.ru

Abstract. The problem of packet routing control in a data transmission network using as a fragment radio packet networks with automatically controlled radio operation modes is being studied. The main difference between the considered problem from traditional tasks is the need to take into account in this case the possibility of assigning

(reassigning) routes that can be implemented when radio facilities operate in different modes, which determine both the corresponding direction of data transmission and the technical speed of information exchange in this direction.

Keywords: data transmission system; packet radio communication network; flexible network topology; distribution of flows; routing.

Введение. В связи с тем, что рой беспилотных летательных аппаратов может выполнять различные функции, тогда вместе с этим постоянно меняется объем циркулирующей информации в рое БПЛА, соответственно стоит задача оптимизации передачи данных, перераспределения задач, переназначения лидера в рое. Для решения такой проблемы рационально пользоваться матрицами тяготения, потому что в сети данных должна передаваться смешанная нагрузка и необходим метод распределения этой нагрузки в сети данных и инвариантный подход к методу переноса информации, такая матрица должна постоянна обновляться в соответствии с полученной нагрузкой.

Для решения задачи существенными являются следующие аспекты, характеризующие построение и принцип функционирования СПД.

Система (подсистема) управления сетью может строиться как система с централизованным, частично (локально) централизованным или децентрализованным управлением. Эти варианты управления также могут комплексироваться, а именно, в некоторых состояниях сети (ее фрагмента) отдельные станции могут брать на себя функции региональных или локальных пунктов управления маршрутизацией. Особенности этих случаев для решаемой задачи состоят в необходимости обеспечения таких станций достаточным вычислительным ресурсом и обеспечении связности и достаточной пропускной способностью сети служебной связи.

Таким образом, полагается, что в СПД реализована подсеть обмена служебной информацией, обеспечивающая обмен управляющих и исполнительных элементов подсистемы управления сетью данными о состоянии линий связи, нагрузках на сеть в информационных направлениях, задержках пакетов в элементах сети, а также командами управления от управляющей станции в случае централизованного или частично централизованного управления.

Режимы функционирования радиосредств могут определяться набором данных, в частности, включающих: направление связи (рабочая частота передачи/приема, параметры управления диаграммами направленности антенн), техническую скорость передачи, мощность излучения и другие. Переключение режимов работы радиосредств должно осуществляться достаточно быстро, чтобы инерционность не приводила к потерям эффективности функционирования СПД. Необходимо обеспечить, чтобы при передаче пакета радиосредством в точке приема был свободный приемник для приема данного пакета.

Комплексное управление маршрутизацией направляется на максимизацию вероятности своевременной доставки сообщений в СПД, что обеспечивается решением задачи оптимизации распределения потоков в сети и построения на этой основе системы таблиц маршрутизации пакетов для всех коммутационных центров сети. На концептуальном уровне задача оптимизации распределения потоков формулируется в виде: где S – оптимизируемое распределение потоков по маршрутам сети (потоковая структура), $\mathcal{S}(C)$ – множество допустимых распределений потоков, определенное политопологической структурой C, Λ – набор параметров, определяющих информационную нагрузку на сеть (матрица тяготения), $P(S|C,\Lambda)$ – показатель, характеризующий среднюю вероятность своевременной доставки сообщений в сети. При управлении в соответствии с в каждом состоянии внешней среды потоковая структура сети переводится в состояние которое является оптимальным в рамках ПТС C при нагрузке на сеть Λ. Распределение $\mathrm{S}^* = \mathrm{S}^*(\mathrm{C},\Lambda)$, в конечном счете, определяет алгоритм маршрутизации пакетов в системе в условиях, соответствующих исходным данным задачи. Реализация алгоритма маршрутизации, соответствующего распределению $S^*(C,\Lambda)$, осуществляется на основе формирования, рассылки и ввода в действие модифицированных технологических данных – таблиц маршрутизации пакетов, которые в данном случае определяют порт выдачи и режим работы радиосредств при передаче каждого пакета (группы пакетов). Принятие решений на формирование, рассылку и соответственно ввод в действие модифицированных таблиц маршрутизации предпочтительно осуществлять при условии заметного (существенного) прироста эффективности функционирования СПД.

Таблицы маршрутизации пакетов (ТМП) строятся в случайном варианте, допускающем возможность случайного выбора порта выдачи пакета для получателя с заданным адресом. Такой вариант маршрутизации непосредственно вытекает из решения задачи оптимизации распределения потоков и соответственно обеспечивает более эффективное управление маршрутизацией пакетов в СПД. При этом процедура маршрутизации на основе случайного ТМП может быть реализована с использованием как датчиков случайных чисел, так и детерминированных алгоритмов, обеспечивающих требуемые частости выбора портов выдачи пакетов.

Вероятность своевременной доставки сообщений в СПД. С учетом введенных определений задач является задачей M-параметрической оптимизации ($\mathrm{M} = |\mathcal{M}|$) и состоит в нахождении оптимального распределения $S \in \mathcal{S}(C)$ информационных потоков по маршрутам СПД с политопологической структурой C, обеспечивающего максимальную вероятность своевременной доставки пакетов данных в системе. Сформированная в соответствии с оптимальным распределением S^* система таблиц маршрутизации определяет для каждого маршрутизируемого пакета, вообще говоря, рандомизированный алгоритм назначения $(k.l)$-пары приемо-передающих радиосредств и их режима работы. При этом таблица маршрутизации по адресу получателя назначает порт выдачи пакета,

который может определяться с использованием датчика случайных чисел либо, например, по циклу с обеспечением требуемого распределения вероятностей выбора $(k.l)$-пары.

В качестве важной особенности сформулированной оптимизационной задачи отметим тот факт, что в ее рамках решается также задача управления нагрузкой. Действительно, при оптимальной функции распределения потоков $< s^*(\mu) >_{\mu \in \mathcal{M}}$ интенсивности результирующих потоков в информационных направлениях $s_{<i,j>}$ могут быть ниже, чем для потоков, заявленных на обслуживание, т. е. $s_{<i,j>} < \lambda_{i,j}$, что обусловлено целесообразностью соответствующего ограничения нагрузки для устранения потери эффективности сети при ее перегрузках. Следует отметить, что при оптимизации распределения потоков по среднему времени задержки сообщений необходимо выполнение условия $s_{<i,j>} = \lambda_{i,j}$, что приводит к необходимости отдельного рассмотрения задачи управления нагрузкой, выходящей за рамки решаемой задачи.

Заключение. Предложенный метод формирования системы маршрутных таблиц для комплексного управления маршрутизацией и режимами работы радиосредств системы связи позволяет реализовать автоматическое управление СПД на сетевом уровне функционирования с позиций обеспечения максимальной эффективности функционирования СПД в целом.

Как показано, комплексное управление может обеспечить существенный выигрыш в эффективности функционирования СПД в целом. В частных случаях такое управление может быть обоснованно декомпозировано на управление канальной структурой СПД и управление маршрутизацией пакетов в рамках заданной канальной структуры.

СПИСОК ЛИТЕРАТУРЫ

1. Чуднов А.М., Кирик Д.И., Курашев З.В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений. // Радиотехнические и телекоммуникационные системы. 2017, №2, с.41-49.
2. Чуднов А. М., Курашев З. В. Принципы формирования маршрутных таблиц на основе оптимизации распределения потоков в сети передачи данных. // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9, № 6 с. 46–51.
3. Путилин А. Н. Алгоритм управления режимами обмена данными в самоорганизующейся сети декаметровой радиосвязи. // Информационная безопасность регионов России (ИБРР-2017). Юбилейная X Санкт-Петербургская межрегиональная конференция, 1-3 ноября 2017 г. Санкт-Петербург. 2017, с. 106-107. Электронный ресурс]. URL: http://www.spoisu.ru/files/ibrr/ibrr2017/ibrr2017_materials.pdf (Дата обращения:17.09.2021).
4. Akyildiz I. F., Wang X., Wireless Mesh Networks, Wiley, Chichester, 2009.
5. Siachalou S. Efficient QoS routing.// The International Journal of Computer and Telecommunications Networking. 2003, vol. 43, iss. 3, p. 351-367.

УДК 004.056.53

ПРОТОКОЛЫ МАРШРУТИЗАЦИИ В СЕТИ ПЕРЕДАЧИ ДАННЫХ БПЛА

Волков Вадим Вагифович, Дмитренко Михаил Евгеньевич, Попов Андрей Иванович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: AdPopovAI@yandex.ru

Аннотация. В настоящее время беспилотные летательные аппараты (БПЛА) являются одним из наиболее динамично развивающихся видов авиационной техники и активно используются при решении широкого спектра задач. Это обусловлено тем, что БПЛА гораздо дешевле пилотируемых аппаратов, проще в обслуживании. Применение роя беспилотных летательных аппаратов (БПЛА) требует передачи данных, связанных с задачей передачи данных, по сети. Ограничения и динамический характер роя создают проблемы для разработки протоколов маршрутизации БПЛА. Привычные схемы не удовлетворяют нынешние запросы, поэтому необходимо искать пути решения данной задачи. Например, протоколы на основе искусственного интеллекта (ИИ), протоколы на основе скелетов (*SSR*).

Ключевые слова: беспилотный летательный аппарат; рой; геометрическая адресация; адаптивная маршрутизация; реактивная; проактивная маршрутизации роя.

COMPLEX ROUTING ALGORITHM IN PACKET MOBILE DATA NETWORKS

Popov Andrey, Volkov Vadim, Dmitrenko Mihail
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: AdPopovAI@yandex.ru

Abstract. This article explores the complexities of routing and data transmission in a swarm of unmanned aerial vehicles. Resource constraints and the dynamic nature of the swarm create problems when developing UAV routing protocols. Most traditional random routing schemes are not intelligent and cannot adapt to the dynamic nature of UAV networks. On the other hand, some artificial intelligence (AI) - based routing schemes can consume significant computing resources in unmanned aerial vehicles. An adaptive routing protocol is proposed, namely skeleton-based swarm routing (SSR), which uses an intelligent online learning algorithm and features of the UAV's flight-controlled topology to distribute traffic along optimal routes.

Keywords: unmanned aerial vehicle; swarm; geometric addressing; adaptive routing; skeleton; wireframe; swarm routing.

Сеть беспилотных летательных аппаратов имеет специфические характеристики с точки зрения модели мобильности, вычислительной мощности, энергопотребления и распространения радиосигнала, которые делают ее отличной от других типов специальных сетей. В связи с растущей популярностью, было проведено много исследований по подходящим протоколам и соответствующим задачам таких сетей.

В целом схемы маршрутизации можно разделить на пять категорий:

Реактивная маршрутизация: эти схемы, такие как специальный вектор расстояния по запросу (*Ad-hoc On-demand Distance Vector (AODV*)), являются по требованию и в основном предназначены для мобильных специальных сетей. Для обнаружения маршрута они полагаются на поступление управляющих сообщений по всей сети, что приводит к дополнительным накладным расходам и задержкам.

Проактивная маршрутизация: эти протоколы, которые основаны на таблицах маршрутизации, которые в свою очередь регулярно обновляются (даже когда нет данных для передачи) и, следовательно, работают быстрее. Однако частое обновление информации о состоянии канала по всей сети приводит к высоким накладным расходам.

Географическая/геометрическая маршрутизация: эти схемы иногда рассматриваются как проактивная маршрутизация, поскольку они не выполняют начальную фазу обнаружения маршрута. Однако, они не нуждаются в периодическом обновлении таблиц маршрутизации и информации обо всех состояниях канала связи сети. Вместо этого они зависят от географического расположения узлов для «жадной» (дистанционной) переадресации. Поскольку географическое расположение узлов может быть не всегда известно, последние проекты маршрутизации по этой теме фокусируются на виртуальных координатах и подходах к именованию.

Перенос из магазина: Эта категория более применима к разреженным и мобильным сетям, где узлы могут перемещаться для доставки пакетов данных. Это решение в основном подходит для централизованных и терпимых к задержкам приложений.

Гибридные: гибридные протоколы маршрутизации объединяют атрибуты других категорий, чтобы лучше адаптироваться к особенностям сети.

Интеграция программно-определяемой сети (*SDN*) с сетью роя БПЛА исследуется в, где политика связи и маршрутизации управляется контроллером *SDN*. В работе изучена несвязная многопутевая схема маршрутизации на основе распределенной архитектуры *SDN*, которая позволяет исключить энергозатраты БПЛА и повторно выбрать новые ВЧ-связи, если некоторые из них нарушены. Для иерархической архитектуры *FANET* на основе *SDN* предлагается централизованный протокол маршрутизации с дифференцированным трафиком, направленный на удовлетворение конкретных требований *QoS*, где каждый кластер беспилотных летательных аппаратов управляется верхним стационарным дирижаблем. Централизованная схема управления топологией и маршрутизацией на основе *SDN*, где контроллер позиционирует ретрансляционные узлы для оптимизации доступности каналов и строит таблицу маршрутизации для каждого узла на основе длины каналов. Развертывание *SDN* требует сбора сетевой информации и использования специальной сетевой инфраструктуры.

Предлагается автономная схема управления флокированием для поддержания иерархической сетевой структуры. Из-за высокой стоимости развертывания *GPS* и возможности потери сигналов *GPS* он использует силу принятого сигнала (*RSS*) для оценки расстояния. В работе решается задача связи и управления треугольным роем из трех связанных сотовой связью беспилотных летательных аппаратов и математически выводится надежность беспроводной системы с точки зрения удовлетворения требований задержки. В статье исследуется влияние беспилотных летательных аппаратов, разделяющих один и тот же спектр с восходящей линией связи пользователей сотовой связи. Результат показывает, что наличие каналов связи БПЛА может несколько ухудшить производительность восходящей линии связи сотовых пользователей. Качество связей БПЛА, а также пользовательских связей ухудшается по мере того, как БПЛА взлетают выше, из-за возможности больших помех прямой видимости.

Некоторые недавние исследования по роевым сетям сосредоточились на новых схемах маршрутизации, поскольку существующие для специальных или сенсорных сетей могут быть недостаточно мобильными-адаптивными, эффективными в связи и вычислениях или поддерживающими связь БПЛА с наземными станциями. Узлы могут оценивать время и потребление энергии для передачи данных на каждом пути, получая доступ к информации о местоположении. Они строят взвешенный ориентированный граф для кластерной архитектуры БПЛА. Основываясь на графическом анализе, оптимальный путь ретрансляции может быть найден с помощью алгоритма Беллмана-Форда. В предложена адаптивная схема, которая динамически регулирует интервал пакетов приветствия и тайм-аут таймера на основе информации о миссии роя и состоянии сети, чтобы минимизировать потребление энергии в схемах маршрутизации *FANET*.

Усовершенствованная версия *AODV*, называемая схемой робастного и адаптивного надежного прогнозирования (*RARP*) , предлагается для сетей *UA*, которая объединяет всенаправленную и направленную передачу и использует модифицированный формат *RREQ*, который включает информацию о траектории отправителя (в 3D), как минимум ожидаемое время соединения тракта и максимальная вероятность отказа узлов. Назначение ждет определенного времени, чтобы получить несколько *RREQ* и выбирает путь на основе функции полезности, которая является взвешенной суммой метрик в *RREQ* и счетчика переходов к назначению. Протокол

PSO-GLFR, который улучшает «жадную» маршрутизацию пересылки (*GFR*) с использованием оптимизации роя частиц (*PSO*) и ограниченного наводнения. Помимо фактора расстояния, протокол *PSO-GLFR* учитывает количество соседей и угол отклонения для поиска следующего ретранслятора пересылки.

Некоторые исследования расширили *OLSR*, чтобы адаптировать его для *FANET*. Чтобы решить проблему высокой мобильности БПЛА, взвешивает метрику ожидаемого количества передач (*ETX*) на основе относительной скорости между узлами с использованием информации *GPS*. Предлагается OLSR с учетом мобильности и нагрузки (*ML-OLSR*), который присваивает степень устойчивости связям на основе статистической информации о расстоянии. Кроме того, коэффициент загрузки вычисляется с использованием буферной нагрузки узла и его соседей, что позволяет избежать выбора перегруженных путей на этапе выбора пути. В рамках аналогичного подхода предложен протокол *OLSR* с учетом качества связи и нагрузки трафика (*LTA-OLSR*), в котором статистическая информация о силе принятого сигнала используется для определения качества связи. Транспортная нагрузка каждого БПЛА получается с использованием буферной нагрузки узла и использования канала, (что является показателем транспортной нагрузки соседей). Несмотря на эффективность таких схем, необходимость частого обновления состояния топологии приводит к высоким накладным расходам, а вычислительная сложность алгоритма выбора траектории может быть помехой, особенно в больших сетях БПЛА с батарейным питанием.

Схема является распределенной и позволяет избежать накладных расходов и сложности централизованных решений, таких как *SDN* и подходы на основе искусственного интеллекта, адаптируясь при этом к сетевым условиям. Он использует геометрическую переадресацию и, следовательно, не полагается на географические координаты (которые иногда могут быть недоступны). Насколько нам известно, это первая работа, которая извлекает выгоду из геометрической адресации, полученной из структуры роя беспилотных летательных аппаратов. По сравнению с, *CCP* перенаправляет данные только подмножеству соседей в направлении назначения (в соответствии с геометрической адресацией) вместо всех соседей, чтобы данные не отклонялись от желаемого тренда в больших сетях.

Заключение. *SSR* не выполняет обнаружение маршрута и, таким образом, избегает задержки и накладных расходов наводнения *RREQ*. Кроме того, он отправляет данные через канал маршрутизации, что значительно повышает пропускную способность.

СПИСОК ЛИТЕРАТУРЫ

1. Маркин В. Г., Рыжкова А. Г. Протоколы маршрутизации в мобильных самоорганизующихся сетях.// Теория и техника радиосвязи, 2013, №4, с.48-56. Siachalou S. Efficient QoS routing.// The International Journal of Computer and Telecommunications Networking. 2003. vol. 43. iss. 3. p. 351-367.
2. Чуднов А. М., Курашев З. В. Принципы формирования маршрутных таблиц на основе оптимизации распределения потоков в сети передачи данных.// Наукоемкие технологии в космических исследованиях Земли. 2017. Т.9, № 6, с. 46–51.
3. Шварц М. Сети связи: протоколы, моделирование и анализ, Ч. 1, 2. М.: Наука. 1992.
4. Toh C. K. Wireless Atm and Ad-Hoc Networks: Protocols and Architectures.// Kluwer Academic Publisherb Group. 1997. – 313 p.

УДК 681.3.067

ОПЫТ СПбГЭТУ «ЛЭТИ» В РЕАЛИЗАЦИИ ПРОЕКТА СЕЙФНЕТ НТИ РФ

Воробьев Евгений Германович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: vrbyug@mail.ru

Аннотация. Рассматриваются средства реализации проекта СейфНет в составе государственной программы Национальной Технологической Инициативы Российской Федерации.

Ключевые слова: киберпространство; квантовые ключи; добавленная реальность, киберполигон.

EXPERIENCE OF SPBETU "LETI" IN THE IMPLEMENTATION OF THE SAFENET NTI PROJECT

Vorobiev Evgenii
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: vrbyug@mail.ru

Abstract. The means of implementing the SafeNet project as part of the state program of the National Technological Initiative of the Russian Federation are considered.

Keywords: cyberspace; quantum keys; added reality, cyberpolygon.

В настоящее время в России решается вопрос создания защищенного киберпространства как техногенной среды существования человека. Проблема состоит в том, что создавать ее приходится из компонентов в основном западного производства, которым доверять невозможно из-за того, что разработчики при создании Интернета, компьютерных систем и сетей использовали идеологию открытых технологий и всеобщей доступности информации и управления системами. При этом наличие недекларируемых возможностей и технологий «этичного» хакинга, ставших достоянием обычных граждан, привели к тому, что попытки создания «умных»

домов, интернета вещей, промышленного интернета, беспилотного транспорта и так далее, неизбежно приведут к провалу государственных программ.

В 2015 году была принята Национальная технологическая инициатива РФ, в составе которой должен быть реализован до 2035 года проект СейфНет как «кокон безопасности» для недоверенных систем, который не меняя их функциональность позволит гарантировать защищенность каждого отдельного человека, его информации и техногенной среды существования.

В настоящее время имеется технологический задел, который позволяет рассчитывать на быструю доработку как национальной концепции обеспечения защиты киберпространства РФ, так и реализацию для обычных граждан защиты по принципу «подключил и забыл», а также создания на основе нано- и квантовых технологий принципиально новых информационных и технических систем с защищенностью от атак старого типа.

СПИСОК ЛИТЕРАТУРЫ

1. «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» (утв. Президентом РФ 24.07.2013 № Пр-1753). URL: http://www.consultant.ru/document/cons_doc_law_179634 (дата обращения 05.12.2020)
2. Роговский Е. А. Кибербезопасность и кибертерроризм. М.: УРСС, 2013 г. 42с.
3. Buchan R., Tsagourias N. Research Handbook on International Law and Cyberspace. P.: Edward Elgar Publishing. Cheltenham. 2015. 560 p.
4. Clarifying Lawful Overseas Use of Data Act of 02.06.2018 H.R.4943–115th Congress.

УДК 355.23

ПРОБЛЕМЫ ПРЕПОДАВАНИЯ СПЕЦИАЛЬНЫХ ДИСЦИПЛИН ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЧЕТВЕРТОЙ ПРОМЫШЛЕННОЙ РЕВОЛЮЦИИ

Воробьев Евгений Германович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: vrbyug@mail.ru

Аннотация. Рассматриваются изменения в современных компьютерных технологиях, ведущие к изменению содержания специальных дисциплин в области информационной безопасности в высшей школе.

Ключевые слова: киберпространство; квантовые ключи; добавленная реальность, киберполигон.

PROBLEMS OF TEACHING SPECIAL DISCIPLINES ON INFORMATION SECURITY IN THE CONDITIONS OF THE FOURTH INDUSTRIAL REVOLUTION

Vorobiev Evgenii
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: vrbyug@mail.ru

Abstract. Changes in modern computer technologies leading to changes in the content of special disciplines in the field of information security in higher education are considered.

Keywords: cyberspace; quantum keys; added reality, cyberpolygon.

Проект создания защищенного киберпространства как техногенной среды существования человека предполагает создание и переход к новым профессиональным стандартам, в частности в области нано- и квантовых технологий. Проблема обучения данным технологиям в высшей школе упирается в отсутствие подготовленных преподавателей высшей школы имеющих нужные компетенции. При этом требуется переработка государственных стандартов обучения, изменение лабораторной базы и многое другое.

В области информационной безопасности обучение в рамках специалитета предполагает изменение базовых дисциплин в области вычислительной техники, программирования и создания информационных систем, так как их современное наполнение уже не отвечает реально внедряемым технологиям создания киберпространства и представления информации в нем.

В настоящее время имеется научно-методический задел, который позволяет рассчитывать на быструю доработку учебных пособий и материалов лабораторных и практических работ в требуемой области, с учетом требований ФУМО ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Алтухов А.И., Багрецов С.А., Капинчук Н.А., Чебурков М.А. Методика оценивания временных затрат на изучение курса учебной дисциплины с применением автоматизированных обучающих систем//Известия «ЛЭТИ». —2016. —№7.
2. Петлин М. А. Социально-философские аспекты киберпространства //Вестник Омского университета. — 2014. — №. 3 (73).
3. Одинцов С. А., Ващенко А. В. Развитие теорий информационного общества и понятия «Киберпространство» //Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. — 2016. — №. 121.
4. Добринская Д. Е. Киберпространство: территория современной жизни //Вестник московского университета. Серия 18. Социология и политология. — 2018. — Т. 24. — №. 1.
5. Дейнеко А. Г. Право киберпространства: pro et contra //Право в сфере Интернета. — 2018. — С. 246—255.

УДК 004.056

ПОДХОД К ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАКЕ

Ганцацук Валентин Владимирович, Зиновьева Надежда Владимировна,
Михайличенко Николай Валерьевич, Смирнова Дарья Владимировна
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: 23esn2008@rambler.ru, gantsatsuk2000@mail.ru

Аннотация. Сформулированы угрозы обеспечения безопасности в облаке. Рассмотрены различные подходы к совершенствованию информационной безопасности современных облачных систем. При этом учитывались различные условия обстановки, различные уровни возможных угроз. Предложен подход для обеспечения защиты информации, обеспечивающий своевременное реагирование на события информационной безопасности.

Ключевые слова: облако; безопасность; физическая безопасность; данные; угроза.

AN APPROACH TO THE ORGANIZATION OF INFORMATION SECURITY IN THE CLOUD

Gantsatsuk Valentin, Zinovieva Nadegda, Mikhailichenko Nikolay, Smirnova Daria
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, gantsatsuk2000@mail.ru

Abstract. Security threats in the cloud are formulated. Various approaches to improving the information security of modern cloud systems are considered. At the same time, various conditions of the situation, different levels of possible threats were taken into account. An approach is proposed to ensure the protection of information, protection of information, providing a timely response to information security events.

Keywords: cloud; security; physical security; data; threat.

Введение. Использование облаков для размещения различного рода данных дает ряд преимуществ с точки зрения управления, доступа к услугам и масштабируемости. Использование облаков позволяет быстро наращивать необходимые мощности, но когда речь заходит о масштабировании ИТ-инфраструктуры, аспекты информационной безопасности уходят на второй план. Ряд предприятий вовсе не задумываются об организации системы защиты, поскольку доверяют системе защиты своих провайдеров. Рассмотрим ряд потенциальных угроз встречающихся при использовании облаков.

Неправильная конфигурация параметров безопасности. Это одна из основных причин утечки данных из облачной среды. Если облачная инфраструктура спроектирована неверно, то возникают риски небезопасного доступа к ресурсам, компрометации учетных данных, выдачи чрезмерных разрешений, отключения журналирования или отсутствия мониторинга, а также неограниченного доступа к портам и службам.

Многие организации не знакомы с защитой облачной инфраструктуры и используют облачные решения от разных поставщиков: частное или публичное облако – каждое со своим набором средств управления безопасностью, предоставляемых поставщиками. Из-за неправильной конфигурации или отсутствия контроля безопасности облачные ресурсы организации могут оказаться открытыми для злоумышленников [1].

Отказ в обслуживании. Функционирование облачной среды напрямую зависит от подключения к интернету. Однако такая инфраструктура особенно уязвима к атакам типа отказ в обслуживании (DoS) и распределенный отказ в обслуживании (DDoS).

Злоумышленники могут наводнить облачную сеть компании большим объемом веб-трафика, делая ресурсы недоступными как для клиентов, так и для сотрудников. Чем больше сервисов и приложений компании размещено в облаке, тем больший ущерб могут нанести действия злоумышленников.

Утечка данных. Недостаточный уровень защиты может позволить злоумышленнику получить прямой доступ к конфиденциальной информации компании и привести к утечке данных, как из локальной сети компании, так и из облачной инфраструктуры.

Взлом аккаунтов. Взлом (компрометация) учетной записи – одна из наиболее серьезных проблем, поскольку сотрудники компании не всегда имеют достаточно сложные пароли, а иногда используют один пароль для нескольких учетных записей. В результате злоумышленник с помощью одного украденного пароля может получить доступ к нескольким системам [2, 3].

Небезопасные API-интерфейсы. Пользовательские интерфейсы приложений (API) предназначены для оптимизации облачных вычислений. Однако, если их оставить без контроля и не применять адекватные меры защиты, API-интерфейсы могут открыть злоумышленникам линии связи для доступа к облачным ресурсам.

Часто разработчики создают API без надлежащих элементов управления аутентификацией, в результате эти интерфейсы можно задействовать для доступа к корпоративным данным и системам. При отсутствии соответствующих элементов управления авторизацией компрометация внутренних данных станет для злоумышленников тривиальной задачей [4].

Многие API-интерфейсы имеют собственные уязвимости безопасности, использование которых может поставить под угрозу облачную среду. Чтобы уменьшить эту угрозу, необходимо регулярно тестировать на

уязвимости приложения, с которыми работают сотрудники, анализировать риски перед их внедрением и оперативно устранять уязвимости. Не забывайте следить за обновлениями безопасности и исправлениями приложений.

Таким образом, проведя анализ вышесказанных угроз можно выдвинуть рад предложений по предотвращению угроз в облачной среде.

Необходимо использовать многофакторную аутентификацию. Помимо введения корпоративного логина и пароля для доступа к корпоративным системам в облаке рекомендуется настроить более строгую аутентификацию пользователя. Сотрудникам при авторизации нужно будет не только ввести доменное имя, но и использовать токены-аутентификаторы. Это обеспечит более высокий уровень безопасности при работе в облаке.

Обеспечить сохранность данных при возникновении угроз. Разработать план действий в нештатных ситуациях. Резервное копирование должно осуществляться по план-графику с минимальным RTPO и оптимальным жизненным циклом восстановления данных. Также можно прибегнуть к услуге аварийного восстановления, которая позволяет в случае реализации угроз переключиться на аварийную площадку с выделенным репозиторием.

Проводить тесты на проникновение в облако. С технической точки зрения тест на проникновение (PenTest) в облачной среде не сильно отличается от любого другого теста на проникновение. Моделирование действий злоумышленника, направленное на обнаружение уязвимостей облачных сред, позволит детально оценить состояние безопасности. К примеру, если конечные пользователи устанавливают дефолтные пароли для доступа к виртуальным машинам, которые имеют внешний интерфейс, они дают злоумышленникам больший простор для атаки на облачную инфраструктуру и приложения. Поэтому тест на проникновение в облако должен быть не разовой инициативой, а регулярной процедурой.

Осуществлять мониторинг. Мониторинг и анализ поведения конечных пользователей в режиме реального времени дают возможность обнаружить несанкционированный доступ или действия, отклоняющиеся от обычных шаблонов, например, вход в систему с ранее неизвестного или подозрительного IP-адреса или устройства, а также предотвратить неосторожные шаги пользователей, которые могут снизить уровень безопасности. Для мониторинга и анализа поступающей информации стоит использовать SIEM-систему, которая позволяет оперативно реагировать на инциденты информационной безопасности, тем самым снижая риск проникновения в облачную инфраструктуру.

Применяйте средства защиты информации (СЗИ). Внедрение комплекса средств защиты информации, обеспечивающих своевременное реагирование на события информационной безопасности, гарантирует сохранность данных. СЗИ могут быть установлены как на виртуальные серверы в облаке, так и на автоматизированные рабочие места сотрудников.

Заключение. Использование облачной инфраструктуры наравне с локальными рабочими сервисами, серверами и приложениями требует проактивного подхода к информационной безопасности. Проактивность позволит предотвратить возникновение серьезных и дорогостоящих проблем.

СПИСОК ЛИТЕРАТУРЫ

1. Авраменко В.С., Бобрешов-Шишов Д.И., Беденков В.Н., Маликов А.В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная научно-техническая и научно-методическая конференция. Т.3. – СПб.: СПБГУТ, 2017. С.13-18.
2. Паращук И.Б. Саенко И.Б. Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конференции. Севастополь, 22-26 сентября 2020 г. / Севастопольский государственный университет, науч. ред. Б.В. Соколов. – Севастополь: СевГУ, Том2, 2020. – 179 с., С. 243-249.
3. Крюкова Е.С. Модель функционирования электронной библиотеки для анализа качества и информационной безопасности. // Вопросы оборонной техники. Серия 16: Теоретические средства противодействия терроризму. 2020. № 9-10 (147-148). С. 16-22.
4. Гордюшин А.В., Лебедева С.В. Облачные технологии. Технология создания «облака». // Вестник молодых ученых Санкт-Петербургского государственного университета технологий и дизайна. 2014. № 3. С.53-57.

УДК 004.056.5

ОРГАНИЗАЦИЯ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ В МОБИЛЬНЫХ ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ

Ганцацук Валентин Владимирович, Михалев Владислав Олегович,
Михайличенко Антон Валерьевич, Михайличенко Николай Валерьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: 23esn2008@rambler.ru, vladmihalev1@yandex.ru, katjuha777@inbox.ru

Аннотация. Сформулировано описание уровней защиты физической безопасности центров обработки данных. Рассмотрены факторы для обеспечения безопасности и защиты от физических атак. При этом учитывались различные условия обстановки, различные уровни возможных угроз и различные физические данные центров обработки данных.

Ключевые слова: центр обработки данных; физическая безопасность; защищенность; показатель; инфраструктура.

PHYSICAL SECURITY ORGANISATION IN MOBILE DATA CENTERS

Gantsatsuk Valentin, Mikhalev Vladislav, Mikhailichenko Anton, 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-mails: 23esn2008@rambler.ru, vlad.mihalev1@yandex.ru, katjuha777@inbox.ru

Abstract. Describes the levels of data center physical security protection. Consider security and protection against physical attacks. This took into account different circumstances, different levels of possible threats and different physical data of the data center.

Keywords: data-processing center; data center; physical safety; security; indicator; infrastructure.

Введение. Мобильные центры обработки данных (МЦОД) представляют собой централизованные центры, в которых размещается вычислительное и сетевое оборудование, которое также известно, как оборудование информационных технологий (ИТ) и сетевая инфраструктура. Сетевая инфраструктура включает шлюзы, маршрутизаторы, коммутаторы, серверы, брандмауэры, системы места хранения данных и контроллеры доставки для управления и хранения данных и приложений. МЦОД хранят большие объемы данных для обработки, анализа и распределения и тем самым подключают организации к поставщикам услуг. Многие организации арендуют место и сетевое оборудование в удаленном центре обработки данных, а не владеют им. Центр обработки данных, который обслуживает несколько организаций, называется центром обработки данных с несколькими арендаторами или центром обработки данных с расположением и управляется третьей стороной.

Промышленные предприятия с локальными центрами обработки данных должны обеспечить безопасность оборудования и программного обеспечения. Существует два типа безопасности: физическая безопасность и безопасность программного обеспечения.

Физическая безопасность — это защита людей, имущества и активов, таких как оборудование, программное обеспечение, сеть и данные, от стихийных катастроф, кражи со взломом, кражи, терроризма и других событий, которые могут причинить ущерб или потерю данных предприятию или учреждению.

Защита программного обеспечения включает в себя методы предотвращения несанкционированного доступа к данным, хранящимся на серверах. Поскольку из года в год разрабатывается новое вредоносное программное обеспечение (вредоносное ПО), чтобы сломать различные брандмауэры, защищающие данные, методы безопасности необходимо периодически обновлять.

Физическая безопасность центра обработки данных включает в себя различные встроенные функции безопасности и защиты для обеспечения защиты помещений и, таким образом, оборудования, которое хранит критические данные для приложений с несколькими арендаторами. Для обеспечения охраны и безопасности помещений необходимо учитывать, контролировать и тщательно проверять различные факторы, начиная от выбора местоположения и заканчивая проверенным доступом персонала в центр обработки данных.

Для предотвращения любых физических атак необходимо учитывать следующие факторы:

– близость к районам повышенного риска, таким как трансформаторные станции и химические предприятия;
– наличие сетевых систем связи, энергоснабжения, водоснабжения и транспортировочных систем;
– вероятность стихийных бедствий, таких как землетрясения и ураганы;
– система контроля доступа, позволяющая одновременно входить только одному человеку;
– единая точка входа в объект.

Организации должны следить за защитой и безопасностью помещения со стойками центра обработки данных с проверенным доступом через следующие системы:

– видеонаблюдение с камер видеонаблюдения в соответствии с политикой организации;
– бдительность 24x7 с помощью охранников на месте и периодическое техническое обслуживание оборудования;
– регулярно проверять и контролировать права управления доступом и при необходимости увеличивать/уменьшать их;
– проверка и контроль температуры и влажности за счет надлежащего управления кондиционированием воздуха и непрямым охлаждением;
– источник бесперебойного питания (ИБП);
– обеспечение как системы пожарной сигнализации, так и аспирационной системы обнаружения дыма (например, VESDA) в центре обработки данных. Система VESDA, или aspiration, обнаруживает и предупреждает персонал до возникновения пожара и должна применятся в зонах повышенной опасности;
– панель детектора утечки воды для контроля любой утечки воды в серверном помещении;
– система отпугивания грызунов в центре обработки данных. Она работает в качестве электронного средства борьбы с вредителями, чтобы предотвратить разрушение крысами серверов и проводов;
– системы противопожарной защиты с двойной блокировкой. При срабатывании как извещателя, так и оросителя вода сбрасывается в трубу. Для защиты оборудования информационных технологий (ИТ) пожаротушение должно быть выполнено с зонированным сухим оросителем;
– кабельная сеть через фальшпол (raised floor), которая позволяет избежать подвесных кабелей, снижает тепловую нагрузку в помещении и эстетически привлекательна.

Безопасность центра обработки данных начинается с его местоположения. Необходимо учитывать следующие факторы: геологическая активность, как землетрясения, высокорискованные отрасли в этом районе, риск затопления и риск форс-мажорных обстоятельств. Некоторые из этих рисков могут быть смягчены барьерами или избыточностью в физической конструкции. Однако если что-то оказывает вредное воздействие на центр обработки данных, желательно полностью избежать его.

Наиболее оптимальным и стратегическим способом обеспечения безопасности центра обработки данных является управление им с точки зрения уровней. Слои обеспечивают структурированный шаблон физической защиты, что упрощает анализ отказа. Внешние слои являются чисто физическими, тогда как внутренние слои также помогают предотвратить любые преднамеренные или случайные нарушения данных.

Меры безопасности можно разделить на четыре уровня: охрана периметра, управление объектами, управление компьютерными помещениями и управление шкафом. Многоуровневое хранение предотвращает несанкционированный вход извне в центр обработки данных. Внутренние слои также помогают уменьшить инсайдерские угрозы.

Первый уровень защиты: охрана периметра. Первый уровень безопасности центра обработки данных заключается в предотвращении, обнаружении и задержке несанкционированного проникновения персонала по периметру. Это может быть достигнуто с помощью системы видеонаблюдения высокого разрешения, охранного освещения с активацией движения, волоконно-оптического кабеля и т.д. Аналитика видеоконтента (VCA) может обнаруживать физических лиц и объекты и проверять любые незаконные действия. Отслеживайте перемещения людей и избегайте ложных тревог.

Второй уровень защиты: средства управления. В случае любого нарушения в мониторинге периметра второй уровень защиты ограничивает доступ. Это система контроля доступа с использованием карточных свайпов или биометрии. Видеонаблюдение и аналитика высокого разрешения могут идентифицировать человека, входящего в него, а также предотвратить проход. Более сложный VCA может считывать номерные знаки, проводить распознавание лиц и обнаруживать дымовые и пожарные угрозы.

Третий уровень защиты: управление комнатой. Третий уровень физической безопасности дополнительно ограничивает доступ с помощью различных методов проверки, включая: мониторинг всех ограниченных зон, развертывание ограничений на вход, таких как турникет, обеспечение VCA, обеспечение биометрических устройств контроля доступа для проверки отпечатков пальцев и больших пальцев, ирисов или сосудистого образца, и использование радиочастотной идентификации. Использование нескольких систем помогает ограничить доступ, требуя нескольких проверок.

Четвертый уровень защиты: управление шкафом. Первые три уровня обеспечивают ввод только авторизованного персонала. Однако дополнительная защита для ограничения доступа включает механизмы блокировки шкафа. На этом уровне рассматривается страх перед «инсайдерской угрозой», например, перед злонамеренным сотрудником. После внедрения первых трех уровней шкафы, вмещающие стойки внутри компьютерного помещения, также должны быть защищены, чтобы избежать любого дорогостоящего нарушения данных.

Заключение. Таким образом физическая безопасность включает в себя четырехуровневую защиту, которая обеспечивает глубокий подход к защите в случае обхода контроля. Элементы управления включают административные решения, такие как расположение сайта, проектирование объекта и контроль/назначение уровня доступа сотрудникам. Физические элементы управления включают мониторинг периметра, обнаружение движения и аварийные сигналы о вторжении. Технические средства управления включают смарт-карты, используемые для контроля доступа, системы видеонаблюдения и системы обнаружения вторжений.

СПИСОК ЛИТЕРАТУРЫ

1. Национальный стандарт Российской Федерации ГОСТ Р 58811 - 2020. Центры обработки данных. Инженерная инфраструктура. Стадии создания. – М.: Стандартинформ, 2020. – 17 с.
2. International society of Automation. Automation Basics. https://www.isa.org/intech-home/2020/march-april/departments/physical-security-of-a-data-center
3. Паращук И.Б., Михайличенко Н.В. Особенности построения и анализа качества дата-центров как базовых элементов IT-инфраструктуры // Перспективные направления развития отечественных информационных технологий: материалы IV Межрегиональной научно-практической конференции. – Севастополь: Севастопольский государственный университет, 2018. – 352 с., С. 28-29.

УДК 681.324

ПРОБЛЕМЫ ОРГАНИЗАЦИИ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ СВЯЗЬЮ

Деев Александр Владимирович, Ковалев Игорь Станиславович, Пантюхин Олег Игоревич, Федоров Андрей Евгеньевич,
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: p_oleg99@mail.ru

Аннотация. Современные требования к системам управления связью обуславливают необходимость внедрения новых информационных технологий. В статье рассмотрено применение автоматизированных систем управления связью для совершенствования процесса организации автоматизации управления связью, повышения качества принимаемых решений, сокращения цикла управления связью.

Ключевые слова: организация автоматизации управления связью.

PROBLEMS OF ORGANIZATION OF AUTOMATION OF COMMUNICATION MANAGEMENT

Deev Alexandr, Kovalev Igor, Pantuhin Oleg, Fedorov Andrey
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: p_oleg99@mail.ru

Abstract. Modern requirements for communication management systems make it necessary to introduce new information technologies. The article considers the use of automated communication management systems to improve the process of organizing communication management automation, improve the quality of decisions made, and shorten the communication management cycle.

Keywords: organization of automation of communication management.

Введение. Совершенствование системы управления является одной из основных задач, успешное решение которой непосредственно связано с ускорением процесса создания и совершенствования средств и комплексов автоматизации.

Это позволит создать единое информационно-коммуникационное пространство, основу которого составляет «глобальная информационная решетка», представляющая собой мощную группировку коммуникационных и навигационных космических летательных аппаратов на околоземной орбите. Именно эта решетка связывает во едино все силы и средства группировки и обеспечивает их всей необходимой информацией.

Известно, что система управления представляет собой совокупность органов управления (ОУ), пунктов управления (ПУ) и средств управления. Под средствами управления понимается совокупность организованных во времени и пространстве (в космосе, воздухе, море и на суше) информационных, вычислительных и телекоммуникационных систем (средств, комплексов, ресурсов), предназначенных для обеспечения управления в едином информационном пространстве. И включает в себя систему связи, комплексы средств автоматизации и другие системы [1, 2].

Система связи – организационно-техническое объединение сил и средств связи, создаваемое для обеспечения обмена всеми видами информации в системе управления. Система связи является важнейшей составной частью средств управления системы управления.

Система связи, как и любая сложная организационно-техническая система, имеет в своем составе систему управления связью, представляющую собой совокупность функционально взаимосвязанных между собой органов, пунктов и средств управления, создаваемых для обеспечения управления системой.

Средства управления связью - совокупность сетей служебной и технологической связи, а также средств автоматизации управления связью, объединенных сетью передачи данных.

Система автоматизации связи — это организационно-техническое объединение сил и средств автоматизации, абонентских и базовой сетей передачи данных для обеспечения автоматизированного управления связью.

Если в контуре управления связью совместно со средствами связи используются средства и комплексы автоматизации, то говорят о создании автоматизированной системы управления связью (АСУС).

Целью автоматизации процессов управления связью является сокращение длительности цикла управления связью, а также повышение эффективности управления.

В широком спектре проблем совершенствования систем связи особое место занимают вопросы создания перспективных автоматизированных систем управления связью и организации в них информационных процессов. Внедрение новых информационных технологий в работу органов управления является основным направлением создания автоматизированной системы управления связью. Вместе с тем, анализ современного состояния процессов развития систем управления и связи, свидетельствует о наличии целого комплекса проблем, которые затрудняют процесс внедрения новых информационных технологий и требуют незамедлительного решения. Комплексное решение задачи внедрения новых информационных технологий в управленческую деятельность должностных лиц органов управления связью и создание высокоинтеллектуальных автоматизированных систем управления связью должно принести ощутимый эффект и позволить [3, 4]:

- повысить качество принимаемых решений;
- сократить цикл управления связью;
- оптимизировать стиль и методы работы персонала органов управления;
- улучшить качество разрабатываемых документов.

Организация автоматизации представляет собой процесс разработки, подготовки и управления осуществлением комплекса мероприятий по созданию (построению, развертыванию), обеспечению эффективного функционирования (применения) и совершенствованию системы автоматизации управления связью.

К средствам автоматизации автоматизированной системы управления связью относятся серверное оборудование и автоматизированные рабочие места персонала органов управления связью.

Указанные средства автоматизации на каждом пункте управления связью объединяются в локальные вычислительные сети (с помощью средств передачи данных), из которой обеспечивается выход в базовую систему обмена данными.

Цель автоматизации процессов управления связью сокращение длительности цикла управления связью, а также повышение эффективности управления за счет:

– сокращения времени на добывание, сбор и обработку информации о состоянии системы связи;

– уменьшения доли времени и усилий, затрачиваемых на техническую и информационно-расчетную работу, документирование принятых управленческих решений;

– повышения, прежде всего, обоснованности принимаемых решений.

Предложения по архитектуре и организационно-технической структуре построения автоматизированной системы управления связью базируются на соблюдении основных принципов, выполнение которых необходимо рассматривать как системную дисциплину при создании, развертывании и функционировании объединённой автоматизированной цифровой системы связи [5]:

– принцип соответствия организационно-технической структуры автоматизированной системы управления связью организационно-технической структуре, объединённой автоматизированной цифровой системы связи;

– принцип многоуровневого, иерархического построения;

– принцип ориентации на передовые информационные и сетевые технологии;

– принцип унификации сетевых и информационных технологий, используемых в автоматизированных системах управления, в системах управления связью;

– принцип обеспечения единства системы именования и адресования объектов и пользователей в системах управления, в объединённой автоматизированной цифровой системе связи;

– принцип сочетания централизации управления объединённой автоматизированной цифровой системой связи с одновременным предоставлением руководителям сетей, входящих в состав объединённой автоматизированной цифровой системы связи, самостоятельности в вопросах управления своей сетью и услугами в пределах их зоны ответственности;

– принцип интеграции управления различными сетями связи в пределах определенной территории (районе, зоне связи, на территории субъектов Федерации);

– принцип гибкости архитектуры управления на основе методологии открытых систем, обеспечивающий возможность ее реконфигурации и наращивания функций управления связью и отдельных элементов сети;

– принцип обеспечения единого автоматизированного информационного взаимодействия с автоматизированными системами управления и системами управления связью операторов Единой сети электросвязи Российской Федерации на основе автоматизированного электронного документооборота с использованием унифицированных форм документов;

– принцип использования единой системы стандартов по техническому, информационному и программному обеспечению на базе Рекомендаций МСЭ, государственных и отраслевых стандартов.

Реализация указанных принципов позволит обеспечить комплексное управление связью в объединённой автоматизированной цифровой системе связи.

Можно утверждать, что в настоящее время наиболее эффективным путем обеспечения современных требований к значениям характеристик существенных свойств процесса управления является совершенствование системы управления на основе комплексной автоматизации управленческой деятельности в ней.

Заключение. Таким образом, можем сделать вывод, что для организации автоматизации необходимо разработать предложения по содержанию документов автоматизации управления связью, а именно:

– модель автоматизированной системы управления связью;

– предложения по развитию и совершенствованию системы поддержки принятий решения.

СПИСОК ЛИТЕРАТУРЫ

1. Официальный сайт Министерства связи РФ - [Электронный ресурс]. - Режим доступа: https://www.businessinsider.com/.
2. Официальный сайт Министерства обороны РФ. - [Электронный ресурс]. - Режим доступа: http://mil.ru/.
3. Чуднов А.М., Кирик Д.И., Курашев З.В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений/ Радиотехнические и телекоммуникационные системы. - 2017. -№2. с.41-49.
4. Михайличенко Н.В. Вероятностно-временная модель для анализа динамики изменения состояний центров обработки данных Системы управления, связи и безопасности. 2019. № 1. С. 54-66.
5. Паращук И.Б. Крюкова Е.С. Михайличенко Н.В. Многопараметрические системы хранения данных, дата-центры и электронные библиотеки: способ контроля параметров технического состояния и анализа качества // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020г.: Материалы конференции. Часть 1. \ СПОИСУ. - СПб, 2020. - 393 с.

УДК 025.2.004; 621.311.23: 629.12

ВИДЫ ТРАФИКА И ПАРАМЕТРЫ ДЛЯ ЕГО КОНТРОЛЯ

Железкина Виктория Вадимовна, Тимошенко Денис Сергеевич, Шинкарев Семен Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного,
Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия
e-mail: den123456789qe@mail.ru

Аннотация. В существующих сетях передачи данных, построенных с использованием современных сетевых протоколов передаются большие объемы различного сетевого трафика. В данной статье рассматривается понятие трафика, его классификация, параметры и особенности передачи. Важным значением при передаче того или иного вида трафика является выбор необходимого параметра контроля для наиболее эффективной передачи.

Ключевые слова: трафик; функции; требования; параметры контроля; передача данных.

TRAFFIC TYPES AND PARAMETERS FOR ITS CONTROL

Zhelezkina Victoria, Timoshenko Denis, Shinkarev Semyon
Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny
Tikhoretsky Ave., 3, St. Petersburg, 194064, Russia
e-mail: den123456789qe@mail.ru

Abstract. In existing data transmission networks, built using modern network protocols, large volumes of various network traffic are transmitted. This article discusses the concept of traffic, its classification, parameters and transmission features. When transmitting a particular type of traffic, an important value is the choice of the necessary control parameter for the most efficient transmission.

Keywords: traffic; functions; requirements; control parameters; data transmission.

Введение. В настоящее время согласно рекомендации ITU-T 1.112: вся совокупность услуг телекоммуникационных служб разделена на два типа [1, 2]:

1. доставки (переноса) информации;
2. предоставления услуг связи.

Услуги службы доставки информации подразумеваются как виды услуг, который обеспечивает прозрачную передачу информации пользователя между интерфейсами «пользователь-сеть» без какого-либо анализа или обработки ее содержания.

Услуги службы предоставления связи подразумеваются как виды, который обеспечивает пользователям все возможности связи с учетом свойств терминального оборудования и сетевых протоколов.

Из этих определений следует, что служба доставки информации является составляющей служб предоставления связи.

Все эти службы генерируют трафик, который при анализе можно классифицировать как:

- трафик передачи данных;
- трафик реального времени.

Каждый вид трафика имеет свою конкретную цель и предназначение.

Трафик передачи данных генерируется с целью безошибочной передачи какой-либо информации в сети. При отправке данных с ошибками, будет происходить переотправка ошибочных пакетов, что в свою очередь будет загружать канал передачи данных, а также увеличит время полной отправки информации [3, 4].

Трафик реального времени генерируется для передачи голосовой или видео информации (видеоконференц связь) между абонентами в сети. Самым важным требованием к этому трафику является минимальная задержка. Так, при разговоре с использованием VoIP технологии, задержка пакета в 400 миллисекунд будет сразу заметна участниками разговора как ухудшение качества связи.

Для оценки требований к трафику используются различные методы. Одним из таких методов является Quality of Service. Качество обслуживания является набором принципов и методов, который используется для обеспечения оптимального качества голосовой связи в условиях ограниченной пропускной способности каналов связи.

Требования к трафику выражают одно или несколько из особенностей его качества, которые можно выделить явно и представить количественно. Любое требование к трафику может быть оценено явно исходя из органолептического восприятия, либо приближенно с помощью измерений соответствующих параметров.

Для большинства случаев, качество трафика определяется четырьмя параметрами:

- скорость передачи информации;
- задержка при передаче пакета;
- колебания при передаче пакетов;
- потеря пакетов.

Качество функционирования сети, как способность обеспечивать информационный обмен между пользователями, характеризуется эффективностью обслуживания трафика, которая в свою очередь зависит от ресурсов и возможностей сетевых элементов, надежности и качества передачи.

Параметры, необходимые для контроля трафика. Для разных видов трафика есть смысл применять свои параметры контроля. Например, трафику передачи данных выделяется низкий приоритет – FTP и SMTP пакетам, приложениям файлообменной сети. Трафику реального времени – высокий приоритет. Это пакеты VoIP.

Так же для различных сетевых приложений так же требуется определенное качество обслуживания:

1. Потоковые мультимедиа – приложения требуют гарантированную пропускную способность.
2. VoIP и видеоконференция – небольшие значения задержки.
3. Ряд приложений, удаленного управления и передачи данных – гарантированный уровень надежности передачи.

Заключение. В современном мире, каждое приложение или сетевая служба имеет свойство генерации определенного вида трафика. Этот трафик предъявляет свои требования к сети, которые необходимо тщательно контролировать, так как эти требования коренным образом влияют на качество предоставляемых услуг в сети передачи данных.

СПИСОК ЛИТЕРАТУРЫ

1. Авраменко В.С., Тарасов А.В. Прогнозирование защищенности информации в автоматизированных системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сборник научных статей VIII Международной научно-технической и научно-практической конференции. Т. 4., – СПб.: ГУТ им. А.А. Бонч-Бруевича. 2019. С. 19-24.
2. Гуров С.В., Уткин Л.В. Надежность систем при неполной информации. – СПб.: Любавич, 1999. 160 с.
3. Паращук И.Б. Саенко И.Б. Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конференции. Севастополь, 22-26 сентября 2020 г. / Севастопольский государственный университет, науч. ред. Б.В. Соколов. – Севастополь: СевГУ, Том2, 2020. – 179 с., С. 243-249.
1. 4.Чуднов А. М., Курашев З. В. Принципы формирования маршрутных таблиц на основе оптимизации распределения потоков в сети передачи данных. // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9, № 6 с. 46–51.

УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОСОБЕННОСТЕЙ ПОСТРОЕНИЯ МОБИЛЬНЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Зубакин Владимир Валентинович, Сазонов Виктор Викторович, Малько Никита Сергеевич, Михайличенко Антон Валерьевич, Михайличенко Николай Валерьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: 23esn2008@rambler.ru, gantsatsuk2000@mail.ru

Аннотация. Сформулированы основные принципы и технологии построения мобильных центров обработки данных. Рассмотрены различные подходы к совершенствованию структуры и процессов управления, протекающих в мобильных центрах обработки данных.

Ключевые слова: мобильный центр обработки данных; информация; инфраструктура; оборудование.

COMPARATIVE ANALYSIS OF THE FEATURES OF BUIDING MOBILE DATA CENTERS

Zubakin Vladimir, Sazonov Viktor, Malko Nikita, Mikhailichenko Anton, 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-mails: 23esn2008@rambler.ru, gantsatsuk2000@mail.ru

Abstract. The basic principles of building mobile data centers and data processing are formulated. Various approaches to improving the structure of the management processes of the ongoing mobile data centers are considered.

Keywords: mobile data center; information; infrastructure; equipment.

Введение. Актуальность работы заключается в том, что на сегодняшний день в мире стремительно растет поток принимаемой и передаваемой информации. Возникает задача, как в значительном росте информационных потоков, в увеличении количества потребителей информации и большой удаленности пользователей друг от друга доставлять информацию к получателю в короткие сроки и с требуемым качеством. Для решения данной задачи создаются мобильные центры обработки информации. Которые и будут являться звеном, выполняющим функции быстрой передачи и доведения информации до получателей [1].

Мобильный центр обработки данных (МЦОД) - это специализированный комплекс аппаратных (блок контейнеров) смонтированных на базе автомобилей семейств КАМАЗ, УРАЛ, МАЗ размещённых внутри аппаратных комплексов информационной, телекоммуникационной и инженерной инфраструктуры, с возможностью подключения к каналам связи, и предназначенный для хранения и обработки информации [2].

Мобильный ЦОД выполняется в виде, приспособленном для транспортировки автомобильным, железнодорожным, морским, авиатранспортом и имеющем в своем составе автономный отказоустойчивый комплекс систем инженерного обеспечения. Мобильные ЦОД иногда называют «контейнерными», так как выполняются они на базе стандартных грузовых «сорокафутовых» контейнеров. Делается это с целью повышения оперативности развертывания и снижения затрат на создание ЦОД. Мобильные ЦОД могут быть весьма эффективны при различных экстренных ситуациях, например, создания оперативных штабов по ликвидации последствий стихийных бедствий, переброски пунктов управления на большие расстояния. Также их можно использовать для оперативного расширения емкости стационарных ЦОД и для резервирования систем хранения с целью повысить уровень ЦОД в случае необходимости.

Мобильный ЦОД является продуктом интеграции в стандартном транспортном контейнере всех элементов ЦОД. Контейнер уже включает в себя стойки с оборудованием, систему кондиционирования, пожаротушения и другие необходимые компоненты. То, как распределяются инфраструктурные ресурсы в этой модели, во многом напоминает распределение вычислительных мощностей в облаке. В этом случае можно относительно легко нарастить или сократить ресурсы. Что невозможно сделать в стационарном дата - центре.

Мобильный центр обработки данных предназначен для [3, 4]:

– консолидации информационных ресурсов федеральных органов исполнительной власти;

– информационного обеспечения деятельности должностных лиц пунктов в целях принятия обоснованных решений;

– гарантированного (в соответствии с предоставленным правом) доступа, региональных и территориальных центров управления.

– информационно-технического взаимодействия автоматизированных систем и комплексов, ведомственных, межведомственных и общегосударственных автоматизированных систем;

– сбора, централизованной обработки в режиме реального времени и гарантированного (в течение установленного срока) хранения информационных ресурсов;

– защиты информационных ресурсов от несанкционированного доступа.

Блок контейнеры, составляющие мобильные ЦОД связаны электросиловыми цепями, линиями мониторинга, видеонаблюдения, пожарной сигнализации и контроля доступа.

В контейнере предусмотрены три отсека:

– тамбур,

– отсек IT-оборудования,

– отсек внешних блоков системы кондиционирования.

Тамбур мобильного ЦОД предназначен для обеспечения необходимого температурно - влажностного режима в отсеке IT-оборудования при эксплуатационно - необходимом доступе в отсек.

В тамбуре размещаются:

– шкаф аккумуляторов ИБП (емкость до 10 минут полного энергопотребления) и аварийного освещения МФО (на 8 часов),

– внутренние блоки системы кондиционирования и вентиляции тамбура,

– распределительное устройство МФО с байпасом ИБП (РУ),

– баллоны системы газового пожаротушения МФО,

– вводный щит электропитания и коммуникационные устройства системы мониторинга и видеонаблюдения с внешними устройствами,

– внутренние коммуникации,

– системы основного и аварийного освещения,

– двери тамбура (наружная и внутренняя в отсек IT-оборудования) снабжены запорными устройствами, обеспечивающими беспрепятственный выход обслуживающего персонала из модуля и устройствами контроля доступа снаружи.

Отсек IT-оборудования модульного ЦОД предназначен для размещения:

– серверного оборудования МФО,

– систем кондиционирования и вентиляции,

– систем газового пожаротушения,

– основного и аварийного освещения,

– систем видеонаблюдения и мониторинга.

Компоновка оборудования в IT-отсеке мобильного ЦОД обеспечивает удобный доступ к IT-стойкам, предусматривающий поочередное выдвижение стоек без отключения от сетей «в бок» (в холодный коридор) для обслуживания и замены блоков. Система кондиционирования IT-отсека организована с помощью воздушных кондиционеров. Внешние блоки системы кондиционирования размещены в «холодном» отсеке внешних блоков.

Все мобильные ЦОД выполнены из сварных цельнометаллических контейнеров, которые обладают надежной защитой от атмосферных осадков и максимально длительный срок службы размещенного оборудования.

Концепция мобильного ЦОД выработана на двух основополагающих моментах:

Во-первых, на основе анализа современных тенденций развития информационных технологий. Исходя из этого, учтена потребность в разработке таких решений, которые позволяют оперативно (мобильно) разворачивать относительно небольшие по масштабу комплексы информационной, телекоммуникационной и обеспечивающей инфраструктуры. Акцентировано внимание на комплексах, разработка которых, с одной стороны, в стационарном (полномасштабном) исполнении является избыточной, а с другой - требует строительной перепланировки и решения проблем инженерного обеспечения.

Во-вторых, на основе обобщения опыта сотрудничества с организациями телекоммуникационной отрасли. При этом в компоновке оборудования, технических решениях и конструкции образца мобильного ЦОД учтена практика проектирования, изготовления, ввода в эксплуатацию и последующего сервисного обслуживания поставляемого оборудования.

Заключение. Таким образом, были формулированы основные принципы и технологии построения мобильных центров обработки данных. Рассмотрены различные подходы к совершенствованию структуры и процессов управления, протекающих в мобильных центрах обработки данных.

СПИСОК ЛИТЕРАТУРЫ

1. Паращук И.Б. Саенко И.Б. Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конференции. Севастополь, 22-26 сентября 2020 г. / Севастопольский государственный университет, науч. ред. Б.В. Соколов. – Севастополь: СевГУ, Том2, 2020. – 179 с., С. 243-249.
2. Паращук И.Б., Михайличенко Н.В. Особенности построения и анализа качества дата-центров как базовых элементов IT-инфраструктуры // Перспективные направления развития отечественных информационных технологий: материалы IV Межрегиональной научно-практической конференции. – Севастополь: Севастопольский государственный университет, 2018. – 352 с., С. 28-29.
3. Трикоз А.С. Строим ЦОД: рекомендации заказчика // ЦОДы РФ. Проектирование, строительство, эксплуатация. 2015, № 11, С. 37-44.
4. Паращук И.Б., Зияев П.В., Михайличенко Н.В. Центры обработки данных: методы и направления совершенствования анализа эффективности их функционирования. // XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Санкт-Петербург, 24-26 октября 2018 г.: Материалы конференции. СПОИСУ. – СПб, 2018. – 631 с. С.82-84.

УДК 621.391

О НЕОБХОДИОМОСТИ СИНТЕЗА АНСАМБЛЕЙ ДИСКРЕТНЫХ ОРТОГОНАЛЬНЫХ СИГНАЛОВ ДЛЯ ПЕРСПЕКТИВНЫХ СИСТЕМ РАДИОСВЯЗИ

Зубакин Владимир Валентинович, Михайличенко Николай Валерьевич,
Ротенбергер Александр Андреевич, Сазонов Виктор Викторович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: a.rotenberger@mail.ru

Аннотация. Предложены два направления создания методов синтеза дискретных ансамблей сигналов с целью повышения помехоустойчивости и скрытности систем связи специального назначения, предложено развить теорию применения уникального математического аппарата систем и ультрасистем для синтеза систем дискретных ансамблей сигналов по совокупности показателей.

Ключевые слова: помехоустойчивое кодирование; широкополосные сигналы; ортогональные сигналы; синтез систем дискретных ансамблей сигналов.

ON THE NECESSITY OF SYNTHESIS OF ENSEMBLES OF DISCRETE ORTHOGONAL SIGNALS FOR PROMISING RADIO COMMUNICATION SYSTEMS

Zubakin Vladimir, Mikhailichenko Nikolay, Rotenberger Alexander, Sazonov Viktor
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: a.rotenberger@mail.ru

Abstract. Two directions of creating methods for the synthesis of discrete ensembles of signals are proposed in order to increase the noise immunity and secrecy of special-purpose communication systems, it is proposed to develop a theory of using a unique mathematical apparatus of systems and ultrasystems for the synthesis of systems of discrete ensembles of signals based on a set of indicators.

Keywords: noise-resistant coding; broadband signals; orthogonal signals; synthesis of systems of discrete ensembles of signals.

Введение. Современный уровень развития средств связи, внёс коренные качественные изменения в средствах и способах организации связи, выдвинули проблему совершенствования систем радиосвязи в число важнейших.

В условиях переоснащения систем связи становится очевидным, что готовность, вероятностно-временные и оперативно-технические характеристики систем управления, реализованных в радиоканалах сверхдлинноволновых, коротковолновых диапазонов и каналам спутниковой связи становятся первостепенными. Однако, используемые в настоящее время сигналы, в качестве переносчиков в указанных выше каналах связи, обладают низкой помехоустойчивостью к воздействию естественных и преднамеренных помех и не позволяют эффективно использовать энергетические и частотные ресурсы линий для обеспечения высокой помехоустойчивости и скрытности.

Существующие пути совершенствования каналов связи ориентированы на применение шумоподобных сложных сигналов в сочетании с использованием помехоустойчивого кодирования и методов оптимального приема. Анализ ряда работ показывает, что применение сложных сигналов позволяет обеспечить требуемую помехоустойчивость и скрытность. Однако использование широкополосных сигналов ориентировано на наличие каналов с избытком частотных ресурсов, что возможно только для каналов с большой частотной емкостью, а помехоустойчивое кодирование сопровождается значительным снижением скорости передачи информации, что в условиях низкоскоростных радиоканалов, недопустимо.

В фундаментальных работах В.А. Котельникова, А.В. Балакришина, К. Шеннона, в которых заложены теоретические основы оптимизации информационных сетей, доказана возможность создания синхронных систем с помехоустойчивостью и скоростью передачи информации, приближающимся к предельно возможным на основе использования ортогональных сигналов. При этом структура сигналов и методы их синтеза не рассматривались, поскольку задача решалась только для каналов с аддитивным гауссовским шумом без учета ограничений на такие характеристики сигналов, как ширена спектра, пик-фактор огибающей, значения боковых пиков корреляционных функций сигналов ансамбля, а также при условии наличия идеальной синхронизации.

В свою очередь каналы системы связи отличаются от рассмотренной модели как по ограниченным потенциальным возможностям частотного и динамического диапазонов, так и по помеховой обстановке, характеризуемой наличием дополнительных мощных узкополосных, сосредоточенных, импульсных и мультипликативных помех естественного и преднамеренного происхождения.

Учет этих факторов предъявляет ряд требований к характеристикам сигналов, реализация которых может быть обеспечена соответствующим выбором их структуры. Последнее обстоятельство явилось основной причиной постоянно растущего интереса специалистов к ансамблям дискретных сигналов, вопросы

теории которых и различных ее приложений постоянно рассматриваются в отечественной и зарубежной литературе.

Анализ известных методов синтеза дискретных сигналов позволяет выделить два направления в этом вопросе.

Первое базируется на анализе свойств сигналов, для описания которых используется широкий класс известных из математики ортогональных полиномов Якоби, Гегенбауэра, Чебышева, Лагерра, Эрмита и дискретных ортогональных функций Уолша, Хаара, Радемахера, Виленкина -Крестенсона и других. Среди работ этого направления особо следует выделить публикации Л.Е. Варакина, А.Г. Леонтьева, М.К. Размахнина, В.П. Яковлева, М.Б. Бэлларада, Х. Хармута.

Второе направление связано с построением производных сигналов на базе перемножения специально подобранных производящих последовательностей на известные дискретные ортогональные функции и достаточно полно представлено работами Л. Е. Варакина, Н.Г. Дядюнова, Д. Стиффлера.

При этом в работах первого направления просматривается решение задачи синтеза сигналов с присущими ей ограниченными возможностями, определяемыми количеством известных ортогональных полиномов. Работы второго направления ограничиваются синтезом ансамблей дискретных сигналов по одной из характеристик, а существующие радиоканалы предъявляют к используемым сигналам требования по энергетическим, корреляционным и спектральным характеристикам.

Заключение. Таким образом, известные методики не могут быть использованы для решения задачи синтеза сигналов по совокупности требований, обусловленных помеховой обстановкой, условиями распространения электромагнитных волн в реальных каналах связи и наличием ограничений на их характеристики. При этом из-за многомерности пространства характеристик и многообразия структур сигналов использование метода перебора с целью выхода на ансамбль с характеристиками на уровне предъявляемых требований исключено.

К недостаткам известных подходов следует также отнести их ограниченные возможности по полноте охвата базисов сигнальных пространств и, как следствие, весьма посредственные характеристики синтезированных ансамблей, не удовлетворяющих предъявляемым требованиям по обеспечению заданной помехоустойчивости и скрытности систем радиосвязи различных диапазонов радиоволн.

Рассматривая задачи синтеза как обратные, следует отметить, что в рассматриваемом случае постановки по совокупности требований они будут иметь неустойчивые и неоднозначные решения. Такие задачи, согласно Адамару, относятся к классу некорректно поставленных задач.

Отмеченные недостатки применявшихся подходов и отсутствие методов решения задач синтеза дискретных сигналов в некорректной постановке, являются в настоящее время основным препятствием на пути кардинального решения вопросов рационального выбора структур сигналов.

Для устранения существующего пробела в теории синтеза дискретных сигналов в докладе предложено развить теорию применения уникального математического аппарата систем и ультрасистем для синтеза систем дискретных ансамблей сигналов по совокупности показателей, который впервые изложен в работах профессора В.С. Попенко [1-3]. В этом случае задача синтеза отличается от традиционных задач оптимизации из-за неклассической постановки за счет многопараметричности и многокритериальности, связанных с формированием систем дискретных сигналов [4].

СПИСОК ЛИТЕРАТУРЫ

1. Попенко В.С. Векторный синтез ансамблей ортогональных сигналов. Ч.1. – Ставрополь: МО РФ, 1992. -130 с.
2. Попенко В.С. Векторный синтез ансамблей ортогональных сигналов. Ч.2. – Ставрополь: МО РФ, 1993. -130 с.
3. Попенко В.С. Векторный синтез ансамблей ортогональных сигналов. Ч.3. – Ставрополь: МО РФ, 1993. -150 с.
4. Пашинцев В.П., Малофей О.П., Жук А.П., Самус М.В., Гайчук Д.В., Сазонов В.В. Развитие теории синтеза и методов формирования ансамблей дискретных сигналов для перспективных систем радиосвязи различных диапазонов радиоволн. – М.: Физматлит. -2010. -196 с.

УДК 377,378

ПРОБЛЕМЫ ПРИМЕНЕНИЯ КОГНИТИВНЫХ ТЕХНОЛОГИЙ И ОРГАНИЗАЦИИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ СПЕЦИАЛИСТОВ ПО УПРАВЛЕНИЮ ТЕХНИЧЕСКИМ ОБЕСПЕЧЕНИЕМ СВЯЗИ И АВТОМАТИЗАЦИИ В ОСОБЫХ УСЛОВИЯХ

Иванов Роман Михайлович, Синицын Дмитрий Валерьевич,
Пантюхин Олег Игоревич, Ковалев Алексей Андреевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: p_oleg99@mail.ru

Аннотация. Изменения характера требований к образовательному процессу обуславливают необходимость подготовки специалистов технических специальностей с конкурентоспособным уровнем квалификации, что сказывается на технологиях их подготовки. Они должны быть сосредоточены на: мобильную настройку модели специалиста; обеспечение индивидуализации образовательных программ и способов их усвоения в зависимости от степени профессиональной подготовки и интересов обучаемых.

Ключевые слова: технологии обучения; когнитивные технологии; дистанционное обучение.

PROBLEMS OF THE USE OF COGNITIVE TECHNOLOGIES AND ORGANIZATION OF DISTANCE LEARNING FOR SPECIALISTS IN THE MANAGEMENT OF TECHNICAL SUPPORT FOR COMMUNICATION AND AUTOMATION IN SPECIAL CONDITIONS

Ivanov Roman, Sinitcin Dmitrii, Pantyukhin Oleg, Kovalev Aleksei
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: p_oleg99@mail.ru

Abstract. Changes in the nature of the requirements for the educational process necessitate the training of specialists in technical specialties with a competitive level of qualifications, which affects the technologies of their training. They need to be focused on mobile customization of the specialist model providing individualization of educational programs and ways of assimilating them, depending on the degree of professional training and interests of the trainees.

Keywords: learning technologies; cognitive technologies; distance learning.

Одним из путей обеспечения личностной направленности профессиональной подготовки специалиста является поиск таких технологий обучения, которые способствовали бы его самореализации и привели бы к созданию образовательных продуктов, адекватных изучаемым предметам и направлениям. В этом случае обучаемый выступает субъектом своего образования, имея возможность выстраивать индивидуальную образовательную траекторию, ставить образовательные цели, выбирать содержание и формы обучения, то есть участвовать в проектировании собственного образования.

В преподавании большое накопление информации привело к непрерывному обучению. Для успешного усвоения материала обучаемым необходим высокий уровень интеллектуального развития восприятия, представлений, памяти, мышления, внимания, эрудиции, широта познавательных интересов, уровень логических операций. При недостаточном развитии этих качеств они способны компенсировать это за счет повышенной мотивации или работоспособности, настойчивости, степени притязаний, скрупулезности и аккуратности в учебной деятельности. Однако интерес к обучению и успеваемость по-прежнему снижаются. Чтобы этого не произошло, приобретенные ими знания должны быть значимыми и ориентированными на ценности. Современное образование предлагает множество видов таких технологий активного обучения. Одной из наиболее эффективных педагогических технологий активного обучения является когнитивная технология.

Кроме того, в соответствии с приказом Министерства науки и высшего образования Российской Федерации в условиях распространения коронавирусной инфекции руководителям организаций, реализующих образовательные программы высшего образования и различные профессиональные программы, было рекомендовано организовать работу обучаемых и преподавателей в электронной информационно - образовательной среде (ИОС) [1]. Учебные заведения Министерства обороны Российской Федерации, в том числе довузовские учебные заведения, в которых обучение организовано в режиме удаленного доступа, переведены на дистанционную форму обучения «LMS-школа» [2].

Справедливо будет уточнить, что Министерство обороны РФ уже давно ведет работу по созданию информационно-образовательной среды в рамках национальной программы «Образование» и в соответствии с Указом Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации».

Таким образом, с технической точки зрения военные вузы были готовы перейти на дистанционное обучение в современных сложных условиях [3]. Однако на практике возник ряд организационных, правовых, экономических и психологических проблем.

Во-первых, необходимо предоставить образовательный контент для всех обучаемых. Все они должны иметь рабочее место, оборудованное персональным компьютером, проверенным службой защиты государственной тайны, и доступ в Интернет.

Во-вторых, без переосмысления роли и места преподавателя в системе образования невозможно его дальнейшее развитие. Идея педагога как носителя знаний, который транслирует мудрость для своих учеников, больше не подходит для целей образования 21-го века. Для тех, кто входит в доступ к знаниям и техническим навыкам на своих телефонах, планшетах и компьютерах, необходимо переосмыслить роль учителей в классе и в лекционном зале. Педагоги по всему миру получают возможность опробовать новые формы взаимодополняемости в работе. Они могут использовать виртуальные классы со всеми необходимыми инструментами. Это делает такие занятия такими же эффективными, как и традиционные. Несмотря на это, в данный момент цифровая трансформация образования, в большинстве случае вызывает настороженные чувства у преподавателей.

В-третьих, на данный момент учитывается возможность оценки эффективности разработки программы обучения. Это может быть концепция, основанная на результатах почти ежедневной сертификации (тестирования). Также только тогда можно будет подтвердить или опровергнуть предположение о том, что у обучаемых нет достойной мотивации и самодисциплины для самостоятельной учебы на онлайн-курсах.

В-четвертых, необходимо рассмотреть возможность перевода специализированных классов общевоинской подготовки, в том числе классов, сертифицированных в соответствии с требованиями нормативно-правовых документов по защите государственной тайны, в дистанционный режим. До получения единого документа, регулирующего этот вопрос, каждое учебное заведение решает его самостоятельно.

В-пятых, поток образовательного контента в Интернете может привести к конкуренции между различными учебными заведениями. По сути, обучаемые и преподаватели воспользовались уникальной возможностью наблюдать за курсами, созданными за пределами стен их альма-матер. В то же время нельзя исключать уверенности в том, что многие из них потом захотят сменить место работы или учебы. В свою очередь, это привело к сокращению числа обучаемых или неуловимых профессиональных кадров, что связано с экономическими последствиями для учебных заведений.

Использование когнитивных технологий в учебном процессе способствует развитию широкого кругозора учащихся. Обучаемые самостоятельно стремятся найти истину, критически воспринимают противоречивые идеи. Они способны анализировать и проектировать свою деятельность, действовать самостоятельно в условиях неопределенности, приобретать новые знания; иметь устойчивое стремление к самосовершенствованию; стремиться к творческой самореализации. Знания и возможности, полученные при таком подходе, способствуют развитию высокого уровня интеллекта, формированию творческого потенциала, накоплению практического опыта, формированию необходимого методологического мышления в новых образовательных условиях.

Блок контроля ввода. В этом блоке занятия предназначены для получения информации об уровне когнитивной готовности учащихся к восприятию и пониманию новой учебной информации и выполнению различных познавательных действий и операций. Познавательная готовность определяет успешность всей дальнейшей деятельности учащихся по усвоению нового учебного материала. Для изучения текущего уровня когнитивного развития используется специальная система мониторинга, которая диагностирует основные когнитивные характеристики интеллекта, имеющие нейрофизиологическую природу; общие академические навыки; междисциплинарные знания и навыки; предметные знания и навыки.

После окончания изучения декларативной и процедурной информации, входящей в группу модулей, объединенных общим предметом изучения, следует триада занятий: обобщающее повторение, тематический итоговый контроль и коррекция. Таким образом, неправильное восприятие или искажение учебной информации, при использовании данной технологии, можно исправить.

В целях повышения степени подготовки специалистов все чаще используются преимущества и принципы мониторинга уровня знаний обучаемых, реализованные в технологиях адаптивного тестирования.

В целом под технологией адаптивного тестирования понимается пакет интерактивного программного обеспечения, позволяющий вариативно изменять порядок выполнения тестовых заданий в зависимости от соотношения правильных и неправильных ответов обучаемого на предыдущие тестовые вопросы [4].

Во время текущего или итогового контроля уровня знаний обучаемых после получения очередного ответа необходимо определить уровень сложности следующего вопроса, который зависит от правильного или неправильного ответа на предыдущий вопрос. Алгоритм выбора и определения сложности следующего вопроса основан на принципе обратной связи. Обычно после правильного ответа обучаемого следующий вопрос в задании будет более сложным, а в случае неправильного ответа обучаемый получит более легкий вопрос в качестве следующего.

В то же время программное обеспечение диалога всегда предоставляет возможность более точно определить уровень знаний обучаемого в той или иной предметной области знаний, отвечая на дополнительные вопросы по разделам и темам учебной программы, которые он еще не полностью освоил.

Заключение. Подводя итоги, можно утверждать, что в современных особых условиях высшее военное образование получило уникальный шанс провести эксперимент, результаты которого должны решить некоторые проблемы современного образования, решить вопросы, требующие от преподавателя переосмысления своего места и роли в системе образования.

СПИСОК ЛИТЕРАТУРЫ

1. Официальный сайт Министерства науки и высшего образования РФ - [Электронный ресурс]. URL: https://www.businessinsider.com (Дата обращения: 28.08.2021).
2. Официальный сайт Министерства обороны РФ. - [Электронный ресурс]. URL: http://mil.ru (Дата обращения: 28.08.2021).
3. Егупов М.В., Жангазин А.А., Пантюхин О.И., Юдин А.А. Электронные учебные издания – новая веха в российском образовании // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей 5-й междун. НТиНМК конф., Санкт-Петербург, 1-2 марта 2016г. СПб.: СПбГУТ, 2016. С.307-313.
4. Авраменко В.С., Купчиненко О.П., Пантюхин О.И. Адаптивное тестирование при автоматизации контроля знаний. // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей 5-й междун. НТиНМК конф., Санкт-Петербург, 1-2 марта 2016г. СПб.: СПбГУТ, 2016. С.213-217.

УДК 621.391 (075.8)

ЗАЩИЩЕННЫЙ КОМПЛЕКС ПРОГРАММ ЭЛЕКТРОННОЙ ПОЧТЫ В ОПЕРАЦИОННОЙ СИСТЕМЕ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Ильина Ольга Борисовна[1], Купчиненко Ольга Павловна[1], Скоропад Александр Витальевич[2]

[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

[2] Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио»
(Филиал ФГУП НИИР-ЛОНИИР)
Большой Смоленский пр., 4, Санкт-Петербург, 192029, Россия

e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Аннотация. Выполнен анализ состава защищенного комплекса программ электронной почты в среде операционной системы специального назначения Astra Linux SE. Рассмотрены вопросы применения программных средств шифрования и создания электронной цифровой подписи в почтовых сообщениях для повышения безопасности почтовой переписки.

Ключевые слова: операционная система специального назначения; электронная почта; сервер электронной почты; клиент электронной почты; открытый ключ; закрытый ключ; шифрование; цифровая подпись.

THE PROTECTED COMPLEX OF EMAIL PROGRAMS IN OPERATING SYSTEMS OF SPECIAL PURPOSE

Ilina Olga[1], Kupchinenko Olga[1], Skoropad Aleksandr[2]

[1] The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

[2] Radio Research & Development Institute «Leningrad Branch of Radio Research & Development Institute» (Branch NIIR-LONIIR)
4 Bolshoy Smolensky Av, St. Petersburg, 192029, Russia

e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Abstract. The analysis of the protected complex of email programs from operating system of a special purpose Astra Linux SE was done. The questions of application of encryption software and digital signature creation in mail messages for increasing the security of mail correspondence were analyzed.

Keywords: operating system of a special purpose; email; mail server; mail client; public key; private key; digital signature.

Введение. Решение задачи обмена сообщениями электронной почты в операционной системе специального назначения (ОС СН) Astra Linux SE реализовано на основе защищенного комплекса программ электронной почты.

В состав защищенного комплекса программ электронной почты входят:

– сервер электронной почты, состоящий из агента передачи электронной почты Exim4 (EXperimental Internet Mailer) и агента доставки электронной почты Dovecot;

– клиент электронной почты Mozilla Thunderbird, который обеспечивает следующие функциональные возможности:

– интеграции с ядром операционной системы и с базовыми библиотеками для обеспечения мандатного разграничения доступа к почтовым сообщениям;

– автоматической маркировки почтовых сообщений пользователя с использованием его текущей мандатной метки.

В ОС СН Astra Linux SE компоненты почтового сервера — это отдельные программы, настраивать их взаимодействие нужно самостоятельно.

Для обеспечения безопасности почтовой переписки пользователи электронной почты создаются в домене Astra Linux (ALD – Astra Linux Domain).

Служба Astra Linux Directory (ALD) представляет собой систему управления Единым пространством пользователя (ЕПП) [1].

Наряду с локальной работой пользователя на рабочей электронной вычислительной машине (ЭВМ) под управлением ОС СН Astra Linux SE имеется возможность организации домена Astra Linux.

При этом под ALD в общем случае понимается одна и более рабочих ЭВМ пользователей, а также специально выделенная ЭВМ, выполняющая функции первичного контроллера домена (PDC – Primary Domain Controller). Все ЭВМ, входящие в домен, работают в едином сетевом сегменте.

Благодаря наличию контроллера домена появляется возможность организации централизованного хранилища учетных записей пользователей домена, а также, при необходимости, централизованного защищенного файлового сервера, содержащего сетевые рабочие директории пользователей домена.

Установка службы ALD может осуществляться как при начальной установке ОС СН, для этого необходимо выбрать соответствующие пункты в программе установки, так и в ручном режиме в работающей системе.

Без установки пакетов расширения совместно с соответствующими основными пакетами невозможна централизация хранения атрибутов системы защиты информации (СЗИ) в распределенной сетевой среде, что может привести к невозможности входа пользователей в систему.

После создания мандатных атрибутов домена на сервере ALD, можно создавать пользователей домена и присваивать дискреционные имандатные атрибуты [2, 3].

Администрирование ALD можно выполнять как в командной строке, так и с помощью графической утилиты «Доменная политика безопасности».

В состав дистрибутива ОС СН Astra Linux SE включен графический клиент электронной почты Thunderbird. Клиент позволяет читать и отправлять письма без использования WEB-браузера. При установке ОС СН клиент Thunderbird устанавливается автоматически.

Thunderbird - почтовый клиент Mozilla Thunderbird, кроссплатформенная программа для работы с электронной почтой и группами новостей.

Для повышения безопасности и приватности почтовой переписки в клиенте Thunderbird можно реализовать защитное преобразование электронной почты. Для этого используются пакеты Gnu Privacy Guard (GPG) (входит в дистрибутив ОС СН, устанавливается по умолчанию) и Enigmail - плагин для почтового клиента Thunderbird, обеспечивает взаимодействие с GPG.

GPG - бесплатная программа с открытым кодом, предназначена для шифрования, расшифровки и создания цифровой подписи (как для текстовых сообщений, так и для файлов). GPG также позволяет управлять открытыми и закрытыми ключами.

Enigmail – это дополнение к Thunderbird, позволяет работать с шифровальными возможностями GPG прямо из Thunderbird.

Программа GPG основана на принципе криптографии с открытым ключом. Каждый пользователь создает свою пару ключей (открытый и закрытый ключи). Эту пару ключей можно использовать для шифрования, расшифровки и цифровой подписи [4].

Открытый ключ можно передавать почтовым корреспондентам. Он не подходит для чтения защищенных сообщений или для их подписи. С помощью открытого ключа другие пользователи будут готовить сообщения для владельца закрытого ключа. Прочитать эти сообщения сможет только обладатель парного закрытого ключа.

Закрытый ключ должен храниться в надежном месте. Владелец закрытого ключа имеет возможность читать письма, защищенные парным ему открытым ключом. С помощью этого же ключа можно подписывать отправляемые сообщения. Закрытый ключ защищен паролем, который вводится при его создании.

Цифровая подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

GPG и Enigmail позволяют прикреплять к сообщениям цифровые подписи. Если первый пользователь подписывает сообщение с помощью секретного ключа, то другой пользователь, у кого есть копия открытого ключа первого пользователя, сможет проверить подпись и убедиться, что сообщение было действительно отправлено им и добралось до назначения без искажений. И наоборот, если у пользователя есть открытый ключ другого пользователя, он можете проверять его цифровые подписи. Enigmail применяет защитное преобразование только к содержанию письма.

Enigmail не защищает:

- тему сообщения;
- адреса получателя и отправителя, а также имена, связанные с этими адресами.

Дополнительно, при работе в клиенте Thunderbird, рекомендуется отключать возможность показа писем в формате HTML. Просмотр писем в HTML может создать определенные уязвимости, используемые для атак на веб-браузеры. Кроме того, составление писем в HTML не позволяет корректно работать шифрованию в программе GPG.

Заключение. Применение программных средств шифрования и использование цифровой подписи в почтовых сообщениях позволяет повысить безопасность почтовой переписки.

СПИСОК ЛИТЕРАТУРЫ

1. Деньжонков К.А., Кий А.В. и др. Основы построения и администрирования защищенной операционной системы специального назначения Astra Linux Special Edition: Учебное пособие. СПб: ВАС, 2019, 288 с.
2. Гринь Д.В., Ильина О.Б., Купчиненко О.П., Скоропад А.В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: Сб. тр. СПб.: СПОИСУ, 2017. Вып.4. С. 76-78.
3. Ильина О.Б., Купчиненко О.П., Скоропад А.В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т.2. С 356-360.
4. Ильина О.Б., Купчиненко О.П., Скоропад А.В. К вопросу о дополнительных средствах защиты информации в операционной системе специального назначения «Astra Linux SE» // Информационная безопасность регионов России: материалы XI Санкт-Петербургской межрегиональной конференции, СПб, 23-25 октября 2019 г. СПБ.: СПОИСУ, 2019. Т.2. С 79-81.

УДК 621.391 (075.8)

ИЗМЕНЕНИЯ В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ В СОВРЕМЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЕ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ASTRA LINUX SE

Ильина Ольга Борисовна[1], Купчиненко Ольга Павловна[1], Скоропад Александр Витальевич[2]

[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

[2] Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио»
(Филиал ФГУП НИИР-ЛОНИИР)
Большой Смоленский пр., 4, Санкт-Петербург, 192029, Россия
e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Аннотация. Рассмотрена мандатная сущностно-ролевая модель управления доступом и информационными потоками, которая содержит дополнительные способы разграничения доступа к информации.

Проанализированы отличия в системе защиты информации и особенности применения режима мандатного контроля целостности в операционной системе специального назначения Astra Linux SE Смоленск версии 1.6.

Ключевые слова: операционная система специального назначения; защита информации; мандатная модель разграничения доступа; мандатный контроль целостности; привилегии.

THE CHANGES IN THE SYSTEM OF INFORMATION'S SECURITY IN OPERATING SYSTEMS OF SPECIAL PURPOSE ASTRA LINUX SE

Ilina Olga[1], Kupchinenko Olga[1], Skoropad Aleksandr[2]

[1] The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

[2] Radio Research & Development Institute «Leningrad Branch of Radio Research & Development Institute»
(Branch NIIR-LONIIR)
4 Bolshoy Smolensky Av, St. Petersburg, 192029, Russia

e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Abstract. The mandatory entity-role model of access control and information flows which contains additional ways to differentiate access, were explored. The analysis of the differences in the system of information's security and features of the application of the mandatory integrity control in operating systems of special purpose Astra Linux SE Smolensk, version 1.6 was done.

Keywords: operating system of a special purpose; information security; mandatory model of access control; mandatory integrity control; privileges.

Введение. В настоящее время операционная система специального назначения (ОС СН) Astra Linux SE, является оптимальной платформой для создания отечественной защищенной ОС СН. Наличие в данной ОС СН большого набора сертифицированных средств защиты информации и применение их в комплексе создает основу для проведения работ по созданию надежной, гибкой и усовершенствованной системы защиты информации (СЗИ) в АС СН [1, 2].

Вместо системы принудительного контроля доступа, в ОС СН Astra Linux SE, начиная с версии 1.5, используется запатентованная мандатная сущностно-ролевая модель управления доступом и информационными потоками (МРОСЛ ДП-модель), которая лишена почти все недостатков предыдущих моделей (деклассификация, нарушение логики доступа к данным при обработке потока информации в распределенной среде) и содержит дополнительные способы разграничения доступа [3].

ДП-модель отличается от классической модели мандатного управления доступом, в ней дополнительно реализован мандатный контроль целостности (МКЦ) дистрибутива и файловой системы, предусмотрено ролевое управление доступом и реализовано применение противодействия запрещённым потокам по памяти и времени.В ОС СН Astra Linux SE Смоленск, версия 1.6, представлены следующие отличия в СЗИ:

– после установки ОС (по умолчанию) включен режим МКЦ ОС, установлен параметр ядра max_ilev = 63, все процессы, начиная от init до менеджера входа fly-dm, имеют уровень целостности 63;

– графический сервер Xorg по умолчанию работает не от имени суперпользователя root, а от пользователя, и работает на выделенном уровне МКЦ=8;

– МКЦ на файловую систему (ФС) после установки не включен, и должен быть включен после настройки ОС администратором;

– в системе мандатного разграничения доступа (МРД) настроено 4 уровня конфиденциальности (0 - 3), количество уровней можно увеличить до 255;

– при входе через консоль или графический интерфейс (по умолчанию) суперпользователь, созданный при установке ОС, получает МКЦ=63, «красный» уровень (при входе суперпользователя предусмотрен диалог для выбора значений мандатных атрибутов), обычные пользователи получают нулевой «синий» уровень МКЦ;

– при входе через SSH (Secure Shell) (по умолчанию) автоматически МКЦ=63 для администраторов из группы astra-admin (диалог выбора значений мандатных атрибутов при входе не предусмотрен), пользователи получают нулевой «синий» уровень МКЦ;

– для отдельных служб можно задать свой определенный уровень МКЦ, так же можно задать для службы systemd свой уровень конфиденциальности;

– после включения МКЦ на ФС службы или процессы на определенном уровне МКЦ (например, МКЦ=1 или 2) не смогут записывать данные в файлы и каталоги, на которых максимальное значение МКЦ=63.

Для сетевых сервисов рекомендуется МКЦ=1, для подсистем виртуализации (для гостевых систем, отличных от ОС СН Astra Linux Special Edition Смоленск) МКЦ=2, для внешнего специального программного обеспечения (СПО) МКЦ=3;

– X-сервер по умолчанию работает от имени пользователя fly-dm, МКЦ=8;

– при установке системы следующим устройствам: dev/sd*, /dev/vd*, /dev/hd*, автоматически присваивается уровень конфиденциальности МКЦ=3.

На контейнеры (каталоги) больше нельзя устанавливать флаги ehole, а допускается только установка флагов ccnr, ccnri.

Для упрощения адаптации пользователей к особенностям реализации МКЦ, при установке обновления безопасности значение мандатного атрибута ccnri фиксируется в состоянии включено для всех каталогов файловой системы. Мандатный атрибут ccnri определяет, что контейнер может содержать объекты с различными уровнями целостности, но не большими, чем его собственный уровень целостности и применяется только к контейнерам (каталогам файловой системы).

Флаг ehole доступен для установки на файлах.

В ОС СН Astra Linux SE, версия 1.6, введен новый флаг whole, который дает разрешение на запись в файл «снизу вверх» (чтение по обычным правилам МРД). Флаг whole запрещено устанавливать на контейнерах.

Запись в каталог с высокой целостностью не может быть выполнена процессом с более низким уровнем целостности, чем у контейнера.

Пользователь не может производить запись в контейнер (каталог) с установленным МКЦ>0 в следующих случаях:

– пользователь не вошел в систему на уровне МКЦ > уровня МКЦ контейнера;

– пользователь не обладает привилегией parsec_cap_ignmacint.

Пользователь не может производить запись в контейнер (каталог) с установленной (ненулевой) меткой конфиденциальности и с установленным флагом ccnr информации, отличной от уровня конфиденциальности контейнера в следующих случаях:

– пользователь не зашел под уровнем конфиденциальности равным уровню конфиденциальности контейнера (каталога).

– пользователь не обладает привилегиями parsec_cap_ignmaccat и parsec_cap_ignmaclvl.

Пользователь, который не обладает никакими привилегиями, может производить запись файлов с любым уровнем конфиденциальности, не больше уровня конфиденциальности каталога, в каталог с установленным атрибутом ccnr, если в загрузчике указан параметр ядра parsec.ccnr_relax=1.

Уровни целостности субъекта и объекта сравнивают по битовой маске. Запись в объект разрешается, если для субъекта набор бит уровня МКЦ «включает» в себя набор бит уровня МКЦ объекта.

После установки контроля целостности на ФС максимальный уровень целостности (по умолчанию 63) будет установлен на следующие каталоги: /etc, /lib, /lib64, /lib32, /bin, /sbin, /boot, /root, /opt, /srv, /usr.

Добавлены новые Parsec-привилегии:

– PARSEC_CAP_IPC_OWNER отменяет мандатные ограничения при работе с объектами IPC (Inter Process Communications - межпроцессное взаимодействие), такими как shared memory, message queue и т. д.;

– PARSEC_CAP_BYPASS_KIOSK разрешает игнорировать ограничения Киоска [4];

– PARSEC_CAP_SUMAC разрешает запускать процессы с другим уровнем конфиденциальности.

Привилегия предыдущих версий ОС СН Astra Linux Special Edition Смоленск PARSEC_CAP_UNSAFE_SETXATTR позволяет устанавливать мандатные атрибуты объектов ФС без учета мандатных атрибутов родительского контейнера.

Заключение. Данные изменения в ОС СН Astra Linux SE Смоленск, версия 1.6, позволяют построить такую СЗИ, при работе с которой случайное или преднамеренное нарушение безопасности информационных ресурсов в АС СН под управлением ОС Astra Linux SE сведено к минимуму.

СПИСОК ЛИТЕРАТУРЫ

1. Гринь Д.В., Ильина О.Б., Купчиненко О.П., Скоропад А.В.. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: Сб. тр. СПб.: СПОИСУ, 2017. Вып.4. С. 76-78.
2. Ильина О.Б., Купчиненко О.П., Скоропад А.В. О дополнительных задачах администрирования средств защиты информации в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т.2. С 318-323.
3. П.В. Буренин, П.Н. Девянин и др. Безопасность операционной системы специального назначения Astra Linux Special Edition: Учеб. пособие. М.: Горячая линия – Телеком, 2018, 311 с.
4. Ильина О.Б., Купчиненко О.П., Скоропад А.В. К вопросу о дополнительных средствах защиты информации в операционной системе специального назначения «Astra Linux SE» // Материалы XI Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2019)» 23-25 октября 2019. Т.2. - СПб.: СПОИСУ, 2019. – С. 224-226.

УДК 621.391 (075.8)

К ВОПРОСУ О СЕТЕВОМ ПРОТОКОЛЕ АУТЕНТИФИКАЦИИ

Ильина Ольга Борисовна[1], Купчиненко Ольга Павловна[1], Скоропад Александр Витальевич[2]

[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного

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

[2] Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио»

(Филиал ФГУП НИИР-ЛОНИИР)

Большой Смоленский пр., 4, Санкт-Петербург, 192029, Россия

e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Аннотация. Рассмотрены задачи и принцип работы сетевого протокола аутентификации Kerberos, который ориентирован на клиент-серверную модель и обеспечивает высокий уровень безопасности информации.

Проведен анализ особенностей протокола Kerberos, который позволяет передавать данные через незащищённые сети для безопасной идентификации пользователей и обеспечивает взаимную аутентификацию.

Ключевые слова: аутентификация; авторизация; сетевой протокол аутентификации Kerberos; клиент-серверная модель; билет; центр распределения ключей; область Kerberos.

TO THE QUESTION OF THE NETWORK AUTHENTICATION PROTOCOL

Ilina Olga[1], Kupchinenko Olga[1], Skoropad Aleksandr[2]

[1] The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

[2] Radio Research & Development Institute «Leningrad Branch of Radio Research & Development Institute»
(Branch NIIR-LONIIR)
4 Bolshoy Smolensky Av, St. Petersburg, 192029, Russia

e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Abstract. The tasks and the principle of operation of the network authentication protocol Kerberos, which is focused on the client-server model and provides a high level of information security, are considered. The analysis of the features of the Kerberos protocol, which allows you to transfer data through unsecured networks for secure user identification and provides mutual authentication, is carried out.

Keywords: authentication; authorization; network authentication protocol Kerberos; client-server model; ticket; key distribution center; realm Kerberos.

Введение. Непрерывное совершенствование информационных и сетевых технологий, повышение их роли и значимости требуют постоянного внимания к вопросам обеспечения политики безопасности, без которой работоспособность сети может оказаться под угрозой. Аутентификация или проверка подлинности представляет собой один из важных компонентов любой современной операционной системы специального назначения. Аутентификация заслуживает особого внимания, когда речь идет о защите, так как это процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь, процесс или устройство является именно тем, кем себя объявляет.

Kerberos — сетевой протокол аутентификации, позволяющий передавать данные через незащищённые сети для безопасной идентификации. Kerberos ориентирован на клиент-серверную модель и обеспечивает взаимную аутентификацию, т.е. оба пользователя через сервер подтверждают личности друг друга. Протокол Kerberos разработан для того, чтобы обеспечить надежную аутентификацию пользователей. Начальный обмен информацией между клиентом и сервером происходит в незащищённой среде, а передаваемые пакеты могут быть перехвачены и модифицированы.

Kerberos предоставляет как сетевую аутентификацию, так и безопасный метод, посредством которого может быть проведена авторизация без необходимости повторного ввода пароля или предоставления других аутентификационных данных [1], поэтому он является основой для построения механизмов технологии единого входа (Single Sign-On) - возможности использования единой учетной записи пользователя для доступа к любым ресурсам области.

Протокол Kerberos обеспечивает высокий уровень безопасности, а его преимуществом является то, что ни пароли, ни значения хеша паролей в открытом виде не передаются при любых взаимодействиях. Kerberos не делает никаких предположений о защищённости той сети, поверх которой он работает (он просто ей не доверяет), но, предполагает, что хосты приложений, а особенно хост, на котором работает центр распределения ключей KDC (Key Distribution Center), являются защищёнными.

Kerberos выполняет следующие задачи:

– для предотвращения несанкционированного доступа к службам [2] Kerberos должен обеспечивать аутентификации в сети, т.е. сервер должен иметь возможность идентифицировать пользователей, а клиент – серверы;

– для решения проблемы открытости паролей некоторых сетевых служб, которые создают угрозу безопасности системы, используется техническое маскирование билетов Kerberos. Основным достоинством технологии Kerberos, которая представляет собой механизм аутентификации сервисов и пользователей, является повышенная защищенность в сети, достигаемая с помощью механизма защищенного обмена билетами между сервисами, пользователями и сервером учетных записей Kerberos. При этом для повышенной защищенности от сетевых атак пароли пользователей по сети не передаются. Защищенность билетов от подделки и их уникальность обеспечивается с помощью синхронизации часов клиентских компьютеров с сервером Kerberos, а также механизма открытых и закрытых ключей;

Kerberos позволяет пользователю, единожды пройдя аутентификацию на компьютере, работать с сетевыми сервисами и не вводить дополнительно пароль для обмена с приложениями.

Особенности Kerberos:

– считается, что сетевой трафик может быть прослушан, т.е. может произойти любой несанкционированный доступ к информации, поэтому удостоверяющие данные или пароли никогда не пересылаются по сети;

– удостоверяющие данные никогда не сохраняются на том хосте, который пользователь использует для входа. После первоначального обмена в рамках аутентификации, хост должен забыть сведения о пароле. Вся информация об удостоверяющих данных или паролях хранится в центре распределения ключей Kerberos, который является единственном защищённым местом;

– любому, кто запрашивает данные, серверы приложений и хосты должны быть в состоянии подтвердить свою идентификационную сущность;

– с помощью различные симметричных алгоритмов шифрования все коммуникации между сервисами приложений и аутентифицированными пользователями должны иметь возможность быть зашифрованными.

Аутентификация через Kerberos является стандартом аутентификации доменных пользователей и применяется в Windows Active Directiry, FreeIPA, Samba AD DC, Astra Linux Directory (ALD). В Linux-системах существуют две основные реализаций Kerberos - Heimdal и MIT.

Суть Kerberos состоит в том, что область содержит как минимум один центр распределения ключей KDC (для обеспечения безотказности лучше больше), содержащий базу данных учетных записей. Если пользователь заходит на рабочую станцию под учетной записью, настроенной на Kerberos аутентификацию, KDC выпускает билет на получение разрешения TGT. Пользователь считается аутентифицированным, если он предоставляет совпадающие параметры, и тогда он может запрашивать сервисные билеты для сервисов, поддерживающих Kerberos, которые позволяют пользователю аутентифицироваться на сервисах без ввода имени и пароля, на сервере выдачи билетов (TGS).

Kerberos для контроля доступа [3] к администрированию сервиса использует списки управления доступом ACL (Access Control List), которые позволяют настроить учетные записи с более ограниченными правами.

Для обеспечения возможности авторизации пользователей через Kerberos используются подключаемые модули аутентификации в стеке авторизации PAM (Pluggable Authentication Modules), которые помогут выполнить аутентификацию в Kerberos при входе в систему, а также в приложениях, использующих системную аутентификацию. Механизм PAM, состоящий из набора разделяемых библиотек и конфигурационных файлов (сценариев процедур аутентификации), предоставляет единые механизмы для использования прикладных программ в процессе аутентификации [4] и позволяет интегрировать различные низкоуровневые методы аутентификации.

Заключение. Защита информации в сетевом протоколе аутентификации Kerberos осуществляется с использованием симметричных ключей в отличие от асимметричных ключей, применяемых в большинстве служб аутентификации, поэтому принцип работы Kerberos напоминает инфраструктуру с частным открытым ключом. Такая модель взаимодействия клиента с сервером может работать только при условии достижения целостности и конфиденциальности транспортируемой управляющей информации. Для предотвращения перехвата и несанкционированного использование информации Kerberos реализует при передаче любой управляющей информации систему многократного шифрования.

СПИСОК ЛИТЕРАТУРЫ

1. П.В. Буренин, П.Н. Девянин и др. Безопасность операционной системы специального назначения Astra Linux Special Edition. Учебное пособие. Под редакцией доктора технических наук П.Н. Девянина. М.: Горячая линия – Телеком, 2018. 311 с.
2. Гринь Д.В., Ильина О.Б., Купчиненко О.П., Скоропад А.В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: Сб. тр. СПб.: СПОИСУ, 2017. Вып.4. С. 76-78.
3. Ильина О.Б., Купчиненко О.П., Скоропад А.В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т.2. С 356-360.
4. Деньжонков К.А., Кий А.В., Пащенко В.В. и др. Основы построения и администрирования защищенной операционной системы специального назначения Astra Linux Special Edition: Учебное пособие – СПб.: ВАС, 2019, 288 с.

УДК 621.391 (075.8)

ОРГАНИЗАЦИЯ ЕДИНОГО ПРОСТРАНСТВА ПОЛЬЗОВАТЕЛЕЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Ильина Ольга Борисовна[1], Купчиненко Ольга Павловна[1], Скоропад Александр Витальевич[2]

[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

[2] Санкт-Петербургский филиал «Ленинградское отделение научно-исследовательского института радио»
(Филиал ФГУП НИИР-ЛОНИИР)
Большой Смоленский пр., 4, Санкт-Петербург, 192029, Россия
e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Аннотация. Проведен анализ средств организации Единого пространства пользователей в операционной системе специального назначения Astra Linux SE. Проанализированы механизмы обеспечения безопасности в Едином пространстве пользователей. Представлена общая структура домена Astra Linux Directory. Рассмотрены задачи администратора домена ALD.

Ключевые слова: автоматизированная система; операционная система специального назначения; защита информации; Единое пространство пользователей; домен; аутентификация.

ORGANIZATION OF THE UNIFIED USER SPACE IN AUTOMATED SPECIAL PURPOSE SYSTEMS

Ilina Olga[1], Kupchinenko Olga[1], Skoropad Aleksandr[2]

[1] The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

[2] Radio Research & Development Institute «Leningrad Branch of Radio Research & Development Institute»
(Branch NIIR-LONIIR)
4 Bolshoy Smolensky Av, St. Petersburg, 192029, Russia

e-mails: nastik94@yandex.ru, k-olga102@yandex.ru, sav01236@yandex.ru

Abstract. The analysis of the means of organizing the Unified User Space in operating systems of special purpose Astra Linux SE is carried out. The mechanisms for ensuring security in the Unified User Space have been analyzed. The general structure of the Astra Linux Directory domain is presented. Considered the tasks of the domain administrator ALD.

Keywords: automated system; operating system of a special purpose; protection of information, information security; Unified User Space; domain; authentication.

Введение. Непрерывное совершенствование информационных технологий, повышение их роли и значимости, расширение сферы применения автоматизированных систем специального назначения (АС СН) в процессах управления Вооруженными силами Российской Федерации требуют повышенного внимания к вопросам обеспечения безопасности информации

Основой построения современных АС СН, надежных и функционально устойчивых в условиях современного информационного противоборства, является использование доверенной программно-аппаратной платформы (среды).

В АС СН с уровнем обрабатываемой информации «совершенно секретно» включительно, данные о пользователях должны храниться централизовано. Для этих целей организовано Единое пространство пользователей (ЕПП). Для управления ЕПП в операционной системе специального назначения (ОС СН) Astra Linux SE реализована служба Astra Linux Directory (ALD), которая обеспечивает автоматическую настройку всех необходимых файлов конфигурации служб, а также предоставляет интерфейс управления пользователями и устройствами, администрирования и настройки гибкой и многофункциональной системы защиты информации (СЗИ) в АС СН.

ЕПП включает средства организации работы пользователя в сети электронно-вычислительных машин (ЭВМ), работающих под управлением ОС СН. В основу ЕПП положен доменный принцип построения сети.

Данный принцип основан на объединении в одну сеть логически связанных между собой СВТ, например, принадлежащих одной организации. В этом случае пользователь получает возможность работы с сетевыми ресурсами и взаимодействия с другими пользователями [1].

Решение задачи организации ЕПП (создание домена) обеспечивает: сквозную аутентификацию в сети; централизацию хранения информации об окружении пользователей; централизацию хранения настроек СЗИ на сервере домена; интеграцию в домен защищенных серверов СУБД, электронной почты, гипертекстовой обработки данных и печати; централизованную настройку правил регистрации событий безопасности в рамках домена; централизованный учет подключаемых устройств.

Сетевая аутентификация и централизация хранения информации об окружении пользователя основана на использовании двух основных механизмов NSS и PAM.

Механизм NSS (Name Service Switch (диспетчер службы имен)) предоставляет всем программам и службам, работающим на локальном компьютере, системную информацию через соответствующие программные вызовы.

Механизм PAM (Pluggable Authentication Modules (подключаемые модули аутентификации)) это набор разделяемых библиотек, с помощью которых администратор ОС СН может организовать процедуру аутентификации (подтверждение подлинности) пользователей запускаемыми программами.

В среде ОС СН пользователю поставлен в соответствие ряд атрибутов, которые характеризуют его мандатные права [2]. Средства организации ЕПП позволяют хранить системную информацию о пользователе (доступные мандатные уровни и категории) централизованно. Вся информация хранится в службе каталогов LDAP (Lightweight Directory Access Protocol).

Домен ALD включает одну и более рабочих ЭВМ пользователей, а также специально выделенную ЭВМ, выполняющую функции первичного контроллера домена (PDC – Primary Domain Controller). Все ЭВМ, входящие в домен, работают в едином сетевом сегменте.

Благодаря наличию контроллера домена появляется возможность организации централизованного хранилища учетных записей пользователей домена, а также, централизованного защищенного файлового сервера. Пользователи, зарегистрированные в домене ALD, могут регистрироваться и получить доступ к своим сетевым объектам с любой рабочей ЭВМ домена.

В свою очередь, администратор домена решает следующие задачи:

- централизованное управление учетными записями пользователей домена,
- настройки СЗИ.

После создания мандатных атрибутов домена, можно создавать пользователей домена и присваивать им наряду с дискреционными атрибутами разграничения доступа к объектам домена [3], мандатные атрибуты.

Для реализации удаленной аутентификации используется служба каталогов LDAP в качестве источника данных для базовых системных служб на основе механизмов NSS и PAM. Администратор централизованно управляет конфигурацией сети, выполняя разграничение доступа к сетевым службам.

Служба каталогов LDAP - общее название клиент-серверной технологии доступа к службе каталогов X.500 с помощью протокола LDAP. Служба каталогов X.500 это средство иерархического представления информационных ресурсов, которые принадлежат некоторой отдельно взятой организации. Служба X.500 содержит информацию об этих ресурсах.

Информация, хранящаяся в каталоге, называется «информационной базой каталога» (DIB – Domain Information Base). Пользователь каталога, человек или компьютер, получает доступ к каталогу через клиента. Клиент от имени пользователя каталога взаимодействует с одним или несколькими серверами. Централизованная база данных учетных записей пользователей домена ALD создается на основе службы LDAP, которая обеспечивает организацию хранилища учетных записей пользователей ALD и процедуру аутентификации пользователя с рабочей ЭВМ на контроллере ALD.

За безопасность процедуры аутентификации пользователей домена отвечает протокол доверенной аутентификации Kerberos.

В терминологии Kerberos принципал – учетная запись Kerberos, с определенным набором прав (уникальное имя для клиента, для которого разрешается аутентификация в Kerberos). Пользователь может получать разные наборы прав от Kerberos (разные принципалы).

Если после аутентификации в домене ALD пользователь продолжает работу на рабочей ЭВМ, с которой он вошел в ALD, то к локальным объектам файловой системы этой ЭВМ применяются настройки разграничения доступа, которые хранятся на контроллере ALD.

Если после аутентификации в домене ALD пользователь продолжает работу на рабочей ЭВМ, с которой он вошел в ALD, то к локальным объектам файловой системы этой ЭВМ применяются настройки разграничения доступа, которые хранятся на контроллере ALD.

Учетная запись пользователя домена содержит всю необходимую информацию о пользователе ЕПП: принципал Kerberos, политику паролей, свойства, необходимые для входа пользователя в систему, настройки подключения домашнего каталога пользователя, привилегии пользователя ЕПП и его атрибуты СЗИ.

Заключение. Для решения задач по управлению устройствами, вычислительными процессами и эффективного распределения вычислительных ресурсов в АС СН в соответствии с требованиями руководящих документов по обеспечению защиты информации, в ОС СН организуется ЕПП под управлением службы Astra Linux Directory.

СПИСОК ЛИТЕРАТУРЫ

1. Деньжонков К.А., Кий А.В., Пащенко В.В. и др. Основы построения и администрирования защищенной операционной системы специального назначения Astra Linux Special Edition: Учебное пособие. – СПб.: ВАС, 2019, 288 с.
2. Гринь Д.В., Ильина О.Б., Купчиненко О.П., Скоропад А.В. Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения Astra Linux SE // Региональная информатика и информационная безопасность: Сб. тр. СПб.: СПОИСУ, 2017. Вып.4. С. 76-78.
3. Ильина О.Б., Купчиненко О.П., Скоропад А.В. О механизмах дискреционного разграничения доступа в операционных системах специального назначения // Актуальные проблемы инфокоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4 т. СПб.: СПбГУТ, 2018. Т.2. С 356-360.

УДК 004.054

ТЕНДЕНЦИИ РАЗВИТИЯ СИСТЕМ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ

Калайтанова Елена Владимировна, Ногин Сергей Борисович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: shuvaev88mail.ru, sprintnsb@mail.ru

Аннотация. Статья посвящена вопросу тенденций развития систем автоматизации управления. Определены основные недостатки уже существующих и представлены направления развития систем автоматизации управления.

Ключевые слова: система автоматизации управления; автоматизация; программное обеспечение; информация; проблемные вопросы автоматизации управления.

IMPROVING THE QUALITY OF SOFTWARE FOR AUTOMATED CONTROL SYSTEMS

Kalaitanova Elena, Nogin Sergey
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: shuvaev88mail.ru, sprintnsb@mail.ru

Abstract. The article is devoted to the issue of trends in the development of control automation systems. The main disadvantages of the existing ones are identified and the directions of development of control automation systems are presented.

Keywords: control automation system; automation; software; information; problematic issues of control automation.

Введение. Повышение экономической эффективности производства, качества продукции является непременным условием успешной работы как крупных промышленных компаний, имеющих международный авторитет и признание, так и сравнительно небольших предприятий, обслуживающих потребности ограниченного региона. Решение этих проблем достигается за счёт внедрения современных технологий, оборудования и материалов, механизации и автоматизации производственных процессов и процессов управления [1, 2].

Система автоматизации (СА) управления представляет собой организационно-техническое объединение сил и средств автоматизации и передачи данных. Основным предназначением системы автоматизации является обеспечение управления людьми, боевыми и специальными средствами путем реализации определенной части информационного процесса в соответствующей системе управления. Чем совершеннее система автоматизации, тем большая часть информационного процесса, протекающего в АСУ, реализуется ею.

В настоящее время системы автоматизации развиваются в основном по следующим направлениям:

– увеличение производительности средств и комплексов автоматизации, а также пропускной способности каналов передачи данных при уменьшении их массогабаритных характеристик;

– совершенствование существующих видов обеспечения автоматизированного управления, в первую очередь специального математического и программного, организационного, информационного и лингвистического;

– переход к новым информационным технологиям: распределенной обработке и хранению информации, интеллектуальной поддержке реализации основных функций управления и обучения ДЛ органов управления в процессе их осуществления, адаптации системы автоматизации к требованиям органов управления, электронным картам, пространственному отображению информации, безбумажному управлению, речевым технологиям и др.;

– повышение значений показателей существенных свойств системы автоматизации: готовности, устойчивости, структурной и функциональной мобильности, производительности, безопасности функционирования, чувствительности и корректности;

– поэтапная интеграция на начальных этапах функциональных подсистем системы автоматизации, в последующем − систем связи и автоматизации и построение на этой основе единой информационно-технической системы (ЕИТС) с высокой степенью интеграции услуг.

Опыт эксплуатации СА подтвердил их полезность, показал, что они благотворно влияют на все стороны функционирования управляемых объектов как технологического, так и организационного типа. В то же время даже лучшие СА еще не достигли высокой степени развития. Им присущ ряд недостатков:

– организационно- техническая разобщенность созданных СА;

– слабая техническая и специально-программная оснащенность СА;

– низкая сопрягаемость СА разных звеньев управления и принадлежности.

Такое положение вынуждает вести поисковые работы по дальнейшему совершенствованию и развитию эксплуатируемых и вновь создаваемых СА. К предпосылкам, обуславливающим необходимость в таких работах, также относятся [3,4]:

– изменения в структуре организации и систем управления войсками;

– развитие методов и способов управления;

– повышение требований к управлению в связи с повышением роли организации со временем;

– достижения научно-технического прогресса;

– повышение экономических возможностей государства.

Анализ работ по развитию СА, проводимых как в нашей стране, так и за рубежом, позволяет выявить ряд тенденций.

Повышение степени автоматизации управления. Степень обеспечиваемой автоматизации повышается за счет [5]:

– охвата автоматизацией новых контуров управления, новых функций и задач управления;

– повышения уровня комплексности решения задач управления;

– увеличения доли оптимизационных задач;

– повышения качества диалоговых режимов взаимодействия сотрудников с ЭВМ.

Расширение масштабов интеграции СА. Интеграция СА происходит по горизонтали, по вертикали и по типам управляемых объектов в системах управления.

Сокращение числа типов СА. В будущем предполагается иметь два организационно-технически выделенных типа СА: командные и технологические. Данные типы систем не исключают, а дополняют друг друга.

Создание многофункциональных СА. Многофункциональные системы обеспечивают комплексную автоматизацию функций, относящихся к процессам управления.

Построение СА на концепции разнородной вычислительной сети.

До недавнего времени концептуальной основой построения СА выступала концепция системы телеобработки данных. К существенным недостаткам построенных на этой концепции систем автоматизации относятся:

– использование для передачи данных между ЭВМ и терминалами индивидуальных каналов;

– снижение эффективности использования ЭВМ с ростом пространственного размаха системы и различий в уровне вычислительной сложности решаемых задач;

– низкий уровень интеграции ресурсов.

Эти недостатки вынуждали искать новые концептуальные решения построения СА и ее объектовых комплексов. В результате этих поисков появилась концепция вычислительной сети. Объединяемые в вычислительную сеть сосредоточенные комплексы средств автоматизации могут быть как однородными, так и разнородными и располагаться с различным, практически произвольным удалением друг от друга. Каждому пользователю вычислительной сети может быть обеспечен доступ ко всем ее ресурсам − аппаратным, программным, информационным и даже кадровым. Таким образом, от предшествующих концепций построения СА вычислительная сеть отличается наличием двух ярко выраженных свойств: свойства распределенной обработки данных и свойства коллективного использования сетевых ресурсов. Благодаря этим свойствам вычислительной сети достигается:

– повышение надежности преобразования данных. Надежность повышается за счет интеграции ресурсов (в вычислительных сетях высокий уровень резервирования средств). При выходе из строя одного элемента сети всегда можно выйти на другой;

– увеличение загрузки оборудования;

– реализация распределенной базы данных в полном соответствии с принципами ее построения;

– высокая адаптируемость к изменениям условий функционирования;

– возможность специализации отдельных ЭВМ (ЭВК) на определенные функции и задачи;

– выравнивание нагрузки на отдельные структурные элементы;

– появление условий для совершенствования и развития.

Данные преимущества дают основание считать сетевую концепцию наиболее приемлемой для построения СА.

Интеллектуализация СА. Для сложившейся и используемой до сих пор организации машинной обработки данных характерно то, что решение любой задачи на ЭВМ возможно лишь при полной формализации этого процесса. Чтобы решить ту или иную задачу с помощью ЭВМ, нужны, во-первых, соответствующая программа и, во-вторых, полные и достоверные исходные данные. Такая организация машинной обработки информации имеет серьезные недостатки:

1. Программам решения задач присуща высокая жесткость.

2. По мере роста сложности решаемых задач быстро повышается трудоемкость и стоимость программирования.

3. Многие задачи управления, прежде всего планирования и оперативного управления плохо или совсем не поддаются формализации.

4. Большое число задач не обеспечивается на момент их решения требуемым объемом исходных данных.

В результате многие важные задачи не удается передать ЭВМ и это существенно снижает уровень автоматизации управленческой деятельности руководящего состава.

Выход на новые информационные технологии. Традиционная технология подготовки и решения задач на автономных ЭВМ и в СА характеризуется следующими отрицательными моментами.

1. Подготовка задач к автоматизированному решению выполняется в основном группой специалистов по автоматизации (системный аналитик, алгоритмист, программист). Результатом их работы выступают функциональные (прикладные) программы. Руководящий состав как конечные пользователи оказываются отчужденными от этого процесса.

2. Необходимо сопровождение функционального программного обеспечения специалистами по автоматизации на всем протяжении его эксплуатации.

3. Решение задач конечным пользователем требует участия посредника в лице прикладного программиста. Затруднения конечного пользователя вызываются различиями в системах понятий предметной области и формальной модели, положенной в основу алгоритма решения задачи. При вводе исходных данных к задаче конечный пользователь должен осуществлять интерпретацию ее постановки (переводить постановку из системы понятий предметной области в систему понятий формальной модели). После получения результатов нужна обратная интерпретация. Процесс интерпретации связан с рядом трудностей объективного и субъективного характера. Чтобы уменьшить эти трудности, применяют различные системы оказания помощи конечному пользователю (helpsistems). Однако полное решение вопроса интерпретации в рамках традиционной технологии подготовки и решения задач не представляется возможным.

В основу новой информационной технологии положена идея, состоящая в том, чтобы информация о соответствии между системой понятий предметной области и системой понятий формальной модели входила в исходную информацию для решения прикладных задач. Переход к такой технологии предоставляет конечному пользователю возможность непосредственного участия и даже самостоятельного выполнения работ по созданию и эксплуатации специальных программных средств.

Средства поддержки новой информационной технологии должны обеспечивать:

– представление информации в естественном для конечного пользователя виде: текстов на естественном языке, речевых сообщений, графических изображений;

– постановку задачи для ЭВМ в виде описания требуемых результатов и условий их получения, вариантов выделения подзадач и последовательности их решения;

– формирование среды решения задачи с использованием понятий из области профессиональной деятельности конечного пользователя;

– задание способа диалогового взаимодействия с ЭВМ.

Информация, необходимая для решения прикладных задач по новой технологии, должна включать:

– сведения о системе понятий предметной области, к которой относятся прикладные задачи;

– сведения о системе понятий формальных моделей, на основе которых решаются прикладные задачи;

– сведения о соответствии систем понятий предметной области и формальных моделей для прикладных задач;

– сведения о методах решения прикладных задач;

– сведения о текущем состоянии предметной области.

Если в традиционной технологии процесс обработки информации определяется как выполнение программ, то в новой − как получение требуемых данных.

Таким образом, решение проблем развития систем автоматизации управления в промышленности, на транспорте, в технике связи, в торговле и различных сферах обслуживания способствует повышению экономической эффективности и технологической целесообразности.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 24.103-84 «Автоматизированные системы управления. Основные положения».
2. Кривоносов В. А. Автоматизация технологических процессов и производств: методическое пособие. − Старый Оскол: СТИ МИС и С, 2009. – 60 с.
3. Чуднов А.М., Кирик Д.И., Курашев З.В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений/ Радиотехнические и телекоммуникационные системы. - 2017. -№2. с.41-49.
4. Михайличенко Н.В. Вероятностно-временная модель для анализа динамики изменения состояний центров обработки данных Системы управления, связи и безопасности. 2019. № 1. С. 54-66.
5. Паращук И.Б. Крюкова Е.С. Михайличенко Н.В. Многопараметрические системы хранения данных, дата-центры и электронные библиотеки: способ контроля параметров технического состояния и анализа качества // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020г.: Материалы конференции. Часть 1. \ СПОИСУ. - СПб, 2020. - 393 с.

УДК 621.391

АНАЛИЗ ПОДХОДОВ К ОЦЕНКЕ УСТОЙЧИВОСТИ СИСТЕМ

Карпов Михаил Андреевич, Лепешкин Олег Михайлович, Остроумов Олег Александрович, Савищенко Николай Васильевич

Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: oleg-26stav@mail.ru, eentrop@yandex.ru

Аннотация. В докладе проведен анализ подходов к оценке устойчивости различных систем.

Ключевые слова: критическая информационная инфраструктура; критически важный объект; система связи; функциональная устойчивость.

APPROACHES ANALYSIS TO SYSTEMS STABILITY ASSESSMENT

Karpov Mikhail, Lepeshkin Oleg, Ostroumov Oleg, Savishchenko Nikolay

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@yandex.ru

Abstract. The report analyzes approaches to the various systems stability assessing.

Keywords: critical information infrastructure; critical object; communication system; functional stability.

Введение. Усложнение систем, их элементов, большое количество информации и средства ее обработки, а также предоставление различных услуг требует от государства обеспечения устойчивого функционирования таких систем и объектов. Вопросам устойчивости уделялось много внимания в различных работах, но сейчас, когда отдельные объекты, процессы, элементы систем имеют критическое значение для обеспечения функционирования целых отраслей промышленности, сфер жизнедеятельности общества вопрос обеспечения устойчивости стоит очень остро.

Устойчивость сетей, систем зависит от живучести, надежности, киберустойчивости, помехоустойчивости и функциональной устойчивости, характеризующей выполнение функций и задач в режиме времени близкому к реальному. Изменение любого из этих показателей, без изменения других, приводит к изменению устойчивости.

Основная часть: В [1] рассматривается подход к оценке инженерной устойчивости объектов киберфизических систем. Рассматриваются различные подходы к оценке устойчивости: количественный/качественный, вероятностный/статистический, динамические подход, подход, основанный на моделировании и анализе сложных структур. В этой работе устойчивость рассматривается в аспекте надежности системы.

Не менее важным является устойчивость не всей системы, а ее части, в частности, системы управления. В сложных системах система управления также является сложной. Сбои в ее работе могут привести к серьезным последствия, поэтому они становятся критичными для сложной системы. В работе [2, 3] рассматривается устойчивость через оценку киберустойчивости. Проведен анализ понятия устойчивость и подходов к оценке. Предложен способ оценки киберустойчивости на основе экспертных оценок, моделирования и автоматизации генерации показателей. Устойчивость оценивается через четыре основных показателя (устойчивость к ошибке (робастность), резервирование, гибкость и быстродействие), каждый из которых делится на три подпараметра, зависящие от определенных величин.

В работе [4] оценивается устойчивость систем управления энергетической отрасли на основе анализа деревьев атак. На основе модели деревьев атак получаются количественные показатели уязвимости системы, используемые для оценки устойчивости.

В работе [5] устойчивость энергосистем оценивается через надежность с учетом киберустойчивости системы управления и сбора данных. Проведены оценки вероятностей проведения кибератак на основе представленных моделей атак. Результаты моделирования показали, что увеличение количества атак, без изменения системы безопасности, существенно снижает устойчивость энергосистем.

В работе [6] оценка уязвимостей энергосистем основана на использовании сетевого брандмауэра Петри и моделей паролей в качестве схем защиты. В [13] атаки на интеллектуальную сеть моделируются иерархическим методом, объединяющим несколько небольших сетей Петри доменов сети.

В работе [7] на основе исследования высоковольтной подстанции оценивается устойчивость энергосистем через надежность. Основное внимание уделяется тому, как влияют воздействия и сбои в работе киберсистем на энергосистемы. Предложен алгоритм оценки надежности при моделировании косвенных взаимозависимости между киберсистемами и электросетями. Разработан алгоритм количественной оценки влияния косвенных зависимостей кибер-мощности на показатели надежности, такие как вероятность потери нагрузки (LOLP) и ожидаемая энергия, не обслуживаемая (EENS).

В работе [8] рассматривается обзор проблемы влияния воздействия на киберсистемы на энергетические системы с точки зрения моделирования, использование аналитических методов, теории вероятности, теории графов, методы сетевого анализа, теории матриц, теоретико-игровые методы и т.д.

В работах [9, 10] количественно оценивается устойчивость современных интеллектуальных сетей в энергосистемах через надежность. Предложена концепция сопоставления отказав в киберсети с отказами в энергосети. На основе оптимизационных моделей показана возможность максимизировать передачу данных в киберсети и минимизировать потери нагрузки в электросети.

В работе [11] подход к оценке устойчивости элементов критической инфраструктуры. В статье выделяют параметры, отвечающие за устойчивость, моделируют систему с учетом выделенных параметров и количественно оценивают устойчивость инфраструктуры по индексу устойчивости.

В работе [12, 13] предлагается при оценке устойчивости городской критической инфраструктуры учитывать компетентность лиц, занимающихся оценкой. В [12] рассмотрены подходы к оценке устойчивости и трудности, возникающие при этом. Предлагается использовать таксономию Блума для обеспечения профилей теоретической подготовки специалистов.

В работах [14-15] представлен методологический подход к необходимости исследования устойчивости критической инфраструктуры, в том числе построенной на интеллектуальных системах.

Вывод: Основные направления изучения, оценки и обеспечения устойчивости различных систем направлены на разработку методологических подходов и обеспечение устойчивого функционирования систем. Усложнение техник приводит к необходимости автоматизации и интеллектуализации систем. Возникает понятие критичности отдельных элементов системы, что требует гарантированного обеспечения их безопасного и устойчивого функционирования.

СПИСОК ЛИТЕРАТУРЫ

1. I. Haring, S. Ebenhoch, A. Stolz Quantifying Resilience for Resilience Engineering of Socij Technical Systems. Springer International Publishing. 2016. pp. 21-58. DOI: 10.1007/s41125-015-0001-x.
2. M. A. Haque, S. Shetty and B. Krishnappa, "ICS-CRAT: A Cyber Resilience Assessment Tool for Industrial Control Systems," 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA, 2019, pp. 273-281, doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00058.
3. M. A. Haque, G. K. De Teyou, S. Shetty and B. Krishnappa, "Cyber Resilience Framework for Industrial Control Systems: Concepts, Metrics, and Insights," 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, USA, 2018, pp. 25-30, doi: 10.1109/ISI.2018.8587398.
4. C. Ten, C. Liu and M. Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees," 2007 IEEE Power Engineering Society General Meeting, Tampa, FL, USA, 2007, pp. 1-8, doi: 10.1109/PES.2007.385876.
5. Y. Zhang, L. Wang, Y. Xiang and C. -W. Ten, "Power System Reliability Evaluation with SCADA Cybersecurity Considerations," in IEEE Transactions on Smart Grid, vol. 6, no. 4, pp. 1707-1721, July 2015, doi: 10.1109/TSG.2015.2396994.
6. C.-W.Ten, C.-C.Liu, and G.Manimaran,“Vulnerability assessment of cybersecurity for SCADA systems” IEEE Trans. Power Syst., vol.23, № 4

pp. 1836–1846, Nov. 2008.
7. B. Falahati and Y. Fu, "Reliability Assessment of Smart Grids Considering Indirect Cyber-Power Interdependencies," in IEEE Transactions on Smart Grid, vol. 5, no. 4, pp. 1677-1685, July 2014, doi: 10.1109/TSG.2014.2310742.
8. Libao Shi, Qiangsheng Dai, Yixin Ni, Cyber–physical interactions in power systems: A review of models, methods, and applications, Electric Power Systems Research, № 163, Part A, 2018, doi.org/10.1016/j.epsr.2018.07.015.
9. B. Falahati, Y. Fu and L. Wu, "Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies," in IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1515-1524, Sept. 2012, doi: 10.1109/TSG.2012.2194520.
10. Burlov, V., Lepeshkin, O., Lepeshkin, M. Mathematical model for managing energy sector in the region Advances in Intelligent Systems and Computing, 2021, 1258 AISC, стр. 659–668.
11. Alsubaie A., Alutaibi K., Martí J. (2016) Resilience Assessment of Interdependent Critical Infrastructure. В кн.: Rome E., Theocharidou M., Wolthusen S. (eds) Critical Information Infrastructures Security. CRITIS 2015. Lecture Notes in Computer Science, vol 9578. Springer, Cham. https://doi.org/10.1007/978-3-319-33331-1_4
12. Brauner F., Claßen M., Fiedrich F. (2018) Competence as Enabler of Urban Critical Infrastructure Resilience Assessment. In: Fekete A., Fiedrich F. (eds) Urban Disaster Resilience and Security. The Urban Book Series Springer, Cham.https://doi.org/10.1007/978-3-319-68606-6_11
13. Burlov, V., Lepeshkin, O., Lepeshkin, M. Algorithmic support for the dynamic functioning of transport systems in the regionIOP Conference Series: Materials Science and Engineering, 2020, 918(1), 012224.
14. Йованович А., Эйен К., Чоудхари А. (2018) индикаторный подход к оценке устойчивости интеллектуальных критических инфраструктур. В кн.: Фекете А., Фидрих Ф. (ред.) устойчивость городов к стихийным бедствиям и безопасность. Серия Городских Книг. Спрингер, Чам. https://doi.org/10.1007/978-3-319-68606-6_17
15. Hammad A. W. A., Haddad A. (2021) устойчивость инфраструктуры: оценка, проблемы и идеи. В: Leal Filho W., Azul A. M., Brandli L., Lange Salvia A., Wall T. (eds) промышленность, инновации и инфраструктура. Энциклопедия Целей устойчивого развития ООН. Спрингер, Чам. https://doi.org/10.1007/978-3-319-71059-4_25-1

УДК 004.054

ПРЕДЛОЖЕНИЯ ПО ПОСТРОЕНИЮ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО КОНТРОЛЯ ТЕХНИЧЕСКОГО СОСТОЯНИЯ КОМПЛЕКСОВ СРЕДСТВ АВТОМАТИЗАЦИИ

Ковалев Алексей Андреевич, Авраменко Владимир Семенович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: marinakova817@gmail.com, vsavr@yandex.ru

Аннотация. Рассмотрены цель, задачи и состав системы автоматизированного контроля технического состояния комплексов средств автоматизации. Представлены направления совершенствования системы автоматизированного контроля технического состояния комплексов средств автоматизации.

Ключевые слова: комплекс средств автоматизации; контроль технического состояния; Zabbix; Astra Linux.

PROPOSALS FOR THE CONSTRUCTION OF A SYSTEM FOR AUTOMATED CONTROL OF THE TECHNICAL CONDITION OF COMPLEX AUTOMATION TOOLS

Kovalev Aleksey, Avramenko Vladimir
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: marinakova817@gmail.com, vsavr@yandex.ru

Abstract. The purpose, tasks, requirements and composition of the system of automated control of the technical condition of automation systems are considered. The direction of improving the system of automated control of the technical condition of automation systems are presented.

Keywords: complex of automation tools; technical condition monitoring; Zabbix; Astra Linux.

Введение. Комплексы средств автоматизации (КСА) являются основой построения современных и перспективных автоматизированных систем. Под КСА понимается совокупность всех компонентов автоматизированной системы (АС), за исключением людей [1].

Устойчивость функционирования КСА, а соответственно, и всей автоматизированной системы в целом, во-многом определяется их техническим состоянием. В свою очередь, одной из ключевых функций управления техническим состоянием КСА является контроль технического состояния.

В процессе эксплуатации комплексов средств автоматизации неизбежно возникновение аварийных (критических) ситуаций, представляющих собой сочетание отказов или сбоев (ошибок) функционирования данного КСА, способных привести к значительным нарушениям работоспособности АС [2].

Для исключения ошибок и отказов, а также для планирования технического обслуживания и ремонта необходимо осуществлять постоянный контроль технического состояния КСА.

Основной целью создания и внедрения системы автоматизированного контроля технического состояния КСА является повышение оперативности, достоверности и полноты данных о техническом состоянии КСА, что позволит обеспечить более высокий уровень готовности к применению КСА по предназначению, особенно в условиях негативных воздействий.

Для достижения вышеуказанной цели система автоматизированного контроля технического состояния КСА должна решать следующие задачи:

– регистрация и учет значений параметров элементов КСА;

– выдача предупреждений при превышении пороговых значений контролируемых параметров элементов КСА;

– определение текущего технического состояния КСА;

– прогнозирование технического состояния отдельных элементов КСА и технического состояния КСА в целом.

Текущие и прогнозные значения контролируемых параметров технического состоянии отдельных элементов КСА необходимы администратору КСА для оперативного реагирования на отказы или сбои отдельных средств технического и программного обеспечения, принятие мер по их предупреждению. Информация о текущем и прогнозном техническом состоянии КСА в целом необходима должностным лицам вышестоящей системы управления КСА для своевременного принятия мер по предотвращению или восстановлению нарушения функционирования АС, элементом которой является КСА

Основными свойствами системы автоматизированного контроля технического состояния КСА, к значениям показателям которых предъявляются требования, следующие:

– оперативность;

– достоверность;

– ресурсоемкость.

Современные КСА, как правило, строятся на основе технологии локальных вычислительных сетей, включают серверы, автоматизированные рабочие места и коммуникационное оборудование, соответствующее общее, общесистемное, технологическое и специальное программное обеспечение.

На основании Постановления Правительства РФ от 16 ноября 2015 г. N 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» Федеральные органы исполнительной власти не могут использовать программное обеспечение, не внесенное в «Единый реестр российских программ для электронных вычислительных машин и баз данных». В качестве операционной системы в КСА, применяемых в государственных структурах, широко используется операционная система специального назначения Astra Linux Special Edition 1.6 «Смоленск», в основной комплект поставки которой входит программное обеспечение Zabbix. Таким образом, с юридической, экономической и функциональной точки зрения целесообразно использовать Zabbix в качестве основы для построения автоматизированной системы контроля технического состояния (АСКТС) КСА.

При построении АСКТС на каждом узле ЛВС, кроме сетевого оборудования, должен быть развернут Zabbix-агент, который будет производить сбор, первичную обработку и отправку значений контролируемых параметров на Zabbix-сервер. При этом для разгрузки Zabbix-сервера возможно использование прокси-среверов Zabbix, которые будут принимать значения контролируемых параметров от оконечного оборудования и передавать их на Zabbix-сервер (использование прокси-среверов Zabbix необходимо при большом количестве контролируемых средств автоматизации и сетевого оборудования) [3].

Программное обеспечение Zabbix позволяет производить сбор значений контролируемых параметров, оповещать оператора о превышении их пороговых значений, строить отчеты и графики, но не позволяет оценивать техническое состояния всего КСА и прогнозировать техническое состояние отдельного элемента или КСА в целом. Для решения данной задачи необходима разработка специального программного обеспечения, которое будет получать данные от API Zabbix, производить необходимые математические расчеты и выдавать данные для администратора КСА и должностных лиц руководящего состава (для принятия решений).

АСКТС включает:

– Сервер мониторинга — предназначен для приема и обработки значений контролируемых параметров элементов КСА, их анализа и оповещения администратора.

– Сервер баз данных — предназначен для хранения значений контролируемых параметров и служебных данных.

– Zabbix-proxy — предназначен для снижения нагрузки с сервера мониторинга, при одновременном контроле большого числа средств автоматизации.

– Zabbix-агент — предназначен для съема данных непосредственно с контролируемого средства автоматизации.

Программное обеспечение для оценки и прогнозирования технического состояния КСА.

Для оценки оценки технического состояния КСА может быть использован подход, предложенный в [4]. Для прогнозирования технического состояния могут быть использованы классические статистические методы прогнозирования, а также методы машинного обучения. При формировании показателей (индикаторов) технического состояния КСА следует учитывать, то, что отказ или сбой одного элемента КСА не всегда приводит к нарушению его работоспособного состояния. Кроме того, в зависимости от задач, выполняемых АС на текущем этапе функционирования, отказы, приводящие к невозможности выполнения одной или нескольких функции КСА (например, отказ сервера удаленного доступа или web-сервера) могут не повлиять на выполнение основных задач АС.

Одним из направлений совершенствования автоматизированных систем контроля технического состояния КСА является реализации функции автоматического диагностирования отказов и сбоев КСА, позволяющей администратору в близком к масштабу времени получить данные о месте и причинах их появления, а также

варианты мероприятий (рекомендации) по их устранению. Функция автоматического диагностирования может быть реализована на основе подхода, предполагающего использование искусственных нейронных сетей [5].

Заключение. Оперативность обработки информации о техническом состоянии КСА во-многом зависит от способностей конкретного человека (группы людей). Использование автоматизированной системы контроля технического состояния значительно повышает оперативность контроля и достоверность данных о контролируемом КСА, а наличие в системе контроля механизма прогнозирования позволяет предсказывать поведение всего КСА в целом, правильно запланировать сроки технического обслуживания и ремонта, исключить отказы в работе сложного и дорогостоящего оборудования КСА.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения».
2. Охтилев М.Ю., Соколов Б.В. Теоретические и прикладные проблемы разработки и применения автоматизированных систем мониторинга состояния сложных технических объектов // Труды СПИИРАН. Вып. 1, том 1 — СПб: СПИИРАН, 2002.
3. Руководство по Zabbix [Электронный ресурс] URL: https://www.zabbix.com/documentation/3.4/ru/ manual/definitions/ (дата обращения: 1106.2021).
4. Ясинский С.А., Крюкова Е.С., Паращук И.Б. Базовые понятия и проблемы разработки экспертных систем для контроля технического состояния и качества услуг электронных библиотек // Труды ЦНИИС. Санкт-Петербургский филиал. 2021. Т. 1. № 11. С. 35-43.
5. Авраменко В.С., Маликов А.В. Диагностирование нарушений безопасности информации в инфокоммуникационных системах на основе искусственных нейронных сетей. // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 4 / СПОИСУ. - СПб.: 2017. - 533 с. С. 24-26.

УДК 004.056.3

УПРАВЛЕНИЕ СВЯЗЬЮ И АВТОМАТИЗАЦИЕЙ В СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Ковалев Игорь Станиславович, Пантюхин Олег Игоревич, Пащенко Василий Владимирович, Логинов Вячеслав Алексеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: iskova@yandex.ru

Аннотация. Рассмотрены проблемы интеграции системы управления связью и системы управления автоматизацией в системах специального назначения. Предложены пути решения данных проблем.

Ключевые слова: системы специального назначения; управление связью; система управления связью; интеграция систем управления; проблемы интеграции.

COMMUNICATION AND AUTOMATION MANAGEMENT IN SPECIAL PURPOSE SYSTEMS

Kovalev Igor, Pantyukhin Oleg, Paschenko Vasiliy, Loginov Vjatcheslav
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: iskova@yandex.ru

Abstract. The problems of integration of the communication control system and the automation control system in special-purpose systems are considered The ways of solving these problems are suggested.

Keywords: special purpose systems; communication management; communication management system; integration of management systems; integration problems.

Введение. Управление связью в системах специального назначения (ССН) заключается в целенаправленной деятельности должностных лиц органов управления связью по созданию и всесторонней подготовке системы связи, поддержанию ее в постоянной готовности к обеспечению управления самой ССН, а также по реализации функций управления системой связи при выполнении поставленных задач.

Главной же целью управления связью является обеспечение наиболее эффективного использования потенциальных возможностей системы связи для достижения цели функционирования ССН. Собственно, процесс управление связью осуществляется путем выполнения циклически повторяющейся последовательности функций управления: планирование, учет, контроль, оперативное управление. Каждая функция управления связью реализуется посредством решения определенной последовательности задач управления связью [1].

Известно [2], что любой процесс, а значит и процесс управления связью, сам по себе существовать не может, а требует для своей реализации систему, в данном случае систему управления связью. Организация управления связью заключается в разработке, подготовке и управлении осуществлением комплекса мероприятий по созданию системы управления связью и обеспечении ее эффективного функционирования.

При этом, если в контуре управления связью совместно со средствами и комплексами связи используются средства и комплексы автоматизации, то в таком случае необходимо говорить уже об автоматизированной системе управления связью (АСУС).

АСУС представляет собой совокупность функционально и организационно связанных между собой органов и пунктов управления связью, а также средств управления связью. К средствам управления относят совокупность сетей служебной и технологической связи, а также средства и комплексы автоматизации

управления связью (серверное оборудование и автоматизированные рабочие места должностных лиц органов управления связью), объединенных сетью передачи данных [2-4].

Целью автоматизации процессов управления связью в ССН является сокращение длительности цикла управления, а также повышение обоснованности принимаемых решений за счет: сокращения времени на добывание, сбор и обработку информации о состоянии системы связи; уменьшения доли времени и усилий, затрачиваемых должностными лицами на решение информационных и расчетных задач, документирование принятых управленческих решений, доведение задач, команд, сигналов и распоряжений боевого управления до подчиненных, а также повышения аргументированности и продуманности принимаемых решений.

При этом, основная задача АСУС заключается в управление своевременным и качественным предоставлением всех видов и услуг связи должностным лицам органов управления систем специального назначения в различных условиях обстановки за счет поддержания на необходимом уровне эксплуатационных характеристик системы связи и наиболее рационального использования боевых возможностей ее элементов.

Организация автоматизации управления связью представляет собой процесс разработки, подготовки и управления осуществлением комплекса мероприятий по созданию и обеспечению эффективного функционирования системы автоматизации (СА) управления связью.

Различают организацию применения и организацию обеспечения применения средств и комплексов автоматизации управления связью в системах специального назначения. Фактически в процессе организации применения средств и комплексов автоматизации управления связью определяется, что необходимо сделать, чтобы эффективно реализовать автоматизацию управления связью, а в процессе организации обеспечения такого применения, как именно это нужно сделать.

Обычно состав и взаимосвязи элементов СА управления связью в ССН рассматривают на трех уровням управления: организационном, оперативно-техническом и технологическом уровнях.

При этом, на организационном уровне управления связью в ССН осуществляется автоматизированное планирование связи, планирование применения подразделений связи, а также управление ими в любых условиях обстановки.

На оперативно-техническом же уровне управления связью в системах специального назначения реализуется автоматизированное управление качеством предоставления услуг связи, сетями связи и элементами этих сетей для обеспечения требуемой готовности и эффективного функционирования действующей системы связи и ее элементов.

И, наконец, на технологическом уровне управления связью в системах специального назначения осуществляется автоматизированное управление оборудованием и программными средствами аппаратных связи различного типа.

Современные тенденции развития и совершенствования средств управления в системах специального назначения направлены на все большую интеграцию систем автоматизации и систем связи вплоть до слияния их в единую систему. Сегодня уже практически невозможно определить, где заканчивается связь и начинается автоматизация. Все это, естественно, приводит к необходимости интеграции систем управления связью и систем управления автоматизацией в ССН [5].

Для обоснованного определения путей решения проблем такой интеграции целесообразно выделить следующие уровни интеграции этих систем управления: организационный; функциональный; алгоритмический; информационный; технический.

Характеризуя организационный уровень интеграции, следует отметить, что центры автоматизации входят в состав узлов связи пунктов управления систем специального назначения. Естественно, что в таком случае управление ими должно осуществляется с пунктов управления связью ССН.

Но проблема здесь существует и обусловлена она, прежде всего, неоднозначностью трактовки в руководящих документах вопросов организации автоматизации и организации управления автоматизацией, а также отсутствием единого пункта управления связью и автоматизацией как в системе управления связью, так и в системе управления автоматизацией в ССН.

На функциональном уровне интеграции наблюдается тенденция комплексирования функций передачи и обработки управленческой информации в функции преобразования информации, которые реализуются на единой алгоритмической и технической основе. Эта тенденция реализуется путем постепенной замены аналоговых средств и комплексов связи цифровыми средствами, причем с широким применением принципов программного управления их функционированием.

Но проблема заключается в недостаточном количестве отечественных цифровых средств, комплексов и систем связи, а также в необходимости значительных финансовых затрат на реализацию такой замены.

Интегрирование на алгоритмическом уровне реализуется путем создания единых алгоритмов технологического управления как средствами и комплексами связи, так и средствами и комплексами автоматизации. И оно станет возможным, когда средства и комплексы связи и автоматизации будут способны выдавать информацию о своем состоянии в подсистему технологического управления и воспринимать управляющую информацию из нее на изменение этого состояния.

Проблемы же сегодня и сейчас состоит именно в переходе к применению средств и комплексов связи с указанными выше возможностями и в разработке единых алгоритмов технологического управления как средствами и комплексами связи, так и средствами и комплексами автоматизации.

Существенных проблем интеграции систем управления связью и систем управления автоматизацией на информационном уровне нет, так как в системах связи и системах автоматизации обрабатывается одна и та же информация, за исключением того, что крайне необходимо привести формы обработки этой информации в обеих системах к одному и тому же стандарту.

Интеграция систем управления связью и систем управления автоматизацией на техническом уровне заключается в переходе от аппаратной реализации процесса работы с информацией в средствах и комплексах связи, к программно-аппаратной его реализации на базе применения средств вычислительной техники. Такие средства и комплексы связи должны строиться на той же технической основе, что и средства автоматизации, представляя собой такое средство управления, которое называется программно-техническим комплексом и которое будет способно осуществлять все виды преобразование информации (от обмена информацией до ее обработки).

СПИСОК ЛИТЕРАТУРЫ

1. Анфилатов В.С., Авраменко В.С., Панттюхин О.И. Теоретические основы автоматизации управления войсками и связью. Часть1. Системные основы автоматизации управления войсками и связью: Учеб. пособие. - СПб.: ВАС, 2014.
2. Теория военного управления. Учебник. / Под редакцией С.В. Чернякова. – СПб.: ВАС, 2019.
3. Системы управления военной связью автоматизированные. Термины и определения. (ГОСТ В 28.892-90).
4. Федеральный закон № 126-ФЗ «О связи», 2003.
5. Новые информационные и сетевые технологии в системах управления военного назначения. Часть 2. Новые информационные технологии в системах военного назначения. Учебник. / Под редакцией профессора И.Б. Саенко. – СПб.: ВАС, 2010. 520с.

УДК 004.056

ИНФОРМАЦИОННАЯ СИСТЕМА РЕЙТИНГОВОГО УЧЕТА ОБУЧАЕМЫХ

Колосовский Никита Эдуардович, Михейкина Елена Викторовна,
Озеров Олег Валентинович, Шинкарев Семен Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: se_men82@mail.ru, colos.nikita@gmail.com

Аннотация. Автоматизация позволяет эффективно выстроить целостную схему жизненных процессов организации, придавая им вид единой системы, представляющей собой совокупность взаимозависимых элементов.

Ключевые слова: СУБД; базы данных; ERP-системы; оценка деятельности военнослужащего; Министерство Обороны; рейтинговая система; информационная система, АСУ.

INFORMATION SYSTEM OF RATING ACCOUNTING OF TRAINEES

Kolosovskiy Nikita, Mikheikina Elena, Ozerov Valentin, Shinkarev Semen
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: se_men82@mail.ru, colos.nikita@gmail.com

Abstract. Auromation allows you to effectivety build a holistic diagram of the organization`s life process, giving them the form of a general system, which is a set of interrelated elements.

Keywords: database; ERP-system; assessment of the military; military of defense; rating system; information system; automation.

Введение. Анализ отечественных и зарубежных подходов к всесторонней оценке обучаемых актуален в настоящее время. Все процессы, протекающие в организации (подразделении, предприятия), так или иначе, взаимосвязаны. В связи с этим возникает потребность эффективного комплексного управления всеми процессами и долгосрочного планирования.

Соответственно, для решения поставленных задач большое количество предприятий прибегает к внедрению систем автоматизированного управления.

Одним из ключевых ресурсов в настоящий момент является время, для его экономии используются различные методы. Для экономии времени и средств организации разного размера и направленности внедряют автоматизированные системы. На данном этапе развития отрасли ERP – систем (EnterpriseResourcePlanning) существует достаточно много качественных и проверенных решений для крупных организаций.

Основная потребность заключается в системах бухгалтерского, кадрового, складского и логистического учета. По мнениям специалистов тщательно спланированный ввод в эксплуатацию автоматизированных систем управления позволяет добиться снижения операционных и управленческих затрат в среднем на 15%, а коммерческих – на 35%.

Основная сложность внедрения ERP-систем заключается в правильном их внедрении. Чем сложнее программный продукт – тем большее количество времени и знаний необходимо для грамотной настройки его работы. В условиях достаточно быстро меняющейся экономической ситуации возникает необходимость быстрого реагирования для принятия решений. Крупные корпорации с их ERP-системами являются

инерционными. Соответственно программный продукт, внедренный несколько лет назад, не теряет своей актуальности, тогда время, затраченное на его внедрение и обучение персонала, не играет огромной роли.

1. Сравнение лидеров производителей ERP-систем. Одни из ведущих производителей ERP-систем SAP, Microsoft, Oracle и 1С предлагают специальные решения для таких предприятий. Но даже для этих предложений остается актуальной проблема внедрения системы и ее стоимости. Важно понимать, что для небольших компаний стоимость автоматизации является одним из ключевых факторов при принятии решения о ее внедрении. Основными разработчиками в данной отрасли, на момент июня 2021 г. являются немецкая SAP, американские ORACLE и Microsoft, российская 1С. На российском рынке наибольшей популярностью пользуется 1С. Причем стоимость 1С не сильно отличается от зарубежных ERP.

2. Оценка деятельности обучаемого. Формирование человека как субъекта деятельности начинается с момента его появления на свет. В дошкольном возрасте знания, умения и навыки детьми приобретаются посредством ролевых игр, подражанием взрослым (военным, летчикам, морякам, космонавтам, учителям, врачам и т. д.). Игра выступает в данном случае как форма познания действительности, как тренировка физических и умственных способностей. Учеба занимает большое место и после окончания школы – в вузе, на курсах повышения квалификации и в процессе самообразования.

Зрелый возраст и старость человека связаны с трудовой деятельностью – главным источником человеческого существования и бытия, ибо он удовлетворяет не только элементарные (присущие всему живому), но и высшие человеческие потребности: потребность в творчестве, познании, общении, самосовершенствовании, прекрасном и т. д.

Таким образом, человеческая деятельность развивается, превращая свои средства в цели, а цели в средства. С этим связаны ее дифференциация, происхождение и развитие ее разнообразных видов.

В основе развития человека лежит образование, как система воспитания и обучения личности, а также совокупность приобретаемых знаний, умений, навыков, ценностных установок, функций, опыта деятельности и компетенций.

Образование целенаправленно осуществляется обществом через учебные заведения: детские сады, школы, колледжи, университеты и другие заведения.

В странах Европы достаточно давно уже принята система бакалавриата, кроме того, по итогам накопительного рейтинга после первых двух лет обучения в вузе нередко отчисляется заметная доля менее успевающих учащихся (в том числе не имеющих неудовлетворительных оценок). В постсоветских странах подобные подходы приживаются с большим трудом. В том числе в связи с установкой финансирующих высшую школу учреждений на то, что из любого поступившего в вуз следует «изготовить» полноценного специалиста (то есть концептуальные подходы высшей школы определяют бухгалтеры), а процент неудач должен быть как можно ниже (что не может не сказываться на качестве подготовки).

Основными учреждениями высшего образования являются университеты, академии, военные училища, а за рубежом – и колледжи. Немаловажным фактором хорошего обучения в вузе, в процессе службы и трудовой деятельности является мотивация.

Каждая организация или работодатель, в рамках законодательства, может самостоятельно определять методы, которые побуждают обучающегося (сотрудник, служащего) и весь коллектив к активной деятельности с целью удовлетворения собственных потребностей и для достижения общей поставленной задачи. Мотивированный сотрудник (обучающийся, служащий) получает удовольствие от работы, к которой привязан душой и испытывает радость.

Насильственным образом этого достичь нельзя. Признание достижений и поощрение работников – непростой процесс, требующий учета количества и качества труда, и все обстоятельства возникновения и развития мотивов поведения. Поэтому для организации (руководителя) крайне важно выбрать правильную систему мотивации в отношении сотрудников (подчиненных).

Мотивация может быть: материальная и нематериальная, внешняя и внутренняя, положительная и отрицательная.

Материальная мотивация предусматривает вознаграждение в денежном эквиваленте, в качестве услуг и материальных объектов. Она применяется в отношении сотрудника (обучающегося, служащего) или группы. К примеру, система поощрений. Это премии, разные надбавки, бонусы и т. п. Сотрудник понимает, что чем добросовестнее и качественнее он будет исполнять свои обязанности, тем большее вознаграждение за это он получит. Система штрафов. За плохо сделанную работу, худших итоговых результатов, сотрудник наказывается штрафом.

Нематериальная мотивация, когда сотрудник (обучающийся, служащий) получает эмоциональные выгоды (устранение комплексов, душевное равновесие, признание собственных достоинств и др.). Она применима к одному сотруднику, и всему коллективу, так как помогает формировать отношение каждого индивида к организации. К примеру, рост по карьерной лестнице. Сотрудник старается работать лучше остальных, чтобы получить желаемое продвижение по должности, а это и увеличение вознаграждение, и другой статус. Трудоустройство и полный социальный пакет, согласно действующему Законодательству, является значимым аспектом в поиске работы, а при ее получении хорошей мотивацией.

Внешняя мотивация (экстринсивная) – мотивация, не связанная с содержанием определенной деятельности, но обусловленная внешними по отношению к субъекту обстоятельствами.

Внутренняя мотивация (интринсивная) – мотивация, связанная не с внешними обстоятельствами, а с самим содержанием деятельности.

В рамках выстроенной системы образования, трудовой деятельности, мотивационных принципов, важнейшей составной частью является система оценки деятельности человека (слушателя, преподавателя, сотрудника, должностного лица) и ее реализация.

С этой целью необходимо провести анализ существующих подходов к оценке деятельности личного состава (обучающегося, преподавателя, служащего и других категорий) в ходе их обучения в учебных заведениях, служебной и трудовой деятельности на примерах зарубежного и отечественного опыта.

СПИСОК ЛИТЕРАТУРЫ

1. Хаммер, М. Реинжиниринг корпорации. Манифест революции в бизнесе. / М.Хаммер, Д. Чампи М.: Эксмо, 2009. – 304 с.;
2. Ойхман, Е.Г. Реинжиниринг бизнеса: реинжиниринг организаций и информационные технологии. / Е.Г. Ойхман, Э.В. Попов М.: Финансы и статистика, 1997. – 340 с.;
3. ERP-системы. [Электронный ресурс]. – Режим доступа: https://pro.rbc.ru/60abac3f9a79470a6ff7638e, свободный (дата обращения 22.06.2021).
4. Принципы работы ERP-системы. [Электронный ресурс]. – Режим доступа: https://studopedia.su/2_33709_printsipi-raboti-ERP-sistemi.html, свободный (дата обращения 21.06.2021).

УДК 004.056

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ИНЖИНИРИНГА ТРАФИКА В МУЛЬТИСЕРВИСНЫХ СЕТЯХ СВЯЗИ

Колосовский Никита Эдуардович, Оранский Сергей Владимирович, Шинкарев Семен Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: se_men82@mail.ru, colos.nikita@gmail.com

Аннотация. В статье более детально описывается технология инжиниринга трафика, представляющая собой методы и механизмы, которые позволяют достичь сбалансированной загрузки всех ресурсов сети путем рационального выбора путей прохождения потоков трафика через сеть, раскрываются задачи данной технологии, а также способы их решения.

Ключевые слова: мультисервисные сети; сети связи; автоматизированная система управления.

APPLICATION OF TRAFFIC ENGINEERING TECHNOLOGY IN MULTISERVICE COMMUNICATION NETWORKS

Kolosovskiy Nikita, Oranskiy Sergei, Shinkarev Semen
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: se_men82@mail.ru, colos.nikita@gmail.com

Abstract. The article describes in more detail the technology of traffic engineering, which represents methods and mechanisms that allow achieving a balanced load of all network resources by rationally choosing the paths of traffic flows through the network, reveals the tasks of this technology, as well as ways to solve them.

Keywords: multiservice networks; communication networks; automated control system.

Введение. В последнее десятилетие основным направлением в области развития телекоммуникационных сетей является создание интегрированной универсальной мультисервисной сети. Такая сеть должна предоставлять пользователям возможность оперативно обрабатывать большой объем разнородной информации, в короткое время принимать обоснованное решение и доводить его до многих исполнителей. Этого можно добиться путем рационального управления трафиком. Технологией, осуществляющей такое управление, является инжиниринг трафика [1, 2].

При традиционной маршрутизации трафик маршрутизируется посредством его передачи от одной точки назначения к другой и следует до пункта назначения по пути, имеющем наименьшую суммарную метрику сетевого уровня. Этот путь может не быть оптимальным, так как он зависит от информации о статической метрике канала. В данном случае, при выборе пути не учитываются свободные сетевые ресурсы, текущая загрузка каналов, а также требования к обслуживанию трафика. Таким образом, если кратчайший путь уже перегружен, то пакеты все равно будут посылаться по этому пути, вследствие чего будет наблюдаться картина загруженности одних каналов связи и простоя других.

При маршрутизации, решения управления трафиком принимаются на основе таких параметров, как число промежуточных узлов или задержка. Хотя в силу простоты подобного подхода маршрутизация IP хорошо масштабируется, как правило, в этом случае не удается оптимизировать уровень использования ресурсов в сетевой магистрали. Данная проблема может быть решена только путем преодоления ограничений маршрутизации в соответствии с адресатом и внедрением в сети механизмов управления трафиком.

Задача ТЕ состоит в определении маршрутов прохождения потоков трафика заданного класса сервиса через сеть, т.е. для каждого потока нужно найти точную последовательность промежуточных маршрутизаторов

и их интерфейсов, находящихся на пути между входной и выходной точками потока. При этом все ресурсы сети должны быть загружены как можно более сбалансированно [3].

Решение задачи ТЕ можно искать по-разному. Во-первых, можно искать его заблаговременно, в фоновом режиме. Для этого нужно знать исходные данные: топологию и производительность сети, входные и выходные точки потоков трафика, среднюю скорость передачи данных в них. После этого задачу рационального распределения путей следования трафика при фиксированных точках входа и выхода, а также заданном уровне максимального значения коэффициента использования ресурса можно передать некоторой программе, которая, например, с помощью направленного перебора вариантов найдет решение. Результатом работы программы будут точные маршруты для каждого потока с указанием всех промежуточных коммутаторов.

Заключение. Таким образом, по мере усложнения сетей и роста требований к ресурсам, инжиниринг трафика будет становиться все более важным средством управления сетевыми ресурсами, позволяя оптимизировать производительность, увеличивать общую эффективность и минимизировать нагрузки. Возможность применения технологии инжиниринга трафика в мультисервисных сетях связи представляется осуществимой только после преодоления ограничений маршрутизации.

СПИСОК ЛИТЕРАТУРЫ

1. Олифер В.Г., Олифер Н.А. Компьютеные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.:Питер, 2010. 944с.
2. Лихтциндер Б.Я., Попов П.М. Инжиниринг трафика в мультисервисных сетях: Электросвязь.2005 - №7. С.22-26.
3. Олифер В. Г., Олифер Н. А. Искусство оптимизации трафика [Электронный ресурс]-режим доступа: http://www.op.ru/lan/2001/12/038.htm. (дата посещения 10.06.2021 г.)

УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ

Коростень Александра Олеговна, Аксенов Сергей Сергеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного,
Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия
e-mail: aleksa22-1@mail.ru

Аннотация. Обеспечение безопасности сайта. Виды уязвимостей веб-приложений. Правила обеспечения безопасности веб-приложения. Аутентификация, способы защиты сайта от посторонних пользователей сайта.

Ключевые слова: сайт; веб-приложение; безопасность; данные; угроза; уязвимости; атаки.

INFORMATION SECURITY OF WEB APPLICATIONS

Gantsatsuk Valentin, Zinovieva Nadegda, Mikhailichenko Nikolay, Smirnova Daria
Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny
Tikhoretsky Ave., 3, St. Petersburg, 194064, Russia
e-mail: aleksa22-1@mail.ru

Abstract. Ensuring the security of the site. Types of web application vulnerabilities. Web application security rules. Authentication, ways to protect the site from unauthorized users of the site.

Keywords: website; web application; security; data; threat; vulnerabilities; attacks.

Введение. Web-приложения являются одними из наиболее небезопасных систем на сегодняшний день. Чем больше критически важных и конфиденциальных данных хранит программное обеспечение, тем важнее становится проведение проверки его безопасности. Многолетний опыт различных компаний показывает, что обеспечение безопасности веб-приложений должно начинаться еще на ранних стадиях процесса проектирования и разработки приложений. При разработке веб-приложений необходимо выполнить следующие задачи: избежать уязвимости в приложениях еще на ранних стадиях разработки; сделать так, чтобы разработчики приложений создавали качественные и безопасные конструкции; если имеются приложения, разработанные не внутри компании, необходимо требовать от поставщиков приложений экспертное заключение с целью обеспечения безопасности. Рассмотрим самые популярные виды уязвимостей, их разновидности и способы защиты от них.

На просторах Интернета можно найти веб-приложения, написанные на различных языках программирования; при этом для каждого языка характерен свой набор наиболее значимых уязвимостей. Что касается классических видов уязвимостей так это: SQL injection; PHP include; XSS.

Атаки и уязвимости. CSRF (англ. Cross Site Request Forgery — «Подделка межсайтовых запросов», также известен как XSRF) — вид атак на посетителей веб-сайтов, использующий недостатки протокола HTTP. Если жертва заходит на сайт, созданный злоумышленником, от её лица тайно отправляется запрос на другой сервер (например, на сервер платёжной системы), осуществляющий некую вредоносную операцию (например, перевод денег на счёт злоумышленника). Это атака, при которой злоумышленник пытается вынудить браузер жертвы создать запрос к целевому серверу, втайне от самой жертвы.

Данная атака в чем-то похожа на классическую XSS, в которой злоумышленнику необходимо было вынудить жертву перейти по некоторой ссылке на уязвимую страницу. Здесь же необходимо вынудить пользователя перейти на специально подготовленную злоумышленником страницу, на которую был добавлен

некоторый код. При выполнении данного кода браузер жертвы совершает некий запрос к другому серверу (допустим под видом загрузки изображения), и тем самым выполняет некие, нужные злоумышленнику действия.

Опасность CSRF в том, что данное поведение браузеров и всего HTTP протокола является нормальным. К примеру, ведь нормально то, что сайт может на своих страницах содержать картинки с другого сайта. А браузеру неизвестно заранее что именно пытаются заставить его загрузить, действительно картинку, или под видом данной загрузки будет выполнено какое-то действие на целевом сайте.

XSS (англ. Cross Site Scripting — «межсайтовый скриптинг») — тип атаки на уязвимые интерактивные информационные системы в вебе, внедрение выполняемых на клиентском компьютере вредоносных скриптов в выдаваемую системой страницу. Специфика подобных атак заключается в том, что для атаки на сервер в качестве средства атаки используется авторизованный на этом сервере клиент. К сожалению, межсайтовые скриптовые атаки происходят, в основном, потому что разработчики не в состоянии обеспечить безопасный код.

К счастью, провести XSS-атаку можно так же легко, как и защититься от нее. Прежде всего, нужно думать о том, что вы пишите. Первое правило, которое нужно знать в любой веб-среде (будь то разработка, постановка задач, или производство) никогда не доверять данным, поступающим от пользователя или от любых других сторонних источников. Каждый бит данных должны быть проверен на входе. Это золотое правило предупреждения XSS.

В целях реализации радикальных мер безопасности, которые предотвращают XSS-атаки, мы должны помнить о проверке данных, санитарной обработки данных, и экранирование.

Проверка данных — это процесс обеспечения того, чтобы ваше приложение работает с правильными данными. Если ваш PHP скрипт ожидает целое число, для ввода данных пользователем, то любой другой тип данных будут отклонен, и пользователь получит сообщение об этом. Каждая часть пользовательских данных должна быть проверена при получении.

Санитарная обработка данных сосредоточена на манипулировании данными, чтобы убедиться, что они безопасны. Происходит удаление нежелательных битов данных и их приведение к правильной форме. Например, если на входе вы ожидаете простую текстовую строку, вы можете удалить любую HTML разметку из него.

Для того, чтобы защитить целостность отображения выходных данных, вы должны экранировать их. Это предотвратит попытку браузера непреднамеренно исказить смысл специальных последовательностей символов, которые могут быть найдены им.

Использование стандартной функции secureInnerData, позволяет защитить от атак типа SQL injection и XSS. Чаще всего их проводят, используя GET или POST запросы которые не фильтруются на стороне сервера. Используя данную функцию в качестве фильтра входящих данных, вы сможете частично обезопасить себя

Аутентификация. Если какие-то области веб-сайта должны быть доступны только некоторым клиентам или зарегистрированным пользователям, для подобного разграничения доступа потребуется метод проверки подлинности пользователей.

Существует несколько способов аутентификации пользователей: базовая аутентификация, дайджест-аутентификация и HTTPS.

При использовании базовой аутентификации имя пользователя и пароль включаются в состав веб-запроса. Даже если контент с ограниченным доступом не слишком важен, этот метод лучше не использовать, так как пользователь может применять один и тот же пароль на нескольких веб-сайтах. Старайтесь защищать пользователей от подобных ошибок, используя более безопасные методы аутентификации.

Дайджест-аутентификация, поддерживаемая всеми популярными серверами и браузерами, позволяет надежно шифровать имя пользователя и пароль в запросе. Она помогает обеспечить безопасность имен и паролей, что производит соответствующее впечатление на пользователей и снижает вероятность успешной атаки на сервер.

Протокол HTTPS позволяет шифровать все данные, передаваемые между браузером и сервером, а не только имена пользователей и пароли. Протокол HTTPS (основанный на системе безопасности SSL) следует использовать в случае, если пользователи должны вводить важные личные данные -- адрес, номер кредитной карты или банковские сведения.

При выборе системы аутентификации рекомендуется использовать самый безопасный вариант из имеющихся в наличии. Другие варианты отпугнут клиентов, заботящихся о защите своих данных, и могут привести к возникновению излишнего риска для пользователей.

Заключение. Для того чтобы знать, как обезопасить собственный ресурс необходимо мыслить как бы со стороны атакующего и при этом знать основные требования для успешного проведения атаки: возможность вынудить жертву перейти на страницу с дополнительным кодом. Или возможность модификации злоумышленником часто посещаемых жертвой; отсутствие защиты от CSRF на целевом сайте; пользователь в момент атаки должен быть авторизован для действия, которое мы хотим выполнить от его имени.

И на основе этих требований необходимо попытаться построить защиту.

СПИСОК ЛИТЕРАТУРЫ

1. Авраменко В.С., Бобрешов-Шишов Д.И., Беденков В.Н., Маликов А.В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная научно-техническая и научно-методическая конференция. Т.3. – СПб.: СПБГУТ, 2017. С.13-18.

2. Паращук И.Б. Саенко И.Б. Перспективные направления развития отечественных информационных технологий: материалы VI межрегиональной научно-практической конференции. Севастополь, 22-26 сентября 2020 г. / Севастопольский государственный университет, науч. ред. Б.В. Соколов. – Севастополь: СевГУ, Том2, 2020. – 179 с., С. 243-249.
3. Козлов Д. Д., Петухов А. А. "Методы обнаружения уязвимостей в web- приложениях" / Программные системы и инструменты: тематический сборник ф-та ВМиК МГУ им. Ломоносова N 7. П/р Л.Н. Королева. М: Издательский отдел ВМиК МГУ. Изд-во МАКС Пресс, 2006 г.
4. Издательство БХВ-Петербург, Тактика защиты и нападения на Web-приложения – 2005. – 432с

УДК 025.2.004; 621.311.23: 629.12

ПОДХОДЫ К ВОПРОСУ ОЦЕНИВАНИЯ КАЧЕСТВА И БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ЭЛЕКТРОННЫХ БИБЛИОТЕК

Крюкова Елена Сергеевна
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: e.kkrukovaa69@yandex.ru

Аннотация. Рассмотрена актуальность исследования качества и безопасности электронных библиотек. Обоснована необходимость именно интервальной оценки качества и безопасности таких сложных динамических информационных систем, как электронная библиотека, изложена суть метода теории интервальных средних и ее преимущества. Описана модель электронной библиотеки на базе управляемых непрерывных цепей Маркова в виде разностных стохастических уравнений с использованием методов теории интервальных средних. Указаны этапы методики интервального оценивания качества и безопасности электронных библиотек.

Ключевые слова: электронная библиотека; показатель; качество; безопасность; анализ; модель; методика; оценка; методы теории интервальных средних.

APPROACHES TO QUALITY AND SAFETY ASSESSMENT MODERN ELECTRONIC LIBRARIES

Kryukova Elena
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: e.kkrukovaa69@yandex.ru

Abstract. The relevance of the study of the quality and safety of electronic libraries is considered. The necessity of interval assessment of the quality and safety of such complex dynamic information systems as an electronic library is justified, the essence of the method of the theory of interval averages and its advantages are described. A model of an electronic library based on controlled continuous Markov chains in the from of difference stochastic equations using the methods of the theory of interval averages. The stages of the methodology of interval assessment of the quality and safety of electronic libraries are indicated.

Keywords: electronic library; indicator; quality; safety; analysis; model; methodology; evaluation; methods of the theory of interval averages.

Введение. В настоящее время одним из приоритетных направлений развития вузов и научно-исследовательских организаций является внедрение в процесс обучения информационной образовательной среды (ИОС). Одним из важнейших элементов ИОС являются электронные библиотеки (ЭБ) [1]. Электронная библиотека — это автоматизированная информационная система по обеспечению управляемого доступа к электронным образовательным ресурсам, профессиональным базам данных, информационным справочным и поисковым системам, а также иным информационным ресурсам [2]. Электронные библиотеки, являясь приоритетным направлением развития ИОС, представляет собой большой интерес для их анализа.

Ввиду того, что ЭБ представляет собой сложную динамическую систему, она подвержена воздействию различных факторов, негативно влияющих на ее функционирование. Анализ этих факторов говорит о том, что необходимо грамотно структурировать систему, максимально ограничив отрицательные воздействия на нее, применяя всевозможные средства защиты, как самой системы, так и содержащейся в ней информации [3].

Основным этапом управления любым технически сложным объектом является этап анализа его технического состояния, оценка качества и безопасности. Качество и безопасность как важные свойства любого объекта представляет собой большой и постоянный интерес для его анализа [4].

Существует большое количество подходов к анализу качества и безопасности сложных информационных систем. Так, исследование этих важных свойств объекта в разных научных областях нашло отражение во многих работах отечественных и зарубежных ученых, таких как: Л.Г. Дымовой, В.С. Зайцевой, В.М. Терентьева, Ю.Н. Бобрика, Мэйна, Осаки и других ученых. Развитые в этих исследованиях методы анализа качества и безопасности легли в основу существующих частных методик оценки качества и безопасности сложных информационных систем.

Вместе с тем, дальнейшее их использование для анализа качества и безопасности, и выработки перспективных направлений их развития становится затруднительным в силу ряда причин, одной из ключевых является то, что подавляющее большинство методов нацелены на точечные, пошаговые оценки, тогда, как система управления ЭБ – инертна и больше нуждается в интервальном анализе, поэтому для анализа такой

системы, как ЭБ наиболее применимы методы теории интервальных средних. Суть данного метода заключается в том, что математический аппарат, используемый в этой теории, позволяет рассматривать произвольные типы неопределенностей, имеющие самые различные источники с учетом неполноты и неоднородности исходных данных об элементах системы или о системе в целом. Достоинства данной теории в том, что она позволяет с единых позиций взглянуть на все подходы в описании неопределенностей и предоставляет возможность назначить не жесткие границы какого-либо параметра, а указать приемлемый диапазон значений [5].

Одним из возможных подходов к аналитическому описанию процесса функционирования ЭБ является моделирование динамики изменения ее показателей качества и безопасности (ПКиБ), в пространстве состояний.

В соответствии с принятыми этапами оценки качества и безопасности ЭБ, формального описания всех ее свойств является введение их количественной меры – системы показателей качества и безопасности (СПКиБ).

Основным отличием разработанной СПКиБ от используемых в работах выше указанных авторов является локальная СПКиБ ее контента, так как электронный образовательный ресурс играет ключевую роль в ЭБ.

Для описания изменения состояния ПКиБ ЭБ в непрерывном времени с использованием методов теории интервальных средних применима модель ЭБ на базе управляемых непрерывных цепей Маркова в виде разностных стохастических уравнений.

Ключевым элементом модели являются элементы матрицы интенсивностей перехода ПКиБ ЭБ из состояния в состояние за интервал времени. В уравнении наблюдения за процессом ключевым элементом является матрица наблюдения за процессом перехода ПКиБ из состояния в состояние [6].

Методика оценивания качества и безопасности ЭБ с использованием методов теории интервальных средних включает в себя четыре этапа.

На первом этапе производится сбор статистических данных о значениях ПКиБ на этапе моделирования процесса функционирования ЭБ.

В ходе второго этапа проводится оптимальная фильтрация по критерию минимального среднеквадратического отклонения с применением фильтра Калмана.

В ходе третьего этапа происходит формирование нижнего и верхнего уровней ПКиБ на интервалах времени оценивания.

На четвертом этапе определяются интервальные оценки обобщенного ПКиБ ЭБ с учетом результатов интервального анализа параметров качества и безопасности системы [7].

Заключение. Таким образом, предложенный подход к оцениванию качества и безопасности сложных информационных систем, а также описанная модель и этапы методики оценки качества и безопасности с использованием методов теории интервальных средних позволят получать более точные (адекватные) оценки, что в свою очередь, позволит должностным лицам системы управления ЭБ принимать обоснованные решения по ее управлению. Модель и методика интервальной оценки качества и безопасности ЭБ могут быть использованы практически как совместно, так и по отдельности для анализа любой сложной информационной системы, для которой точечные оценки не являются информативными, а необходимы именно оценки, полученные за интервалы времени наблюдения, что представляет собой большую практическую значимость.

СПИСОК ЛИТЕРАТУРЫ

1. Зуйкина К.Л., Соколова Д.В., Скалабан А.В. Электронные библиотеки в России. Текущий статус и перспективы развития. – М.: Ваш формат, 2017. 120 с.
2. Национальный стандарт Российской Федерации ГОСТ Р 7.0.96 - 2016. Электронные библиотеки. Основные виды. Структура. Технология формирования. – М.: Стандартинформ, 2016. 13 с.
3. Авраменко В.С., Тарасов А.В. Прогнозирование защищенности информации в автоматизированных системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сборник научных статей VIII Международной научно-технической и научно-практической конференции. Т. 4., – СПб.: ГУТ им. А.А. Бонч-Бруевича. 2019. С. 19-24.
4. Паращук И.Б., Чернявский А.В., Крюкова Е.С. Анализ задач, функций и признаков современных электронных библиотек // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020): сборник научных статей IX Международной научно-технической и научно-методической конференции. В 4-х т., – СПб.: ГУТ им. А.А. Бонч-Бруевича. 2020. С. 440-445.
5. Гуров С.В., Уткин Л.В. Надежность систем при неполной информации. – СПб.: Любавич, 1999. 160 с.
6. Крюкова Е.С. Модель функционирования электронной библиотеки для анализа ее качества и информационной безопасности // Вопросы оборонной техники. Научно-технический журнал. Технические средства противодействия терроризму. Серия 16. Выпуск № 9-10 (147-148), 2020. С. 16-22.
7. Крюкова Е.С., Малофеев В.А., Паращук И.Б. Анализ современных подходов к оценке качества систем хранения данных и электронных библиотек // Новые информационные технологии и системы: сборник научных статей XVI Международной научно-технической конференции (г. Пенза, 27–29 ноября 2019 г.). – Пенза: Изд-во ПГУ, 2019. С. 177-180.

УДК 004.056

ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЯ ВЫБОРА ПРОГРАММНЫХ СРЕДСТВ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК НА ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ

Малофеев Валерий Александрович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: valeron12.1366@gmail.com

Аннотация. Проведена технико-экономическая оценка рыночного потенциала полученных в процессе выполнения ПНИЭР результатов. Выполнен обзор программных средств, предназначенных для решения задач выявления сетевых атак, защиты от них и повышения уровня информационной безопасности и функциональности информационно-телекоммуникационных систем, характеризующихся высоким объемом трафика. Рассмотренные программные продукты имеют в своей основе методы и алгоритмы анализа, мониторинга и оценки значительных, но не сверхбольших объемов данных, относящихся к обнаружению сетевых атак и защите от них, характеризуются жестко задаваемой структурой для выявления отклонений в трафике.

Ключевые слова: сетевые атаки; выбор программных средств; безопасность; отклонения в трафике; защита информации; информация.

FEASIBILITY STUDY OF THE CHOICE OF SOFTWARE FOR DETECTING NETWORK ATTACKS ON TELECOMMUNICATION NETWORKS

Malofeev Valery
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: valeron12.1366@gmail.com

Abstract. A technical and economic assessment of the market potential of the results obtained in the process of implementing the PNERD has been carried out. A review of software tools designed to solve the problems of detecting network attacks, protecting against them and increasing the level of information security and functionality of information and telecommunication systems characterized by a high volume of traffic has been performed. The considered software products are based on methods and algorithms for analysis, monitoring and evaluation of significant, but not very large amounts of data related to the detection of network attacks and protection against them, are characterized by a rigidly defined structure for detecting deviations in traffic.

Keywords: network attacks; choice of software; security; traffic deviations; information protection; information.

Введение. Системы предотвращения вторжений (IPS Intrusion Prevention System) это системы анализа трафика, которые позволяют определить и предотвратить сетевые атаки, опираясь на сигнатурный и поведенческий метод. Встроенные системы обучения позволяют значительно снизить количество ложных срабатываний и снизить риск использования существующих уязвимостей. Особенностью некоторых систем является возможность устанавливать виртуальную заплатку на найденную уязвимость, чтобы предотвратить ее эксплуатацию, до того времени, пока производителем не будет выпущено обновления с исправлением данной уязвимости. Защита от сетевых атак просто не предусмотрено, в большинстве организаций информационная безопасность сводится в лучшем случае к установке антивируса. При этом с каждым днем их видов становится на сотни больше и ущерб от последствий только растет

Экспериментальный образец программного обеспечения (ЭО ПО) для обнаружения сетевых атак и защиты от них на основе выявления отклонений в эвристиках трафика сверхвысоких объемов, предназначен для решения задач сбора, предобработки и хранения сетевого трафика сверхвысокого объема, выявления отклонений в эвристиках этого трафика на базе комплексного использования биоинспирированных подходов, методов аналитического моделирования, обнаружения и анализа сигнатур, методов визуальной аналитики, а также выбора контрмер для защиты от сетевых атак.

В состав ЭО ПО входят: компонент сбора и предобработки сетевого трафика сверхвысокого объема; модуль работы с хранилищем данных; компонент обнаружения сетевых атак на основе анализа сигнатур; компонент обнаружения сетевых атак на основе биоинспирированных подходов; компонент обнаружения сетевых атак на основе аналитического моделирования и машинного обучения; компонент комбинирования различных методов обнаружения аномальной активности; компонент противодействия сетевым атакам, а также компонент взаимодействия с оператором системы.

Рассмотрим основные показатели качества, предъявляемые к программным продуктам, и оценим их для данного ЭО ПО.

Надежность ЭО ПО обеспечивается за счет отказоустойчивого и бесперебойного функционирования как отдельных компонентов системы, так и всей системы в целом при условии отсутствия каких-либо внешних воздействий на нее или ее компоненты с участием людских или техногенных факторов. При разработке данного ЭО ПО применялось проектирование «сверху вниз»: сперва определяется общая архитектура системы и ее отдельные компоненты, затем осуществляется детальная реализация каждого отдельного компонента разрабатываемой системы [1-2].

Такой принцип программирования позволяет повысить надежность программ за счет нисходящего уточнения отдельных сущностей и тестирования их взаимодействия на каждом этапе жизненного цикла программы.

Кроме того, в ЭО ПО имеется возможность автоматического возобновления его работы: при возникновении системных сбоев, вызванных отключением электропитания или ошибками в программном коде операционной системы, происходит автоматический запуск ЭО ПО.

Практичность обеспечивается за счет наличия в данном ЭО ПО двух режимов работы: текстового и графического.

Первый режим работы рекомендуется использовать более опытным пользователям, знакомым с командами Linux-интерпретатора. Он обладает более широкими возможностями по настройке системы, включая изменение скриптовых файлов, а также управление отдельными кластерами, процедурами сбора, предобработки и хранения сетевого трафика сверхвысокого объема и распределенной файловой системой (РФС).

Второй режим имеет графический интерфейс пользователя, реализованный на языке программирования C++. В этом режиме системы пользователь получает удобный доступ к основным функциям ЭО ПО. В отличие от текстового режима, в графическом режиме пользователь избавляется от необходимости ручного ввода команд и знаний особенностей работы РФС и используемой Hadoop/Spark, особенностей различных используемых подходов и методов выявления отклонений в эвристиках трафика сверхвысоких объемов для обнаружения сетевых атак и защиты от них. Вместо этого ему предлагается понятная оболочка, с помощью которой можно запускать процессы сбора, предобработки и хранения сетевого трафика сверхвысокого объема, выявления отклонений в эвристиках этого трафика на базе комплексного использования биоинспирированных подходов, аналитического моделирования, обнаружения и анализа сигнатур, запускать модуль визуализации и процедуры выбора контрмер для защиты от сетевых атак.

Эффективность использования ЭО ПО заключается в следующем. По типу архитектуры ЭО ПО принадлежит к классу распределенных систем. Особенностью таких систем является возможность разбиения задачи на отдельные подзадачи и решения каждой из них на отдельном сервере (вычислительном узле). После выполнения всех подзадач мастер (управляющий менеджер) объединяет (агрегирует) их. Такой подход позволяет повысить скорость обработки трафика сверхвысоких объемов и снизить нагрузку на отдельные кластеры (компоненты) внутри всей программной системы для обнаружения сетевых атак и защиты от них.

Сопровождаемость программы характеризуется наличием в ее составе компонента, осуществляющего функции по уведомлению администратора о случаях внештатных сбоев посредством отправки электронных писем или SMS-сообщений. В разработанном ЭО ПО таких функций не предусмотрено в соответствии с требованиями Технического задания [3-5].

Мобильность программы подразумевает ее возможность переноса на другую программную или аппаратную платформу (кроссплатформенность). Данный ЭО ПО частично поддерживает эту функцию, а именно компоненты, реализованные на языке C++, могут быть портированы. без существенных изменений, как под различные операционные системы, так и под различные аппаратные платформы, для которых существует соответствующая им версия виртуальной машины.

Заключение. Как правило, такие программные обеспечения используют упрощенные алгоритмы обработки трафика, базы данных сигнатур атак на основе простых реляционных моделей, не предлагают выбор контрмер для защиты от сетевых атак, что не позволяет в достаточной степени эффективно выявлять сетевые атаки и защищаться от них в условиях наличия сетевого трафика сверхвысокого объема. Для решения этой задачи был разработан методический подход к построению комплексной, многокомпонентной системы выявления отклонений в эвристиках трафика сверхвысоких объемов, для обнаружения сетевых атак и защиты от них, обладающей большей оперативностью, гиб-костью и требующей меньших вычислительных ресурсов и ресурсов памяти за счет наличия низкоуровневых драйверов захвата сетевого трафика, механизмов его балансировки, использования распределенной шины данных и технологии netflow для агрегации трафика, за счет использования распределенные системы хранения, параллельных алгоритмов сигнатурного анализа, биоинспирированных методов, нейросетевых и нейронечетких алгоритмов.

СПИСОК ЛИТЕРАТУРЫ

1. Тютюнников, Н.Н. Оценка затрат на разработку и сопровождение программных средств терминологического фонда по базовому уровню модели COCOMO [Текст] / Н.Н. Тютюнников // Актуальные вопросы экономических наук. – 2013. – №35. – С. 89–94.
2. Авраменко В.С., Тарасов А.В. Прогнозирование защищенности информации в автоматизированных системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сборник научных статей VIII Международной научно-технической и научно-практической конференции. Т. 4., – СПб.: ГУТ им. А.А. Бонч-Бруевича. 2019. С. 19-24.
3. Гуров С.В., Уткин Л.В. Надежность систем при неполной информации. – СПб.: Любавич, 1999. 160 с.
4. Созинова Е.Н. применение экспертных систем для анализа и оценки информационной безопасности // Молодой ученый. №10. 2011. С. 64-66.
5. Ненадович Д.М., Паращук И.Б., Лещенко А.С. Особенности экспертных систем в интересах анализа информационной безопасности телекоммуникационных сетей // V-я Санкт-Петербургская Межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)». Материалы конференции. – СПб.: СПОИСУ, 2007. С. 114-115.

УДК 004.056.5

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ: ЭТАПЫ РАЗРАБОТКИ МЕТОДИКИ АНАЛИЗА В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

Михайличенко Николай Валерьевич, Паращук Игорь Борисович, Михайличенко Антон Валерьевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: 23esn2008@rambler.ru, shchuk@rambler.ru, katjuha777@inbox.ru

Аннотация. Сформулированы задачи и предложено описание физической сущности этапов разработки методики многокритериального анализа информационной безопасности мобильных дата-центров. Рассмотрены различные подходы к совершенствованию методологии и инструментария анализа информационной

безопасности современных мобильных центров обработки данных в условиях неопределенности. При этом учитывались различные условия обстановки, различные уровни возможных угроз и различные аспекты неопределенности исходных данных, которые могут быть идентифицированы и нейтрализованы с использованием нейро-нечетких сетей и гранулярных вычислений.

Ключевые слова: мобильный центр обработки данных; нейро-нечеткая сеть; гранулярные вычисления; анализ; информационная безопасность; защищенность; показатель; этап.

INFORMATION SECURITY OF MOBILE DATA CENTERS: STAGES OF DEVELOPMENT OF THE METHODOLOGY OF ANALYSIS IN CONDITIONS OF UNCERTAINTY

Mikhailichenko Nikolay, Parashchuk Igor, Mikhailichenko Anton
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, katjuha777@inbox.ru

Abstract. The tasks are formulated and the description of the physical essence of the stages of development of the methodology for multi-criteria analysis of information security of mobile data centers is proposed. Various approaches to improving the methodology and tools for analyzing the information security of modern mobile data centers in conditions of uncertainty are considered. This took into account different environmental conditions, different levels of possible threats, and various aspects of the uncertainty of the source data, which can be identified and neutralized using neuro-fuzzy networks and granular computing.

Keywords: mobile data center; neuro-fuzzy network; granular computing; analysis; information security; security; indicator; stage.

Введение. Для реализации своевременного и эффективного управления всеми сферами жизни страны и общества необходимо использовать новейшую IT-инфраструктуру. Ключевым элементом построения IT-инфраструктуры практически любого масштаба являются центры обработки данных (ЦОД), иногда называемые дата-центрами [1]. В большинстве случаев под ЦОД понимается специализированное помещение, стационарное сооружение или мобильное помещение для размещения серверного и сетевого оборудования. С помощью этого оборудования к ЦОД подключаются абоненты по каналам специализированных сетей или сети Интернет.

Особое внимание специалистов в последние годы сосредоточено на поиске новых технических и программных решений по хранению и обработке больших массивов данных. В этих условиях все более очевидна необходимость разработки гибких и масштабируемых систем хранения данных, а эффективным решением данных проблем могут стать мобильные ЦОД (МЦОД) [2, 3].

Мобильные ЦОД предназначены для: оперативного развертывания IT-инфраструктуры в труднодоступных и, зачастую, отдаленных местах; для «приближения к клиенту» – размещения IT-инфраструктуры рядом с потребителями; для реализации возможности частого перемещения (перевозки) и установки в различных местах; для быстрого развертывания инфраструктуры или увеличения ее мощности (масштабирование), а также для выполнения функций резервного ЦОД [4, 5].

Вместе с тем, необходимо признать, что пока не существует единого подхода в вопросах управления МЦОД и в вопросах анализа и обеспечения их информационной безопасности. Все это делает, безусловно, актуальной проблему выработки системного подхода в вопросах оценивания и обеспечения информационной безопасности МЦОД, а также задачу разработки моделей и методов повышения защищенности элементов таких систем (аппаратных, программных, иных) и, в целом, защищенности систем такого класса [6].

Решение предложенной проблемы на основе новых моделей и методов, позволит унифицировать механизмы оценивания и обеспечения информационной безопасности МЦОД и упростить внесение изменений в его инфраструктуру безопасности, будет способствовать повышению защищенности МЦОД, а также тиражируемости и масштабируемости структурных решений, нацеленных на повышение информационной безопасности систем такого класса. По-прежнему, важно получить ответ на вопрос – как в условиях постоянного роста цены ресурсов, затрачиваемых на защиту, получать максимальную отдачу от эксплуатации системы информационной безопасности МЦОД. При этом возникают сопутствующие задачи, которые необходимо решать при управлении информационной безопасностью мобильных ЦОД: как добиться существенного увеличения основных показателей защищенности; каким образом при минимизации затрат учесть возможный рост уровня и количества угроз безопасности, предусмотреть восстановление полной работоспособности МЦОД после компьютерных атак. Решение этих основных и сопутствующих задач возможно в рамках и по результатам процесса анализа информационной безопасности МЦОД.

При этом важным является решение задачи создания достоверных и оперативных алгоритмов анализа информационной безопасности, которые позволят максимально точно, в оговоренные сроки и полноценно оценить защищенность МЦОД с учетом динамики изменения условий их применения, динамики угроз, а также с учетом неопределенности исходных данных, необходимых для принятия решения по управлению информационной безопасностью МЦОД. Предполагается сосредоточиться на создании методики, достоверных и оперативных частных алгоритмов многокритериального оценивания информационной безопасности МЦОД, причем надо пройти несколько последовательных этапов:

Первый этап: формулировка системы показателей информационной безопасности МЦОД, а также синтез вероятностно-временной модели процесса смены состояний защищенности мобильного дата-центра, которая будет учитывать неопределенный характер изменения значений показателей информационной безопасности на основе применения математического аппарата условных вероятностей, нейронных сетей и методов гранулярных вычислений [7].

Второй этап: разработка обобщенного и частных алгоритмов анализа информационной безопасности МЦОД в условиях неопределенности.

Описание программных средств формирования и расчета информационной безопасности МЦОД в условиях неопределенности, а также рекомендации по использованию программно-алгоритмических средств при управлении защищенностью МЦОД, могут составлять содержание третьего этапа.

И наконец, в рамках четвертого этапа возможно проведение проверки конструктивности разработанной методики и алгоритмов анализа информационной безопасности МЦОД в условиях неопределенности. Проверка конструктивности позволит разработать научно-технические предложения по совершенствованию системы обеспечения информационной безопасности сложных мобильных информационных объектов такого класса.

Объективно существующая неопределенность исходных данных, важных для анализа информационной безопасности МЦОД, обуславливает необходимость привлечения для задач анализа защищенности новых методов и средств, например, таких, как часто применяемые в рамках интеллектуальной обработки данных нейро-нечеткие сети [8] и алгоритмы гранулярных вычислений [9, 10].

Заключение. Таким образом, рассмотрен новый подход к совершенствованию методологии и инструментария анализа информационной безопасности современных мобильных ЦОД. Сформулированы частные задачи и проведено описание этапов разработки методики многокритериального анализа информационной безопасности мобильных ЦОД в различных условиях обстановки, с учетом различных аспектов неопределенности исходных данных, которые могут быть учтены в рамках математики нейро-нечетких сетей и гранулярных вычислений. Это позволит повысить достоверность анализа информационной безопасности МЦОД за счет уточнения (реконструкции, верификации) неточных, зашумленных нечетких исходных данных большой размерности, повысить объективность задания этих исходных данных, а в конечном итоге, получить выигрыш в достоверности и оперативности анализа информационной безопасности, что призвано способствовать повышению эффективности процесса информационной поддержки принятия решений по обеспечению защищенности мобильных ЦОД в условиях различного вида угроз и негативных воздействий.

СПИСОК ЛИТЕРАТУРЫ

1. Национальный стандарт Российской Федерации ГОСТ Р 58811 - 2020. Центры обработки данных. Инженерная инфраструктура. Стадии создания. – М.: Стандартинформ, 2020. – 17 с.
2. Мобильный модульный центр обработки данных. [Электронный ресурс] // ПитерЭнергоМаш. URL: http://piterenergomash.ru/index.php/katalog-produktsii/kontejnernye-resheniya/kontejnernye-tsod (дата обращения 30.04.2021).
3. Паращук И.Б., Михайличенко Н.В. Особенности построения и анализа качества дата-центров как базовых элементов IT-инфраструктуры // Перспективные направления развития отечественных информационных технологий: материалы IV Межрегиональной научно-практической конференции. – Севастополь: Севастопольский государственный университет, 2018. – 352 с., С. 28-29.
4. Google Unveils Its Container Data Center. Data Center Knowledge. [Электронный ресурс] // Google (Alphabet). URL: https://www.datacenterknowledge.com/archives/2009/04 /01/google-unveils-its-container-data-center/ (дата обращения 30.04.2021).
5. Мобильные центры обработки данных. [Электронный ресурс] // Инженерно-техническая компания «ИЛТОР». URL: https://iltor.ru/projects/data-centry/ (дата обращения 30.04.2021).
6. Авраменко В.С., Бобрешов-Шишов Д.И., Беденков В.Н., Маликов А.В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная научно-техническая и научно-методическая конференция. Т.3. – СПб.: СПБГУТ, 2017. С.13-18.
7. Бутакова М.А., Климанская Е.В., Чернов А.В. Формальные структуры и представления для гранулярных вычислений. // Современные наукоемкие технологии. 2018. №5. С. 36-40.
8. Андриевская Н.В., Резников А.С., Черанев А.А. Особенности применения нейро-нечетких моделей для задач синтеза систем автоматического управления. // Фундаментальные исследования. Технические науки. № 11. 2014. С. 1445-1449.
9. Минаев Ю.Н., Филимонова О.Ю., Минаева Ю.И. Гранулярный компьютинг в системе нечетких множеств на уровне тензорных гранул // Проблемы информатизации и управления. 2012. №4(40). С. 51-61.
10. Бутакова М.А., Гуда А.Н., Иванченко О.В., Карпенко Е.В. Элементы теории гранулярных вычислений с нечеткими приближенными информационными гранулами. // Вестник Ростовского государственного университета путей сообщения. 2015. № 4(60). С. 27-33.

УДК 621.391.28

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ СКВОЗНОГО КАЧЕСТВА УСЛУГ B2C В СЕТИ LTE

Мошак Николай Николаевич, Щербак Владимир Игоревич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: nnmoshak49@mail.ru, ius@sut.ru

Аннотация. Анализируются проблемы сопоставления значений индикатора качества услуг QCI сети LTE и кода дифференцированных услуг DSCP сети DiffServ.

Ключевые слова: параметры QoS LTE; услуги B2C LTE; соединение E2E LTE; технология DiffServ.

PROBLEMS OF ENSURING END-TO-END QUALITY OF B2C SERVICES IN LTE NETWORK

Moshak Nikolay, Shcherbak Vladimir
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: nnmoshak49@mail.ru, ius@sut.ru

Abstract. Problems of matching values of QCI quality of service indicator of LTE network and differentiated service code of DSCP DiffServ network are analyzed.

Keywords: QoS LTE parameters; services B2C LTE; E2E LTE connection; DiffServ technology.

Сеть LTE или развитая пакетная система EPS (Evolved Packet System) состоит из сети радиодоступа RAN (Radio Access Network) и ядра сети EPC (Evolved Packet Core). Для передачи сервисного информационного потока конкретной услуги B2C в сети LTE организуют составной сквозной E2E (end-to-end) виртуальный канал (bearer) соответствующего класса обслуживания QoS между двумя оконечными точками: либо между двумя оконечными устройствами UE (Urser Equetvitment), либо, например, между UE и каким-либо интернет-сервером. Соответственно этому, возникают понятия части сквозного канала, представленные на рис.1: радиоканал (radio bearer) между UE и eNB, S1- bearer между eNB и S-GW, канал радиодоступа E-RAB (E-UTRAN Radio Access Bearer) между UE и S-GW, S1-S5/S8- bearer между S-GW и P-GW, EPS-канал (EPS-bearer) выделенной пакетной системы EPS между UE и P-GW, внешний канал (external bearer) – между P-GW и внешней IP-сетью и др. Канал E-RAB является частью канала EPS-bearer [1]. Таким образом, канал EPS (EPS- bearer) — это маршрут, который пользовательский трафик (IP-потоки) использует между UE и P-GW.

Аналогично понятию сквозного канала вводится понятие сквозной услуги B2C в сети LTE - сервис E2E (end-to-end service) как последовательность действий между двумя оконечными пользователями и, соответственно, частей услуг — по их отношению к определённых сетевым составляющим: в локальном канале «оконечное оборудование— пользовательский терминал» (Terminal Equipment / Mobile Terminal local Bearer Service), в канале сети LTE (LTE Bearer Service), во внешнем канале (External Bearer Service). Таким образом, возникает многоуровневое взаимодействие при передаче услуги в различных сетевых узлах и на различных уровнях.

В сетевой структуре LTE существует два разных уровня IP-сетей. Первый — это сквозной уровень, который обеспечивает сквозное E2E соединение для пользователей. Этот уровень включает в себя UE, PGW и удаленный хост (включая возможные интернет-маршрутизаторы и хосты между ними), но не включает eNB и SGW. При этом LTE EPC может поддерживать протоколы типа IPv4 и IPv6. Второй уровень IP-сетей — это внутренняя сеть EPC. Она включает в себя все узлы eNB, узлы SGW и узлы PGW. Эта сеть реализована как набор двухточечных линий связи, которые соединяют каждый eNB с его соответствующим узлом SGW и двухточечной линии связи, которые соединяют каждый узел SGW с его соответствующим узлом PGW. Таким образом, каждый SGW имеет набор двухточечных устройств, каждое из которых обеспечивает возможность подключения к другому eNB. При передаче данных по сети пользовательские потоки должны пройти несколько интерфейсов (LTE-Uu, S1, S5/S8) прежде, чем они попадут во внешнюю сеть или на абонентский терминал. Сквозной E2E IP-канал туннелируется по внутренней IP-сети EPC с использованием двух туннелей на интерфейсах S1 и S5/S8. На интерфейсах S1 и S5/S8 каждый поток определяется идентификатором GTP (GPRS Tunneling Protocol туннеля [2].

Концепция качества сервиса QoS, используемая в сетях LTE, основана на классе, где каждому типу канала-носителя назначается один идентификатор класса качества обслуживания QCI (Quality Chanel Indicator) сетью. Идентификатор QCI - это механизм, используемый в сетях LTE для гарантии того, что трафику канала EPS назначается соответствующее качество обслуживания QoS. Различному трафику EPS канала требуется разное QoS и, следовательно, разные значения QCI. Значения QCI стандартизированы в стандарте 3GPP TS 23.203 «Policy and charging control architecture» [3] и связаны с конкретными характеристики QoS. Характеристики каждого значения QCI используется оператором для предварительной конфигурации параметров, специфичных для узлов сети, чтобы гарантировать, что приложения/услуги, которые используются в сети LTE, отображаются на заданный индикатор QCI и получают одинаковый уровень QoS в мультивендорных средах, а также в роуминге.

Индикатор QCI используется в сети доступа на узлах eNB для контроля приоритета пакетов, доставляемых по радиоканалам. Кроме того, характеристики QCI также отображаются на параметры соответствующих узлов ядра базовой сети EPC и параметры транзитных маршрутизаторов внешней мобильной IP-сети на технологии DiffServ [RFC 2475] оператора связи. Это реализуется с помощью предварительно сконфигурированного отображения индикатора QCI в определенные значения кода дифференцированных услуг DSCP (DiffServ Code Point). В качестве кодов DSCP используются шесть первых битов поля DS (Differentiated Service) заголовка пакета IPv6. Весь сетевой трафик внутри домена DiffServ получает определенный режим обслуживания PHB (Per-Hop Behavior) в зависимости от указанного в байте DS класса трафика, называемый «Режимом на переходе» из группы режимов PHB, поддерживаемых в пределах домена. Документ [RFC 2475] определяет PHB как комбинацию функций маршрутизации, классификации, обработки очередей и методов сброса пакетов на каждом шаге передачи пакета от узла к узлу внутри домена DiffServ. Режим PHB можно рассматривать как совокупность параметров, в соответствии с которыми маршрутизатор устанавливает порядок направления пакетов на интерфейс вывода. Это могут быть отдельные очереди с заданными приоритетами, определенные параметры для установления длины очереди или алгоритмы удаления пакетов из обращения в зависимости от их приоритета и веса. Группа режимов — это набор одинаковых или различных режимов PHB, каждый из которых может быть реализован на УК одновременно с

другими при обслуживании очередей. Пакеты «окрашенные» одинаковым кодом DSCP получат одинаковый класс сервиса в сеансе связи во всех транзитных маршрутизаторах домена выбранного маршрута посредством предоставления соответствующей услуги PHB для всего агрегированного потока. Значение кода DSCP устанавливается в соответствии с заранее оговоренным уровнем сервиса в соответствии с характеристиками индикатора QCI и предоставляемым пользователю при поступлении от него потока пакетов на обслуживание. В [4] определяется эквивалентное отображение идентификатора QCI в значение кода DSCP. В зависимости от значения, принятого QCI в сети к пакету, применяется тот или иной механизм обслуживания QoS [5]. Стандарты LTE допускают существование домена Diffserv внутри UE и за пределами границ EPS. Домен Diffserv не рассматривается в EPS, где QCI используются для определения и передачи параметров QoS. Рекомендации 3GPP по отображению подмножеств профилей QoS на идентификаторы QCI и наоборот применяются в точке соединения между сетью сотового доступа и IP-сетью. Такая точка соединения может обычно возникать в eNB и в шлюзе пакетных данных P-GW. Для преобразования параметров Diffserv в параметры QCI и наоборот используется функция диспетчера службы носителя протокола Интернет (IP BS Manager), которая может быть интегрирована как в UE (как граница домена Diffserv между доменом Diffserv, присутствующим в сетевом стеке UE, и сетью радиодоступа LTE), так и в P-GW.

Стандарты 3GPP не определяют и не рекомендуют какое-либо конкретное сопоставление между каждым значением индикатора QCI и значением кода дифференцированных услуг DSCP. Выбор этого сопоставления оставляют за оператором пограничного домена. Однако 3GPP определяет, что «для магистрали на основе IP должны использоваться дифференцированные услуги, определенные IETF» ([TS 23.107] v15 6.4.7) [3]. Кроме того, новые QCI могут потребовать новых классов трафика и маркировки Diffserv. Таким образом, на практике узлам ядра EPC LTE и транзитным маршрутизаторам внешних операторов сложно одновременно обрабатывать и пересылать пакеты на основе характеристик QCI. Требования сквозного QoS могут не соблюдаться, особенно внутри зашифрованного туннеля. Кроме того, например, маршрутизаторы Cisco или Juniper при обслуживании пакетов только решают вопрос очередности их отправки с помощью механизмов планирования (WFQ, DWRR, SPQ и др.) исходя из приоритета пакетов без учета задержки, уровня ошибок и потерь. Это требует ручной настройки параметров QoS на узлах ядра сети и узлах внешних операторов. При этом, если в любом месте сквозного соединения E2E LTE на транзитных маршрутизаторах имеются неправильные настройки, то сервисы B2C, не будут должным образом предоставлены сетью для пользователя с требуемым качеством вплоть до полной их деградации.

В докладе анализируются проблемы сопоставления значений индикатора QCI сети LTE и значений кода дифференцированных услуг DSCP сети Diffserv.

СПИСОК ЛИТЕРАТУРЫ

1. Гельгор А.Л. Технология LTE мобильной передачи данных: учеб. пособие / Гельгор А.Л., Попов Е.А. — СПб.: Изд-во Политехн. ун-та, 2011. — 204 с.
2. Мошак Н.Н., Харитонов Г.Д. ОРГАНИЗАЦИЯ ТРАНСПОРТНЫХ ТУННЕЛЕЙ В ЯДРЕ СЕТИ LTE. Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 9 / СПОИСУ. – СПб., 2020. – 304 с. ISBN 978-5-907223-89-9, с. 268-270 http://spoisu.ru/news/165-ri-2020-finish.
3. 3GPP TS 23.203 version 15.4.0 Release 15 [Электронный ресурс] Режим доступа: https://www.etsi.org/deliver/etsi_ts/.
4. Diffserv to QCI Mapping-01 - IETF Tools [Электронный ресурс] Режим доступа: https://tools.ietf.org › draft-he.
5. Мошак Н.Н., Харитонов Г.Д. МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ QOS В СЕТИ LTE. Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября Р32 2020 г.: Материалы конференции. Часть 2. \ СПОИСУ. – СПб, 2020. – 335 с. ISBN 978-5-907223-86-8, с. 296-297. http://www.spoisu.ru/conf/ri2020/materials.

УДК 621.391

ПОНЯТИЙНЫЙ АППАРАТ ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ СИСТЕМЫ СВЯЗИ

Остроумов Олег Александрович, Лепешкин Олег Михайлович, 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, lepechkin1@yandex.ru, eentrop@yandex.ru

Аннотация. В докладе рассмотрена проблема обеспечения функциональной устойчивости системы связи и ее критической информационной инфраструктуры и критически важных объектов. Представлен понятийный аппарат функциональной устойчивости системы связи.

Ключевые слова: критическая информационная инфраструктура; критически важный объект; система связи; функциональная устойчивость.

CONCEPTUAL APPARATUS OF COMMUNICATION SYSTEM FUNCTIONAL STABILITY

Lepeshkin Oleg, Ostroumov Oleg, Sinyuk Alexander
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, lepechkin1@yandex.ru, eentrop@yandex.ru

Abstract. The report considers the problem of ensuring the communication system functional stability and its critical information infrastructure and critical facilities. The functional stability conceptual apparatus of the communication system is presented.

Keywords: critical information infrastructure, critical object, communication system, functional stability.

Введение: в современных условиях людям приходится сталкиваться с большими объемами информации, новыми и сложными системами, для которых при эксплуатации, предоставлении услуг дополнительных знаний не требуется, однако процессы обеспечения такой эксплуатации требуют углубленных технических знаний. В процессе функционирования сложных систем возникают ситуации нарушения их функционирования отдельных элементов системы, при этом может сохраняться функциональность всей системы. Некоторые элементы имеют важное критическое значение, нарушение функционирования таких элементов приводит к нарушению функционирования всей системы. Особенностью является то, что критичный объект для системы будет таковым не всегда, а в определенные моменты времени, определяемые целями и задачами системы в данный момент. Определение критичности отдельных элементов системы в масштабе времени близком к реальному имеет важное значение. Анализируя критичность должностные лица выявляют такие объекты, ее причины и принимают действия на уход от критичности или ее снижение, а также принимают меры для обеспечения безопасного и устойчивого функционирования таких объектов и системы в целом.

По взглядам руководства страны [1-3] одной из угроз национальной безопасности является нарушение безопасного и устойчивого функционирования объектов инфраструктуры государства, кроме подчеркиваются задачи и приоритеты развития и обеспечения информационной безопасности, которые направлены на обеспечение бесперебойного, устойчивого и безопасного функционирования критических объектов инфраструктуры государства, развития механизмов обнаружения и предупреждения угроз, а также ликвидация их проявлений.

Это обуславливает необходимость создания и обеспечения функционирования систем, обеспечивающих безопасность критичным объектам систем. Под безопасностью критической информационной инфраструктуры понимается состояние защищенности инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак. В [4, 5] определено создание субъектами критической информационной инфраструктуры (КИИ) системы безопасности объекта, обеспечивающей ее устойчивое функционирование. На государственном уровне создана система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, которая осуществляет координацию и взаимодействие с системами безопасности объектов КИИ субъектов. Основной угрозой безопасности КИИ рассматривается компьютерная атака (КА). При воздействии КА происходит нарушение (прекращение) функционирования объекта КИИ, либо нарушение (создание угрозы) безопасности обрабатываемой информации.

Требуется расширения перечня угроз, обуславливающих нарушение устойчивого функционирования объектов [6-10], а также расширения перечня объектов КИИ, исходя из не из особенностей обработки информации и угрозы - КА, а исходя из возможных последствий воздействия различных дестабилизирующих факторов на объекты, нарушение устойчивого функционирования которых приведет, в первую очередь, к нарушению (прекращению) управления объектов, системой, регионом, страной, а также может повлечь нарушение жизнедеятельности населения.

Для систем управления, включающих органы и средства управления, а также места их размещения. Критичным объектом можно рассматривать системы, обеспечивающие управление — автоматизированные системы управления и систему связи.

Под функциональной устойчивостью системы связи (СС) будем понимать часть общей устойчивости системы, характеризующая ее способность обеспечивать выполнение функций и задач системы связи с требуемым качеством и в установленные сроки в условиях воздействия различных дестабилизирующих факторов любой природы.

Под критичностью системы связи будет пониматься состояние системы связи, при котором нарушение (прекращение) ее устойчивого функционирования из-за воздействия на нее различных дестабилизирующих факторов любой природы приведет (может привести) к прекращению (нарушению) устойчивого функционирования системы управления или ее отдельных процессов, объектов, срыву управления, а также другим необратимым последствиям для обороноспособности государства, экономики, хозяйства и жизнедеятельности населения.

Критически важный объект (КВО) СС — объект СС, нарушение (прекращение) устойчивого функционирования которого из-за воздействия на него различных дестабилизирующих факторов любой природы приведет (может привести) к прекращению (нарушению) устойчивого функционирования системы связи или ее отдельных процессов, объектов, срыву управления, а также другим необратимым последствиям для обороноспособности государства, экономики, хозяйства и жизнедеятельности населения.

Вывод. Для обеспечения функциональной устойчивости СС необходима разработка понятийного, методологического, методического и математического аппарата для описания критичности системы связи и системы управления, методологии синтеза системы связи и ее объектов, а также системы мониторинга и контроля по принципу обеспечения устойчивого функционирования для обеспечения управления и предотвращения необратимых последствий для государства и жизнедеятельности населения. Нормативная база должна решить, в первую очередь, следующие вопросы: как и кто будет управлять этой системой? и на основании каких принципов будут осуществляться взаимодействие систем различных ведомств? Возникает необходимость разработки

понятийного, методологического, методического и математического аппарата для описания критичности системы управления.

СПИСОК ЛИТЕРАТУРЫ

1. Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации».
2. Указ Президента РФ от 25.12.2014 N Пр-2976 «Военная доктрина Российской Федерации».
3. Указ Президента РФ от 5.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
4. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
5. Лысов А.В. Обеспечение безопасности значимых объектов критической информационной инфраструктуры: Уч. пособие. СПб.: Медиапапир, 2019. 314
6. Лепешкин О.М., Остроумов О.А., Черных И.С. Система мониторинга и контроля функционального состояния критически важных объектов и объектов критической информационной инфраструктуры. В сборнике: в 3-х томах. 2016. с. 240-243
7. Нижегородцев А.В., Закалкин П.В., Стародубцев Ю.И., Кабанов А.С. Роль мониторинга в системе обнаружения, предупреждения и ликвидации последствий компьютерных атак. Промышленные АСУ и контролёры. 2013. № 7. С. 67-71.
8. *Лепешкин М.О., Лепешкин О.М., Сагдеев А.К.* Методологический подход оценки функциональной безопасности критической социотехнической информационной системы. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании Сборник научных статей: в 3-х томах. 2016. С. 294-299.
9. Burlov, V., Lepeshkin, O., Lepeshkin, M. Mathematical model for managing energy sector in the regionAdvances in Intelligent Systems and Computing, 2021, 1258 AISC, стр. 659–668.
10. Burlov, V., Lepeshkin, O., Lepeshkin, M. Algorithmic support for the dynamic functioning of transport systems in the region IOP Conference Series: Materials Science and Engineering, 2020, 918(1), 012224.

УДК 621.396.24: 621.371.38

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ МНОЖЕСТВЕННОГО ДОСТУПА В САМООРГАНИЗУЮЩЕЙСЯ СЕТИ ДЕКАМЕТРОВОЙ РАДИОСВЯЗИ В УСЛОВИЯХ СЛОЖНОЙ РАДИОЭЛЕКТРОННОЙ ОБСТАНОВКИ

Панин Роман Сергеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: zzz822@mail.ru

Аннотация. Показана актуальность использования каналов радиосвязи в телекоммуникационных системах для решения задачи защиты передаваемой информации от преднамеренных помех. Рассмотрен режим псевдослучайной перестройки рабочей частоты как мера защиты передаваемой в телекоммуникационных системах информации от преднамеренных помех.

Ключевые слова: автоматизированная радиосеть; множественный доступ; псевдослучайная перестройка рабочей частоты.

FEATURES OF PROVIDING MULTIPLE ACCESS IN A SELF-ORGANIZING DECAMETER RADIO COMMUNICATION NETWORK IN A COMPLEX ELECTRONIC ENVIRONMENT

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-mail: zzz822@mail.ru

Abstract. The article shows the relevance of the use of radio channels in telecommunications systems to address the problem of protecting transmitted information from jamming. The pseudo-mode tuning the operating frequency is considered as a measure of protection in telecommunication systems transmitted information from jamming.

Keywords: automated radio network; multiple access; pseudorandom tuning of the operating frequency.

Введение. Высокие требования, предъявляемые к современным системам декаметровой связи по помехоустойчивости и пропускной способности, вызывают необходимость поиска новых путей их совершенствования. Одним из направлений совершенствования систем декаметровой связи, функционирующих в условиях сложной радиоэлектронной обстановки, является создание самоорганизующихся сетей радиосвязи (ССР) [1, 2]. Это радиосети с децентрализованным управлением, не имеющие постоянной структуры. При наличии доступности, любые радиостанции могут соединяться в произвольном порядке. Частотный ресурс используется коллективно. Каждая абонентская радиостанция может быть ретранслятором, динамически определяя направления пересылки чужих данных. ССР не разделяются на подсети абонентского доступа и магистральные транспортные каналы между станциями доступа, что имеет место для большинства существующих в РФ сетей дальней радиосвязи. Как правило, данные сети строятся на технологии коммутации пакетов, и развертываются для обслуживания мобильных абонентов.

В перспективе данная сеть должна представлять собой совокупность взаимоувязанных между собой стационарных и полевых радиоцентров, расположенных на всей территории страны.

Реализация потенциальных возможностей самоорганизующейся пакетной радиосети предполагает решение целого ряда проблем. Основными из них следует считать:

– на физическом уровне – обоснование видов сигналов (АТ, ЧТ, ОФТ, ФТ, ППРЧ, т.п.); выбор методов передачи служебных команд (совмещенный, автономный, комбинированный); классификация факторов, определяющих топологию пакетной радиосети;

– на канальном уровне – выбор протоколов множественного доступа (МД) корреспондентов пакетной радиосети к общему частотно-временному ресурсу; определение оптимального баланса между способами исправления ошибок на основе адаптивного управления частотным и энергетическим ресурсами пакетной радиосети, видами сигналов, использования помехоустойчивого кодирования и адаптивных алгоритмов МД с учетом потоковой и помеховой обстановки, складывающейся в пакетной радиосети;

– на сетевом уровне – разработка алгоритмов определения связности между корреспондентами сети; обоснование методов маршрутизации пакетов, способов передачи служебных пакетов, необходимых для эффективного управления топологической структурой сети.

Для выполнения возложенных на радиосвязь задач по своевременной, достоверной и безопасной передаче формализованной информации целесообразно в рамках создания, построения и модернизации существующих сетей радиосвязи предусмотреть специальный режим, основанный на принципах пакетной передачи информации, адаптивной маршрутизации и множественного доступа к группе радиоканалов общего пользования. Это позволит в наибольшей степени реализовать такие положительные качества радиосвязи, как высокую оперативность доведения сообщений в разветвленных структурах, возможность реконфигурации сети в зависимости от состояния среды распространения радиоволн и конкретной помеховой обстановки. Перспективность применения пакетных радиосетей объясняется возможностью объединения достоинств систем радиосвязи, имеющих общую среду распространения радиоволн для всех пользователей, с преимуществами информационных сетей с коммутацией, базирующихся на разветвленной вычислительной инфраструктуре.

В работах [2-4], посвященных построению автоматизированных сетей радиосвязи, алгоритмы, реализующие основные функции управления АРЛ, имеют ограниченное применение, так как разработаны либо без учета моделей конфликтного взаимодействия противодействующих систем, либо предлагают наличие полной взаимной информированности о стратегии друг друга. Отмеченные обстоятельства вызывают необходимость использования для решения проблемы управления АРЛ в условиях сложной радиоэлектронной обстановки (РЭО) нового подхода к проектированию с позиций противоборства друг с другом антагонистических систем с противоположными целями в условиях различного рода неопределенностей относительно стратегии противодействующей системы.

В области радиосвязи данное направление особенно ярко выразилось в реализации широкомасштабных программ создания помехозащищенных систем и средств радиосвязи, в том числе использующих режим псевдослучайной перестройки рабочих частот (ППРЧ). По существу, реализуемый в системах радиосвязи режим ППРЧ представляет собой способ расширения спектра сигнала в пределах заданной полосы частот путем скачкообразного изменения номинала несущей частоты одновременно на всех радиостанциях системы радиосвязи по априорно известному абонентам псевдослучайному закону с неисчерпываемым за время его использования периодом [4]. При этом достигаемый эффект надежности связи определяется большим объемом используемых частот, из которого осуществляется случайный для стороннего наблюдателя выбор очередной рабочей частоты, и малым временем существования сигнала на этой частоте. Это значительно усложняет контроль (обнаружение и измерение параметров) сигналов систем связи с ППРЧ и возможность постановки преднамеренных помех. А повышение разведзащищенности и помехоустойчивости, в свою очередь, повышает надежность связи. Однако в систему связи с ППРЧ изначально заложен элемент «ненадежности». Это вызвано тем, что одновременно на одних частотах работает несколько независимых систем связи, что приводит к случайным совпадениям частот, т.е. к возникновению внутрисистемных помех, снижающих значение коэффициента готовности связи.

Острота данной проблемы снижается при использовании всеми станциями сети для установления соединения не одной частоты, а группы стартовых рабочих частот. После установления соединения по каналу обратной связи передаются служебные данные для автоматической замены непригодных стартовых рабочих частот на запасные рабочие частоты. Вероятность наличия для любого направления связи хотя бы одной пригодной рабочей частоты растет с увеличением числа стартовых частот. С другой стороны, увеличение этого числа выше потребностей радиосети, определяемых входной нагрузкой, приводит к нерациональному использованию частотного ресурса, вследствие простоя радиоканалов.

Выбор группы рабочих частот (ГРЧ) для установления и поддержания соединения в сети режима ППРЧ и алгоритм множественного доступа (АМД), определяющий порядок их использования радиостанцией, непосредственно связаны и взаимно зависимы. Для различных подсетей и направлений связи рабочие частоты и АМД могут различаться.

Так, например, в ближней и дальней зонах будут оптимальны ГРЧ различных поддиапазонов. Оптимальная вероятность захвата АМД канала доступа или «настойчивость протокола» будет зависеть от количества частотных каналов в группе [7], что требует совместной оптимизации выбора рабочих частот и параметров алгоритмов множественного доступа.

Выбор группы рабочих частот должен быть обусловлен состоянием ионосферы, взаимным положением корреспондирующих радиостанций, а также характеристиками их радиосредств. При данном выборе также должна быть учтена пригодность каждой рабочей частоты для установления соединения в различных направлениях радиосвязи и радиосетях, образуемых в соответствии со схемой организации связи.

В рассматриваемой технологии ППРЧ из комплекта частот для каждого направления передачи производится упорядоченная выборка пакета рабочих частот, в котором на первых местах находятся стартовые частоты, на них и происходит установление сеансов связи. Радиоданные сети определяют множество упорядоченных выборок частот, с указанием количества стартовых частот.

В отличие от радиосетей с простой ППРЧ, рассматривается адаптивная радиосеть, в которой алгоритм выбора из ГРЧ может основываться на информации о состоянии совокупности выделенных частот с позиции возможности их использования для эффективной передачи информации [6].

Рассматриваемый адаптивный алгоритм АСРС основывается на информации о последовательности наилучших для передачи сигналов номеров частот из состава ГРЧ, определенных матрицей вероятностей установления соединения в направлении передачи данных d на частоте f при скорости V: $P(d, f, V)$, которая может быть получена либо априорно из модели *IRI*-2016, зондированием рабочих частот, использованием методов зондирования ионосферы, на основе статистики прохождения радиоволн от спутников систем ГЛОНАС, *GSM*, Галилео и *BeeDo*, прослушиванием сигналов маркерных станций и станций точного времени, а также другими методами, либо апостериорно на основе статистики ошибок при прохождении информации на различных частотах как при воздействии случайных, так и преднамеренных помех [6].

В современных системах радиосвязи с ППРЧ в качестве оперативных мер защиты от радиоразведки и радиопротиводействия возможна полная или частичная смена ключевых данных, т.е. алгоритма формирования частотной последовательности и текущего заполнения генераторов ПСП. В перспективных радиостанциях возможна реализация оперативной смены любого правила формирования частотно-временной матрицы в любом их сочетании. Таким образом, режим псевдослучайной перестройки рабочей частоты является одним из наиболее эффективных методов повышения надежности в системах радиосвязи. Эффективность этого метода обусловлена сокращением времени существования сигнала на текущей рабочей частоте, что затрудняет обнаружение таких сигналов и, тем более, постановку эффективных преднамеренных помех. Однако существование целого ряда возможных способов создания помех и непрерывное совершенствование средств помех обусловливают необходимость обоснования параметров систем радиосвязи ППРЧ (время излучения сигнала на частоте, количество используемых частот, полоса частот) с целью поиска технических решений, оптимальных по показателю «производительность».

Существенным достоинством предлагаемого подхода к формированию оптимальной стратегии управления ЧВР является возможность реализации динамического управления в реальном масштабе времени с использованием принципа «ситуационного управления», что позволит существенно сократить временной цикл управления. Вместе с тем применение стратегии управления ЧВР радиолинии с ППРЧ, отличной от оптимальной, возможно для обеспечения разведзащищенности функционирования радиолинии с ППРЧ. Результаты сравнительного анализа эффективности функционирования радиолиний, использующих рассмотренный алгоритм управления ЧВР, и радиолиний, функционирующих без использования данного алгоритма, свидетельствуют о том, что применение предлагаемого алгоритма в условиях сложной РЭО обеспечивает повышение вероятности радиосвязи с достоверностью, не хуже заданной на рабочих частотах на 10...15% [6].

Заключение. Таким образом, при значительном превышении времени реакции в радиолинии с ППРЧ времени реакции КРП противоборствующей стороны значение критериального функционала определяется величиной показателя эффективности при завершении цикла управления КРП противоборствующей стороны. Поэтому необходимо добиваться уменьшения времени реакции в радиолинии с ППРЧ, повышения эффективности ее функционирования при применяемых стратегиях.

СПИСОК ЛИТЕРАТУРЫ

1. Путилин А.Н., Хвостунов Ю.С. Концепция телекоммуникационной технологии сети дальней радиосвязи // Материалы XI Санкт-Петербургской Международной конференции «Региональная информатика 2010», Санкт-Петербург, 20-22 октября 2010 г.
2. Шаров А.Н. Автоматизированные сети радиосвязи. – Л.: ВАС, 1988. – 178 с.
3. Путилин А.Н. Модель взаимодействия линии радиосвязи и станции радиоэлектронного подавления / Доклад на конф. «Региональная информатика 2012», 24-26 октября 2012 г. – СПб.: СПОИСУ, 2012.
4. Борисов В.И. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты / В.И. Борисов, В.М. Зинчук, А.Е. Лимарев, Н.П. Мухин, В.И. Шестопалов. – М. : РадиоСофт, 2008. – 512 с.
5. Управление ресурсом сетей ДКМ радиосвязи с использованием удаленных ретрансляторов / С.Д. Коровин // Материалы XII международной научно-технической конференции «Радиолокация, навигация, связь». – Воронеж, 2006. – С. 1057-1062
6. Обухов А.Н. Частотно-временные аспекты защиты информации в системах радиосвязи. – М.: Экслибрис-Пресс, 2008. – 212 с.
7. Панин Р.С., Путилин А.Н., Хвостунов Ю.С. Использование частотного ресурса системой декаметровой связи в режиме псевдослучайной перестройки рабочей частоты. Научно-технический журнал «Техника средств связи». 2020. № 3 (151). С. 2-13.
8. Бунин С.Г., Войтер А.П. Вычислительные сети с пакетной радиосвязью. Киев: Тэхника, 1989. - 129 с.

УДК 025.2.004; 621.311.23: 629.12

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СОВРЕМЕННЫХ ЭЛЕКТРОННЫХ БИБЛИОТЕК: ОСОБЕННОСТИ И СТАДИИ ИНТЕРВАЛЬНОГО АНАЛИЗА

Паращук Игорь Борисович, Крюкова Елена Сергеевна
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: shchuk@rambler.ru, e.kkrukovaa69@yandex.ru

Аннотация. Проведена оценка и рассмотрены особенности современных подходов к интервальному анализу информационной безопасности электронных библиотек. Приведены примеры параметров (показателей) информационной безопасности систем такого класса. Исследуются сущность и содержание стадий (этапов) интервального анализа информационной безопасности, заключающиеся в последовательном вычислении интервальных оценок информационной безопасности электронных библиотек на основе методов теории интервальных средних.

Ключевые слова: показатель; информационная безопасность; электронная библиотека; состояние; анализ; контроль; оценка; интервальные средние.

INFORMATION SECURITY OF MODERN ELECTRONIC LIBRARIES: FEATURES AND STAGES OF INTERVAL ANALYSIS

Parashchuk Igor, Kryukova Elena
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: shchuk@rambler.ru, e.kkrukovaa69@yandex.ru

Abstract. The features of modern approaches to interval analysis of information security of electronic libraries are evaluated and considered. Examples of parameters (indicators) of information security of systems of this class are given. The article examines the essence and content of the stages (stages) of interval analysis of information security, which consist in the sequential calculation of interval estimates of information security of electronic libraries based on the methods of the theory of interval averages.

Keywords: indicator; information security; electronic library; status; analysis; control; evaluation; interval averages.

Введение. Важным элементом сложных управляемых информационных систем, элементом, занимающим все более существенное место в Едином информационном пространстве России, являются современные электронные библиотеки (ЭБ) [1-3]. Традиционные подходы, составляющие основу методологии анализа состояния информационной безопасности (ИБ) таких ЭБ, анализа качества защиты информации в ЭБ и эффективности функционирования подсистем защиты информации в рамках ЭБ, обычно сложны и требуют больших вычислительных затрат [4]. При этом точечный, текущий анализ ИБ не всегда эффективен с точки зрения управления ИБ ЭБ на интервалах времени. Это обуславливает актуальность формулировки и решения задачи построения методики интервального анализа ИБ современных ЭБ, оценки защищенности ЭБ на любом (t+Δt)-ом временном интервале ее функционирования [5].

Показатели ИБ ЭБ могут быть сгруппированы в систему ПИБ (СПИБ), которая, содержит показатели в виде текущих отклонений параметров ИБ ЭБ от требований к ним. Так, текущий векторный ПИБ, который характеризует такие наиболее важные свойства системы защиты ЭБ, как доступность, целостность, конфиденциальность информации, хранимой, обрабатываемой и передаваемой в ЭБ, ресурсопотребление на реализацию процесса обеспечения безопасности информации в ЭБ и имеет вид:

$$\Delta\vec{Y}_{\text{ф}}(t+\Delta t)=[\Delta\bar{t}^{\,усл/\,угр}_{\text{дост}}(t+\Delta t);\ \Delta K_{\text{п дост}}(t+\Delta t);\ \Delta K_{\text{иск}}(t+\Delta t);\ \Delta K_{\text{конф инф}}(t+\Delta t);\ \Delta\vec{3}_{\text{ф}}(t+\Delta t)]^{\text{т}}, \quad (1)$$

где доступность характеризует $\Delta\bar{t}^{\,усл/\,угр}_{\text{дост}}(t+\Delta t)$ – отклонения времени доступа легальных (авторизированных) пользователей к защищаемому информационному ресурсу на (t+Δt)-ом интервале функционирования ЭБ; целостность (достоверность и неискаженность информации, несмотря на наличие угроз и уязвимостей) характеризуют $\Delta K_{\text{п дост}}(t+\Delta t)$ – отклонения коэффициента потери достоверности информации и $\Delta K_{\text{иск}}(t+\Delta t)$ – отклонения коэффициента искажений информации на (t+Δt)-ом интервале функционирования ЭБ; конфиденциальность (способность ЭБ сохранять информацию в тайне от субъектов, не имеющих полномочий на доступ к ней) характеризует $\Delta K_{\text{конф инф}}(t+\Delta t)$ – отклонения коэффициента конфиденциальности хранимой, обрабатываемой и передаваемой информации на (t+Δt)-ом интервале функционирования ЭБ. Помимо этого, выражение (1) содержит отклонения вектора затрат ресурсов $\Delta\vec{3}_{\text{ф}}(t+\Delta t)$ на построение подсистемы ИБ ЭБ и реализацию процесса функционирования этой подсистемы на (t+Δt)-ом интервале функционирования ЭБ.

Таким образом, предложенная СПИБ ЭБ, развитая на случай динамического интервального анализа информационной безопасности систем такого класса, обладая полнотой и безизбыточностью, вместе с тем, позволяет расширить диапазон исследуемых характеристик защищенности современных электронных библиотек. Предлагаемая совокупность методов оптимального анализа частных ПИБ ЭБ на определенном временном интервале, основанная на методах теории интервальных средних и методах теории фильтрации, позволяет, в отличие от общепринятых комплексных методов, значительно сократить размерность задачи анализа, предполагая наличие двухэтапной процедуры:

Первый этап – применение модели процесса смены состояний ПИБ ЭБ в виде непрерывных цепей Маркова в форме разностных стохастических уравнений, что позволяет свести размерность задачи к $K\times M\times\tau$, где τ – временные интервалы оценивания ПИБ ЭБ [6].

Второй этап – замена процедуры непосредственного K-кратного интегрирования совместной плотности распределения вероятностей размерности $K\times M\times\tau$ процедурами сбора данных наблюдения (или моделирования)

и вычисления оценочных значений нижнего и верхнего средних уровней ИБ (частных ПИБ) элементов ЭБ и ИБ ЭБ в целом на интервале времени (τ+$\Delta\tau$) с использованием методов теории интервальных средних.

При этом временной интервал оценивания (τ+$\Delta\tau$) включает конечное множество T непрерывных отсчетов наблюдения (моделирования): (τ+$\Delta\tau$)= {(t_1+Δt) + (t_2+Δt) +… +(t_T +Δt)}. Ключевыми стадиями интервального анализа частных показателей ИБ ЭБ являются:

Стадия сбора (с использованием математической, имитационной модели или на основе наблюдения в реальной ЭБ) статистических данных о значениях ПИБ ЭБ за период наблюдения или шаг моделирования (на (t+Δt)-ом временном отрезке функционирования ЭБ),

$$\Delta\vec{Y}_j(t+\Delta t) = f(\Delta y_1(t+\Delta t); \Delta y_2(t+\Delta t); \dots \Delta y_i(t+\Delta t); \dots \Delta y_N(t+\Delta t)), \quad (2)$$

где $\Delta y_1(t+\Delta t); \Delta y_2(t+\Delta t); \dots \Delta y_i(t+\Delta t); \dots \Delta y_N(t+\Delta t)$ – частные ПИБ ЭБ, рассмотренные нами в рамках выражения (1).

Стадия оптимальной по критерию минимального среднего квадрата ошибки (МСКО) фильтрации значений показателей ИБ электронных библиотек за период наблюдения или шаг моделирования (на (t+Δt)-ом временном отрезке функционирования ЭБ), которую можно представить в виде выражения

$$\Delta\hat{\vec{Y}}_j(t+\Delta t) = f(\Delta\hat{y}_1(t+\Delta t); \Delta\hat{y}_2(t+\Delta t); \dots \Delta\hat{y}_i(t+\Delta t); \dots \Delta\hat{y}_N(t+\Delta t)). \quad (3)$$

Стадия формирования интервального оценочного нижнего $\underline{\Delta\hat{y}_i}(\tau+\Delta\tau)$ и верхнего $\overline{\Delta\hat{y}_i}(\tau+\Delta\tau)$ средних уровней значений каждого из ПИБ ЭБ на интервале времени оценивания (τ+$\Delta\tau$) на основе оценочных значений этих ПИБ за все непрерывные отсчеты (периоды) наблюдения или шаги моделирования (t+Δt), составляющие в сумме содержание шага оценивания (τ+$\Delta\tau$).

Стадия определения интервальных оценок нижних $\underline{\Delta\hat{\vec{Y}}_i}(\tau+\Delta\tau)$ и верхних $\overline{\Delta\hat{\vec{Y}}_i}(\tau+\Delta\tau)$ значений обобщенного показателя (коэффициента) ИБ ЭБ с учетом результатов интервальных оценок (идентификации) ее частных показателей информационной безопасности [5, 7].

Особого внимания, на наш взгляд, заслуживает заключительная стадия – определение интервальных оценок обобщенного показателя (коэффициента) ИБ ЭБ с учетом результатов интервального анализа (идентификации) параметров ИБ системы:

$$\underline{\Delta\hat{\vec{Y}}}(\tau+\Delta\tau) = \prod_j^J \underline{\Delta\hat{\vec{Y}}_j}(\tau+\Delta\tau); \quad \overline{\Delta\hat{\vec{Y}}}(\tau+\Delta\tau) = \min_{j=1,\dots,J} \overline{\Delta\hat{\vec{Y}}_j}(\tau+\Delta\tau). \quad (4)$$

Заключение. Таким образом, в соответствии с предложенным методологическим подходом могут быть получены интервальные частные (нижняя и верхняя) оценки ИБ и обобщенная оценка ИБ ЭБ на основе методов теории интервальных средних. Полученные интервальные результаты анализа ИБ, оценочные значения параметров ИБ системы за интервал времени, позволят повысить достоверность оценивания защищенности ЭБ, что, в конечном итоге, сыграет свою важную роль в повышении качества управления информационной безопасностью, управления структурой, параметрами и режимами работы подсистем защиты информации для современных электронных библиотек.

СПИСОК ЛИТЕРАТУРЫ

1. Зуйкина К.Л., Соколова Д.В., Скалабан А.В. Электронные библиотеки в России. Текущий статус и перспективы развития. – М.: Ваш формат, 2017. 120 с.
2. Антопольский А.Б., Маркарова Т.С., Крюкова О.П., Харламов А.А. Электронные библиотеки в образовании / Под редакцией О.П. Крюковой, А.А. Харламова. – М.: 2009. 94 с.
3. Национальный стандарт Российской Федерации ГОСТ Р 7.0.96 - 2016. Электронные библиотеки. Основные виды. Структура. Технология формирования. – М.: Стандартинформ, 2016. 13 с.
4. Авраменко В.С., Тарасов А.В. Прогнозирование защищенности информации в автоматизированных системах специального назначения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сборник научных статей VIII Международной научно-технической и научно-практической конференции. Т. 4., – СПб.: ГУТ им. А.А. Бонч-Бруевича. 2019. С. 19-24.
5. Гуров С.В., Уткин Л.В. Надежность систем при неполной информации. – СПб.: Любавич, 1999. 160 с.
6. Крюкова Е.С. Модель функционирования электронной библиотеки для анализа ее качества и информационной безопасности // Вопросы оборонной техники. Научно-технический журнал. Технические средства противодействия терроризму. Серия 16. Выпуск № 9-10 (147-148), 2020. С. 16-22.
7. Крюкова Е.С., Малофеев В.А., Паращук И.Б. Анализ современных подходов к оценке качества систем хранения данных и электронных библиотек // Новые информационные технологии и системы: сборник научных статей XVI Международной научно-технической конференции (г. Пенза, 27–29 ноября 2019 г.). – Пенза: Изд-во ПГУ, 2019. С. 177-180.

УДК 004.056.5

ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ТЕЛЕКОММУНИКАЦИЙ ОТ СЕТЕВЫХ АТАК, АНАЛИЗ ИХ ВОЗМОЖНОСТЕЙ И СПЕЦИФИКА ПРИМЕНЕНИЯ

Паращук Игорь Борисович, Малофеев Валерий Александрович, Морозов Иван Васильевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: shchuk@rambler.ru, valeron12.1366@gmail.com, moroz_i.v@mail.ru

Аннотация. Рассматриваются вопросы анализа возможностей и особенностей применения современных программных средств защиты телекоммуникаций от сетевых атак. Проведена оценка потенциальных условий их наиболее эффективного применения с учетом достоинств и недостатков. Исследование проводилось с целью повышения обоснованности принятия решений при выборе систем обнаружения атак в интересах обеспечения защиты от вредоносных воздействий информации, которая хранится, обрабатывается и передается по каналам телекоммуникационной сети или системы.

Ключевые слова: сетевая атака; защита; обнаружение; программное средство; телекоммуникационная сеть; система; воздействие; блокирование; угроза; ресурс.

SOFTWARE TOOLS FOR PROTECTING TELECOMMUNICATIONS FROM NETWORK ATTACKS, ANALYSIS OF THEIR CAPABILITIES AND APPLICATION SPECIFICS

Parashchuk Igor, Malofeev Valery, Morozov Ivan
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: shchuk@rambler.ru, valeron12.1366@gmail.com, moroz_i.v@mail.ru

Abstract. The article deals with the analysis of the capabilities and features of modern software tools for protecting telecommunications from network attacks. An assessment of the potential conditions for their most effective use, taking into account the advantages and disadvantages, is carried out. The research was conducted in order to increase the validity of decision-making when choosing attack detection systems in the interests of ensuring protection from malicious influences of information that is stored, processed and transmitted through the channels of a telecommunications network or system.

Keywords: network attack; protection; detection; software; telecommunications network; system; impact; blocking; threat; resource.

Введение. Угрозы безопасности данных, циркулирующих в телекоммуникационных сетях и системах – потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, используемой сетью (системой), а также условиями обработки и хранения данных.

Одной из самых опасных угроз являются сетевые атаки – злоумышленные действия (мероприятия, процедуры), целью которого является захват контроля над удаленной локальной телекоммуникационной сетью или системой.

При этом принято различать сетевые атаки на телекоммуникационные сети: атаки типа mailbombing, переполнение буфера, атаки с использованием специализированных вредоносных программ (вирусов, снифферов, троянских коней, почтовых червей и т.д.), сетевая разведка, а также «фишинг»-атаки [1, 2].

При этом, в рамках комплексной защиты информации, циркулирующей в телекоммуникационные сети, от актуальных угроз, наиболее вредоносными принято считать сетевые атаки типа «захват» (системы, данных, управления, информации), типа «срыв» (нарушение, деградация, отрицание, уничтожение) и типа «манипуляция» (внешней информацией, датчиками и подмена системной информации) [3, 4].

Существует несколько ключевых направлений обеспечения безопасности телекоммуникаций от сетевых атак, причем базовым инструментом обнаружения сетевых атак являются программы и программные комплексы, способные выявлять (идентифицировать) и блокировать воздействия такого типа.

Причем обнаружение атак – динамический процесс определения и реагирования на любую подозрительную деятельность, направленную на сетевые или вычислительные ресурсы телекоммуникаций.

Проведем сравнительный анализ потенциала и обзор особенностей современных программных средств защиты телекоммуникаций от сетевых атак.

Рассмотрим популярные и зарегистрированные в реестре ФСТЭК России программные комплексы и системы обнаружения атак, такие как: система обнаружения атак «ФОРПОСТ»; система обнаружения вторжений Dallas Lock; система ViPNet HIDS; система Security Capsule SIEM; система Kaspersky Anti Targeted Attack и система обнаружения вторжений «Кречет».

Система обнаружения сетевых атак «ФОРПОСТ» предназначена для автоматического выявления воздействий на контролируемую телекоммуникационную сеть, которые могут быть классифицированы как сетевые атаки или вторжения, а также для блокировки развития выявленных сетевых атак.

Достоинствами этой системы является ее способность обнаруживать и предотвращать развитие сетевых атак, нацеленных на серверы телематических служб (FTP, Web, электронная почта, СУБД пр.) и рабочие станции, размещенные в контролируемых сегментах телекоммуникационной сети или системы [5].

Система обнаружения вторжений Dallas Lock предназначена для противодействия сетевым атакам различной степени сложности путем реализации ряда функций: сигнатурный и эвристический анализ попыток нарушения защиты; обнаружение вторжений по результатам анализа служебной информации протоколов сетевого уровня; определение аномалий в действиях пользователя сети; динамические настройки реагирования на попытки нарушений, а также дискреционный и мандатный контроль доступа к объектам и устройствам телекоммуникационной сети [6].

Программно-аппаратный комплекс ViPNet HIDS предназначен для обнаружения вторжений в телекоммуникационные сети или системы. Это реализуется на основе динамического анализа сетевого трафика стека протоколов TCP/IP. При этом анализ осуществляется для протоколов всех семи уровней модели взаимодействия открытых систем. Важным достоинством таких систем является их способность собирать данные и выявлять признаки вторжений непосредственно на серверах (хостах) защищаемой телекоммуникационной сети [7].

Система Security Capsule SIEM предназначена для мониторинга и управления событиями безопасности телекоммуникационных сетей и позволяет контролировать состояние информационной безопасности, управлять информацией об угрозах, оценивать эффективность применяемых средств защиты, а также полноту и корректность настроек средств и механизмов защиты. Помимо этого, система способна восстанавливать работоспособность после сбоев и отказов [8].

Система Kaspersky Anti Targeted Attack позволяет обнаруживать многоступенчатые сетевые атаки и блокировать их за счет уникальной платформы противодействия комплексным угрозам на уровне сети. Обладает средствами наглядной визуализации, опирается на прозрачность инфраструктуры телекоммуникационных сетей или систем. Эта система позволяет автоматизировать процессы сбора и хранения информации и «цифровых улик». Система способна готовить данные для оперативного расследования и реагирования, автоматизировать задачи расследования инцидентов и, как следствие, позволяет оптимально расходовать ресурсы служб безопасности телекоммуникаций [9].

Система обнаружения вторжений «Кречет» – программный инструмент, реализующий в телекоммуникационной сети или системе функции автоматизированного обнаружения и блокирования действий, нацеленных на несанкционированный доступ к данным, негативных воздействий на информацию в целях ее добычи, модификации (изменения) и блокирования доступа к ней.

Данное программное средство встраивается в существующую сетевую инфраструктуру и анализирует копию сетевого трафика, проходящего через пограничное устройство телекоммуникационной сети [10].

Заключение. Таким образом, проведен сравнительный анализ современных программных средств защиты телекоммуникаций от сетевых атак. Полученные в ходе исследования данные могут дать реальную возможность осуществить оценивание потенциальной эффективности применения тех или иных средств обнаружения вредоносных воздействий с учетом достоинств и недостатков рассмотренных программных средств.

Помимо этого, результаты анализа, по мнению авторов, позволят повысить обоснованность принятия решений при выборе систем обнаружения атак в интересах обеспечения защиты данных в телекоммуникационной сети или системе.

СПИСОК ЛИТЕРАТУРЫ

1. Бокова О.И. Оптимальное управление безопасностью территориальных сегментов информационно-телекоммуникационных систем: монография / О.И. Бокова. – Воронеж: Воронежский институт МВД России, 2006. 153 с.
2. Miller D., Harris S., Harper A., VanDyke S. Security Information and Event Management Implementation. – London: McGraw-Hill. 2010. 464 p.
3. Паращук И.Б., Чернявский А.В., Шестаков Е.О. Эффективность комплексной защиты информации в системах хранения данных и электронных библиотеках: модели и методы оценивания. // Информационная безопасность регионов России (ИБРР-2019) XI-я Санкт-Петербургская Межрегиональная конференция, Материалы конференции, – СПб.: СПОИСУ, 2019. С. 248-250.
4. Авраменко В.С., Бобрешов-Шишов Д.И., Беденков В.Н., Маликов А.В. Определение актуальных угроз безопасности информации в инфокоммуникационных системах на основе аппарата нечеткой логики // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2017). VI Международная конференция. Т.3. – СПб.: СПБГУТ, 2017. С.13-18.
5. Система обнаружения атак «Форпост» версия 3.0. [Электронный ресурс] // Акционерное общество «Российские наукоемкие технологии» (АО «РНТ»). URL: https://www.rnt.ru/ru/production/detail.php?ID=689 (дата обращения 27.04.2021).
6. Обнаружение и предотвращение вторжений. [Электронный ресурс] // ООО «Конфидент». URL: https://dallaslock.ru/resheniya/obnaruzhenie-i-predotvraschenie-vtorzhenii/ (дата обращения 26.04.2021).
7. ViPNet IDS. [Электронный ресурс] // Компания «ИнфоТеКС». URL: https://infotecs.ru/product/setevye-komponenty/vipnet-ids/ (дата обращения 26.04.2021).
8. Система мониторинга и корреляции событий информационной безопасности Security Capsule SIEM. [Электронный ресурс] // Инновационные технологии в бизнесе. URL: https://www.itb.spb.ru/products/Security_Capsule_SIEM/ (дата обращения 27.04.2021).
9. Kaspersky Anti Targeted Attack. Комплексная защита от сложных угроз и целевых атак. [Электронный ресурс] // ОАО «Лаборатория Касперского». URL: https://www.kaspersky.ru/enterprise-security/anti-targeted-attack-platform (дата обращения 27.04.2021).
10. Система обнаружения вторжений «Кречет». [Электронный ресурс] // НПП «Гамма». URL: https://nppgamma.ru/catalog/setevaya_bezopasnost/krechet/ (дата обращения 27.04.2021).

УДК 004.7

ОЦЕНКА СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК РАЗЛИЧНЫХ ТИПОВ ФРЕЙМОВ IEEE 802.11 ДЛЯ СЕРВИСОВ МЕСТОПОЛОЖЕНИЯ

Петров Владислав Андреевич[1], Ковцур Максим Михайлович[1], Кистуга Антон Юрьевич[2], Штеренберг Станислав Игоревич[1]

[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия

[2] ООО "Фаст Лайн"
Профессора Попова ул., 37В, Санкт-Петербург, 197136, Россия

e-mails: vladpetrovvv@gmail.com, maxkovzur@mail.ru, anton.kistruga@gmail.com, vladimir.i.andrianov@gmail.com

Аннотация. В докладе исследуется методы позиционирования в беспроводных сетях стандарта IEEE 802.11. Рассмотрены механизмы получения пакетов путем перехвата и последующего исследования сетевого

трафика с дальнейшей обработкой средствами анализатора Wireshark. На основе результатов исследования делается вывод о пригодности каждого типа фреймов для использований в качестве источника данных для позиционирования.

Ключевые слова: беспроводные сети; IEEE 802.11; Wireshark; RSSI; Wi-Fi; типы фреймов IEEE 802.11, позиционирование.

ASSESSMENT OF THE STATISTICAL CHARACTERISTICS OF VARIOUS TYPES OF IEEE 802.11 FRAMES FOR LOCATION SERVICES

Petrov Vladislav[1], Kovtsur Maxim[1], Kistruga Anton[2], Andrianov Vladimir[1]
[1] The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
[2] LLC "Fast Lane"
37B Professor Popov St, St. Petersburg, 197136, Russia
e-mails: vladpetrovvv@gmail.com, maxkovzur@mail.ru, anton.kistruga@gmail.com, vladimir.i.andrianov@gmail.com

Abstract. The report examines the methods of positioning in wireless networks of the IEEE 802.11 standard. The mechanisms of receiving packets by intercepting and then studying network traffic with further processing by means of the Wireshark analyzer are considered. Based on the results of the study, a conclusion is made about the suitability of each type of frame for use as a source of data for positioning.

Keywords: wireless networks; IEEE 802.11; Wireshark; RSSI; Wi-Fi; IEEE 802.11 frame types; positioning.

В беспроводных сетях стандарта IEEE 802.11, для передачи, контроля и управления пользовательскими данными применяются 3 группы фреймов: management, control, data. Информация, содержащаяся в этих фреймах, позволяет устройствам точно взаимодействовать друг с другом в автоматическом режиме, решая проблему мониторинга, отладки основных показателей, загруженности сети и т.д.

Для устройств, работающих в этом стандарте, при перехвате трафика, информация о передаче добавляется после обработки на сетевой карте в заголовок фрейма на принимающей стороне. Примером дополнительной информации, которая записывается при создании дампа трафика, служит параметр RSSI (англ. Received Signal Strength Indicator) — полная мощность сигнала на принимающей стороне. Специализированное программное обеспечение, например Wireshark, способно собирать и обрабатывать передаваемый трафик, а также представлять в удобном для человека виде - в графиках и таблицах. Зная мощность передатчика и уровень принимаемого сигнала, а также наличие и характер преград на пути распространения радиосигнала, на основе опытных экспериментов можно рассчитать потери радиосигнала на распространение в пространстве, которые являются функцией расстояния между этими устройствами.

В работе рассмотрены существующие группы фреймов – data, control, management, сравнительно представлена их структура, особенности, характер появления, а также сделан вывод о достоинствах и недостатках касаемо применения в позиционировании. Представлены статистические характеристики фреймов, а также исследована возможность применения данных типов фреймов для определения местоположения.

СПИСОК ЛИТЕРАТУРЫ

1. Красов А.В., Гельфанд А.М., Коржик В.И., Котенко И.В., Петрив Р.Б., Сахаров Д.В., Ушаков И.А., Шариков П.И., Юркин Д.В.Построение доверенной вычислительной среды // Санкт-Петербург, 2019.
2. Ковцур М. М., Симанов М. С. Анализ особенностей организации авторизации пользователей в сетях коллективного доступа стандарта IEEE 802.11. Актуальные проблемы инфотелекоммуникаций в науке и образовании. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2019. Т. 4. С. 537–541.
3. Александрова Е.С., Иванов Г.Н., Ковцур М.М. Анализ механизмов защиты Wi-Fi сетей.Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). // С 47-51.
4. Ковалев Д., Ковцур М. Механизмы аутентификации и управления ключами стандарта IEEE 802.11-2012 // Первая миля. 2014. № 3 (42). // С. 72-77.
5. Петров В.А., Ковцур М.М., Кистуруга А.Ю. Исследование методов дальнометрии в беспроводных сетях. // REDS: Телекоммуникационные устройства и системы, 2021. т. 11, №4. // С. 42-49.

УДК 621.391

АЛГОРИТМ РАБОТЫ ПОМЕХОЗАЩИЩЁННОЙ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ

Ротенбергер Александр Андреевич, Сазонов Виктор Викторович
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: a.rotenberger@mail.ru

Аннотация. Предложен алгоритм работы помехозащищённой системы передачи данных с кодовым разделением каналов на основе использования ансамблей дискретных ортогональных сигналов с заданными характеристиками. Значения характеристик ансамблей и их количество определяется на каждом из этапов работы системы передачи данных.

Ключевые слова: помехоустойчивость и скрытность системы передачи данных, кодовое разделение каналов, корреляционные характеристики ортогональных сигналов, функция Уолша, аутентификация, синхронизация, передача данных.

ALGORITHM OF OPERATION OF AN INTERFERENCE PROTECTED DATA TRANSMISSION SYSTEM WITH CODE SEPARATION OF CHANNELS

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

Abstract. An algorithm for the operation of a noise-immune data transmission system with code division of channels based on the use of ensembles of discrete orthogonal signals with given characteristics is proposed. The values of the characteristics of the ensembles and their number are determined at each stage of the operation of the data transmission system.

Keywords: noise immunity and secrecy of the data transmission system; code division of channels; correlation characteristics of orthogonal signals; Walsh function; authentication; synchronization; data transmission.

Введение. Развитие информационной инфраструктуры нашей страны, увеличивает значение систем передачи данных (СПД) по каналам связи. Особое место занимают СПД с дискретными ортогональными сигналами, например, сотовые системы подвижной радиосвязи стандарта CDMA. В них реализована технология многостанционного доступа с кодовым разделением каналов. Данная технология легла в основу большей части стандартов, разрабатываемых для глобальных систем подвижной связи. В связи с чем, в настоящее время к СПД с кодовым разделением каналов (КРК) предъявляются повышенные требования по помехозащищённости.

Помехозащищённость передачи данных по радиоканалам СПД КРК может быть достигнута путем обеспечения энергетической скрытности сигналов - переносчиков данных, структурной скрытности этих сигналов и информационной скрытности самого сообщения. При этом лишь направление повышения структурной скрытности, где основополагающую роль играет количество структур ансамблей дискретных ортогональных сигналов (АДОС), наименее проработано в существующих СПД КРК.

Оценка помехозащищенности существующих СПД КРК в рамках повышения структурной скрытности показывает:

Во-первых, для формирования АДОС используются линейные псевдослучайные последовательности (М-последовательности и коды Голда), которые не обеспечивают структурной скрытности шумоподобного сигнала из-за его предсказуемости.

Во-вторых, для формирования АДОС используется всегда лишь одна структура, причем известная (функция Уолша).

В-третьих, корреляционные свойства используемых АДОС не удовлетворяют условию малости боковых пиков функций корреляции сигналов в ансамбле.

Таким образом, в практике обнаруживается противоречие, заключающееся в том, что для использования большого количества структур АДОС для помехозащищённой СПД КРК необходимо значительное увеличение её аппаратной сложности, поскольку единый принцип формирования структур АДОС не используются.

Оценку подходов формирования АДОС удобно вести, разделив на три основные направления [1, 2]:

Первое направление базируется на анализе свойств сигналов, для описания которых используется широкий класс известных в математике ортогональных полиномов Якоби, Гегенбауэра, Чебышева, Лагерра, Эрмита, дискретных ортогональных функций Уолша, Хаара, Радемахера, Виленкина-Крестенсона, Трофимова - Ласунского. Среди работ этого направления следует выделить публикации Л.Е. Варакина, А.Г. Леонтьева, М.К. Размахнина, В.П. Яковлева, Х. Хармута.

Второе направление связано с построением производных сигналов на базе перемножения специально подобранных производящих последовательностей на известные ортогональные функции и достаточно полно представлено работами Л.Е. Варакина,Н.Г. Дядюнова, Д. Стиффлера.

Третье направление связано с векторным синтезом АДОС по совокупности требований к ним. Среди работ этого направления известны работы В.С. Попенко, А.П. Жука,З.В. Черняка и других.

Анализ работ первого направления показывает, что оно ограничено и остается только на уровне рассматриваемых систем сигналов, а работы второго направления ограничиваются синтезом АДОС всего лишь по одной характеристике и не могут быть использованы для решения задачи синтеза систем сигналов по совокупности предъявляемых требований и ограничений. Третье направление имеет математические ограничения по размерности синтезируемых АДОС [3, 4].

На основании вышеизложенного видно, что для разработки алгоритма работы помехозащищённой СПД КРК, необходимо использовать третье направления с ограничениями накладываемых каналом связи.

Работа алгоритма состоит из пяти этапов: установление соединения и аутентификации; установление синхронизации; синтез АДОС; принятие и использование АДОС для передачи данных; разрыв соединения.

Этап установления соединения и аутентификации включает в себя:

1. Станция на передающей стороне подает адресный (циркулярный) вызов, на который отвечает станция на приемной стороне.

2. Для выполнения условий безопасности связи станцией на передающей стороне производится запрос на аутентификацию станции на приемной стороне. Безопасность связи достигается: соблюдением правил ее эксплуатации; предварительным шифрованием данных, использованием таблиц позывных; ограничением круга лиц, допускаемых к ведению переговоров по разрешенным к применению открытым каналам связи; проверки подлинности полученных данных путем обратной передачи принятых данных; выполнением требований режима секретности при обработке и хранении информации в автоматизированных системах управлений.

В нашем случае предлагается ввести сигнальную конструкцию, включающую в себя двоичную кодовую последовательность длительностью от 32 до 64 бит, которая заранее известна доверенным станциям. Заблаговременное введение базы подобных последовательностей в станции приемной и передающих сторон имеет ряд преимуществ:

- множество конструкций последовательностей данной длительности;
- псевдослучайный выбор последовательности на аутентификацию при организации передачи данных
- возможно ввести соответствие разных последовательностей на запрос и ответ;
- высокая степень подтверждения об установлении канала связи с нужным абонентом.

Этап установление синхронизации является основным средством поддержания всего цифрового оборудования в сети передачи данных на одной средней скорости. Все системы, установленные в сети передачи данных, должны быть засинхронизированы от одного или нескольких ведущих генераторов. Основным требованием к синхронизации является значительно большая помехоустойчивость выделения синхросигналов по сравнению с информационными символами.Этого можно достичь за счет:

- синхросигналов с накоплением или использованием широкополосных сигналов с хорошими корреляционными свойствами;
- включения в синхросигнал тактовых синхроимпульсов и группы сигналов цикловой синхронизации (выполнение условия повышение помехоустойчивости);
- сознательного увеличения времени передачи синхроимпульса в полтора раза, чем длительность времени запаздывания сигнала в точке приема.

Основным преимуществом применения данных условий синхронизации будет являться то, что нет необходимости прецизионной синхронизации, достигаемой в результате использования сигналов времени от GPS (Global Positioning System). Работа разработанного алгоритма не предполагает поддержание связи постоянно или периодически, а осуществляют работу по заказу должностных лиц, что является выполнением требований по скрытности.

Этап синтеза АДОС выполняется на основе получаемых данных от сигналов, приходящих от станции на передающей стороне. Станция приемной стороны определяет лучший АДОС по помехозащищенности для осуществления передачи данных не только в условиях быстроменяющейся оперативной обстановки, но и в условиях нестабильности среды передачи данных по каналу радиосвязи. Изменяя требования к их характеристикам и структуре в целом (от сеанса к сеансу изменяя структуру используемого АДОС) при передаче данных решается задача по повышению помехозащищённости СПД с КРК.

Этап разрыва соединения осуществляется по инициативе передающей стороны, которая в передаваемые данные включает соответствующую квитанцию, при её получении приемная сторона понимает, что обмен данными завершён. При необходимости повторной передачи данных алгоритм отрабатывается заново.

Заключение. Разработанный алгоритм работы помехозащищённой системы передачи данных с кодовым разделением каналов, может найти своё применение при проектировании стандартов для систем подвижной связи.

СПИСОК ЛИТЕРАТУРЫ

1. Жук А.П., Сазонов В.В. Повышение помехозащищённости систем связи с ортогональными сигналами // Известия ЮФУ. Технические науки. №4 (48). 2005.-С. 163-166.
2. Пашинцев В.П., Малофей О.П., Жук А.П. и др. Развитие теории синтеза и методов формирования ансамблей дискретных сигналов для перспективных систем радиосвязи различных диапазонов радиоволн. - М.: Физматлит. - 2010. – 264 с.
3. Сазонов В.В., Беззубов О.В. Вариант синтеза ансамблей дискретных ортогональных сигналов с требуемыми параметрами скрытности. Труды XVII Всероссийской научно-практической конференции РАРАН. 2014. С. 114-117
4. Сазонов В.В., Жук А.П., Жук Е.П. «Инфокоммуникационные технологии» Том 16, № 1, 2018, с. 33-39

УДК 004.056

АКТУАЛЬНОСТЬ СИТУАЦИОННОГО УПРАВЛЕНИЯ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Синяков Евгений Анатольевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: doc.margo-85@mail.ru

Аннотация. Проникновение современных информационных технологий практически во все сферы деятельности Вооруженных Сил Российской Федерации заставляет все более тщательно подходить к построению системы защиты информации.

Ключевые слова: автоматизированная система; защита информации; система защиты информации; ситуационное управление.

RELEVANCE OF SITUATIONAL MANAGEMENT OF INFORMATION SECURITY SYSTEM IN SPECIAL PURPOSE AUTOMATED SYSTEMS

Sinyakov Evgeny
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: doc.margo-85@mail.ru

Abstract. The penetration of modern information technologies into almost all spheres of activity of the Armed Forces of the Russian Federation makes it necessary to take a more and more careful approach to building an information security system.

Keywords: automated system; information security; information security system; situation management.

Введение. Современные высокотехнологичные комплексы невозможно представить без использования передовых средств и систем управления, систем связи для передачи команд и сигналов по управлению. Осуществляется активное внедрение роботизированных технологий (беспилотные летательные аппараты, танки, инженерные машины и т.д.) [1].

В целях недопущения воздействия внешних и внутренних угроз на находящуюся на автоматизированные системы и передаваемую, обрабатываемую и хранящуюся в них информацию, для каждой системы создается система защиты информации, которая обеспечивает гарантированную защиту информации, находящейся в ней.

Система защиты информации создается применительно к каждой автоматизированной системе индивидуально в связи их предназначением, характером передаваемой информации, ее важности и сроками актуальности.

В связи с постоянно вновь появляющимися средствами и способами воздействия на защищаемую информацию, постоянно совершенствуется организационно-штатная структура подразделений по защите информации, средства и способы ее защиты.

Актуальность предлагаемого способа управления системой защиты информации обусловлена следующими факторами [2, 3]:

1. Постоянное совершенствование методов и способов воздействия на защищаемую информацию в автоматизированных системах.

2. Необходимость постоянного анализа существующей системы защиты информации на предмет ее соответствия современным вызовам и способности противостоять временным и перспективным угрозам, способности ее трансформации.

3. Современный уровень проникновения информационных технологий во все сферы деятельности человечества, а также внутренних "демократично настроенных" элементов из числа граждан России воздействовать на происходящие в стране процессы, позволяют сделать выводы о желании и наличии возможностей воздействия на существующую систему управления.

4. Динамичность изменения обстановки в аспекте защиты информации от несанкционированного доступа требует перехода от интуитивных способов защиты информации к системным.

Заключение. Исходя из вышеизложенного можно сделать вывод, что существующее дискретное управление системой защиты информации от несанкционированного доступа не может гарантированно защитить информацию.

Для гарантированного функционирования системы защиты информации от несанкционированного доступа в автоматизированных системах необходимо:

– постоянный мониторинг происходящих воздействий на систему защиты информации от несанкционированного доступа;

– обнаружение угроз;

– анализ обнаруженных угроз;

– ситуационная настройка системы защиты информации от несанкционированного доступа (выдача рекомендаций администратору безопасности).

СПИСОК ЛИТЕРАТУРЫ

1. Горбылев А. Л. Программный комплекс для автоматизированной генерации организационно-распорядительных документов по защите информации в критических инфраструктурах. Информационные и математические технологии в науке и управлении. Том 3. 2016. стр. 185-191.
2. Бондарь И. В. Методика построения модели угроз безопасности информации для автоматизированных систем. Вестник Сибирского государственного аэрокосмического университета имени академика М. Ф.Решетнева. 2012, стр. 7 -10.
3. Кубарев А. В. Подход к формализации уязвимостей информационных систем на основе их классификационных признаков. Вопросы кибербезопасности №2 2013.

УДК 004.942

МОДЕЛЬ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ОПТИМАЛЬНОГО ВЫБОРА ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ СИГНАТУРНОГО МЕТОДА ИДЕНТИФИКАЦИИ

Солодухин Борис Владимирович, Пантюхин Олег Игоревич, Рябов Геннадий Анатольевич, Фот Роман Сергеевич

Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: p_oleg99@mail.ru, soloduxin@yandex.ru

Аннотация. В статье приводятся предложения по построению модели для решения задачи оптимального выбора программных средств защиты информации на основе сигнатурного метода идентификации программных средств защиты информации в системе защиты, приводящего к уменьшению времени распознавания образов при защите информации в автоматизированных системах управления специального назначения.

Ключевые слова: программные средства защиты информации; системы защиты информации.

MODEL FOR SOLVING THE PROBLEM OF OPTIMUM SELECTION OF SOFTWARE INFORMATION PROTECTION BASED ON SIGNATURE IDENTIFICATION METHOD

Solodukhin Boris, Pantyukhin Oleg, Ryabov Gennady, Fot 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: p_oleg99@mail.ru, soloduxin@yandex.ru

Abstract. The article presents proposals for constructing a model for solving the problem of optimal choice of information security software based on the signature method of identifying information security software in a security system, leading to a decrease in the time of pattern recognition when protecting information in special-purpose automated control systems.

Keywords: information security software; information security systems.

Информационная безопасность автоматизированных систем управления специального назначения (АСУ СН), в которых циркулирует критически важная информация, является неотъемлемой частью национальной безопасности Российской Федерации. Анализ современных военных конфликтов показывает, что в настоящее время противоборствующие стороны всё чаще применяют информационные технологии для различного рода атак на АСУ СН. Значимость эффективной программной системы защиты информации (ПСЗИ) АСУ СН от несанкционированного доступа (НСД) возрастает с каждым днём. ПСЗИ АСУ СН представляет собой совокупность программных средств защиты информации (ПСрЗИ), для выбора которых существует множество подходов. Все подходы к выбору ПСрЗИ для ПСЗИ учитывают требования нормативно-методической базы органов Российской Федерации, например, [1-3], которые детализируют и определяют взаимосвязи требований и функций безопасности.

В докладе приводится общий вид целевой функции при оценке показателей эффективности ПСЗИ АСУ СН, устремлённой в максимум. При этом положительное влияние оказывают: достоверность поступивших сведений каждого ПСрЗИ АСУ СН на *i*-ю оценку требованиям нормативно-методической базы (i=1,…,*N*); *N* – число исследуемых ПСЗИ каждого объекта АСУ СН; эффективность ПСЗИ АСУ СН. Отрицательное влияние оказывают: вероятность ошибки при оценке ПСрЗИ АСУ СН на *i*-ю оценку требованиям нормативно-методической базы; время работы ПСЗИ АСУ СН, представленное как совокупность времени каждого этапа отражения угрозы информационной безопасности и времени работы АСУ СН с учетом затрат времени работы ПсрЗИ; затраты ПСЗИ объекта, представленные как совокупность затрат на закупку ПсрЗИ, настройку ПСрЗИ и т. д.

Таким образом, критерий оценки показателей эффективности ПСЗИ АСУ СН, выражается в минимизации вероятности ошибки при оценке ПСрЗИ АСУ СН согласно выполнению требований нормативно-методической базы, в максимизации поступивших достоверности сведений каждой системы защиты информации исследуемого объекта АСУ СН и эффективности защиты.

Математическая модель оценки эффективности выполнения требований нормативно-методической базы может быть представлена как задача распознавания образов. Требуется определить степени соответствия каждого ПСрЗИ на место выдвигаемым требованиям к ПСЗИ АСУ СН при заданных ограничениях (например, класс межсетевого экрана, класс средства антивирусной защиты и т.д.). Подробно решение данной задачи представлена в [4].

Применение принципа ассоциативности в модели позволяет при вводе в систему анализа любой характеристики исследуемой ПСЗИ АСУ СН, например, показатель класса криптографического средства защиты информации, антивирусного средства и т.д., выбирать из базы программ параллельно все виды нормативно-методических документов, соответствующие (ассоциирующие) значению введенной характеристики образа исследуемой системы защиты информации объекта.

Данная модель позволяет проводить параллельно проверку соответствия каждого ПСрЗИ объекта по всем имеющимся требованиям разных документов нормативно-методической базы.

Принятие решения о соответствии ПСрЗИ объекта требованиям нормативно-методического документа принимается по мажоритарному правилу, или по правилу большинства, что повышает достоверность принятия решения.

В процессе оценки ПСЗИ формируется ранжированный ряд соответствий образа ПСЗИ АСУ СН по всем нормативно-методическим документам регуляторов РФ [5-6].

Сигнатурный метод как метод сжатия информации при проверке соответствия эталонам получил широкое распространение, и представляет собой метод исследования реакций на подачу определенных последовательностей.

Анализ последовательностей очень трудоёмок, вследствие чего необходимо определить количество таких потоков, при расположении значений, которых, дальнейшее распознавание образа можно остановить.

Предложенная модель распознавания образов в системе отбора ПСрЗИ – динамическая, т.е. имеет множество состояний в процессе отбора. При ее исследовании был проведен ряд экспериментов [4, 5].

Применяя сигнатурный метод распознавания образов ПСрЗИ, значительно сокращается время анализа зарегистрированных значений образов ПСЗИ, тем самым, повышая производительность системы отбора ПСрЗИ в ПСЗИ.

СПИСОК ЛИТЕРАТУРЫ

1. Информационное сообщение. Об утверждении Требований к средствам доверенной загрузки от 6 февраля 2014 г. № 240/24/405 [Электронный документ] - https://fstec.ru/component/ attachments/download/663 - Дата обращения: 01.06.2021.
2. Информационное сообщение об утверждении требований безопасности информации к операционным системам от 18 октября 2016 г. N 240/24/4893 [Электронный документ] - https://fstec.ru/normotvorcheskaya/ informatsionnye-i-analiticheskie-materialy/1206-informatsionnoe-soobshchenie-fstek-rossii-ot-18-oktyabrya -2016-g-n-240-24-4893 - Дата обращения: 01.06.2021.
3. Фот Ю.Д., Аралбаев Т.З. Модель отбора персонала на основе принципов ассоциативности и мажоритарности принятия решения // Интеллект Инновации Инвестиции. Академический журнал №1, Оренбург – 219 с. 2011.
4. Солодухин Б.В., Фот Р.С. Сигнатурный метод оптимизации модели распознавания образов программных средств защиты информации. Труды ВАС. НТС №111. СПб: ВАС, 2020. – с.41-52.
5. Солодухин Б.В., Редченко И.В., Фот Р.С. Разработка подхода к выбору показателей эффективности программных систем защиты информации и к их оценке. Труды ВАС. НТС №112. СПб: ВАС, 2020. – с.84-94.
6. Тарасов, В. Н. Сигнатурный метод оптимизации модели идентификации в системе отбора персонала / Тарасов В. Н., Фот Ю. Д. // Инфокоммуникационные технологии, - № 4 (10), 2012. - с. 79-83.

УДК 004.056.5

АНАЛИЗ СОВРЕМЕННЫХ СРЕДСТВ МУЛЬТИФАКТОРНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫМИ СЕТЯМИ

Сундуков Вячеслав Алексеевич, Паращук Игорь Борисович, Селезнев Андрей Васильевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: slava.sundukov.2014@mail.ru, shchuk@rambler.ru, andrsel@mail.ru

Аннотация. Рассмотрены современные подходы к мультифакторной аутентификации пользователей автоматизированных систем управления телекоммуникационными сетями. Эти подходы разнообразны и основаны на использовании в комплексе различных средств, механизмов и процедур проверки подлинности субъекта доступа. Результаты решения задачи эффективного комплексного применения различных средств мультифакторной аутентификации пользователей позволят повысить защищенность ресурсов автоматизированных систем управления и безопасность данных абонентов телекоммуникационных сетей.

Ключевые слова: телекоммуникационная сеть; автоматизированная система управления; мультифакторная аутентификация; пользователь; защищенность; идентификатор.

ANALYSIS OF MODERN MEANS OF MULTI-FACTOR AUTHENTICATION OF USERS OF AUTOMATED TELECOMMUNICATIONS NETWORK MANAGEMENT SYSTEMS

Sundukov Vyacheslav, 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: slava.sundukov.2014@mail.ru, shchuk@rambler.ru, andrsel@mail.ru

Abstract. Modern approaches to multi-factor authentication of users of automated control systems of telecommunications networks are considered. These approaches are diverse and are based on the use of various tools, mechanisms and procedures for verifying the authenticity of the access subject in a complex. The results of solving the problem of effective complex application of various means of multi-factor authentication of users will increase the security of resources of automated control systems and the security of data of subscribers of telecommunications networks.

Keywords: telecommunications network; automated control system; multi-factor authentication; user; security; identifier.

Введение. Современные телекоммуникационные сети (ТКС) являются сложными управляемыми объектами информационно-телекоммуникационной инфраструктуры. Управление объектами такого класса традиционно осуществляется на основе помощи специальных автоматизированных систем. При этом автоматизированные системы управления (АСУ) ТКС позволяют обеспечить эффективность функционирования ТКС с минимальными затратами, позволяют обеспечить качество управления сложными объектами такого класса. Иными словами, АСУ ТКС на современном этапе их развития являются не только гарантом достижения целей создания, развития и функционирования сети, но и ключевым элементом информационно-телекоммуникационной инфраструктуры любой системы, включая систему безопасности государства [1, 2].

Одним из ключевых требований, предъявляемых к АСУ ТКС, является требование по защищенности информации, циркулирующей в системах такого класса [3-5]. При этом важным аспектом защищенности принято считать предотвращение несанкционированного доступа (НСД) пользователей к информации [3].

Это связано с тем, что неуклонно растет количество проникновений в корпоративные сети с использованием чужих данных для аутентификации (более 30% всех инцидентов безопасности), анализ вирусов, социальной инженерии, фишинга и других векторов атак указывает на то, что сами по себе пароли недостаточны для адекватной защиты. Более того, с введением карантина и массовым переходом на удаленную работу число попыток внешних атак увеличилось в среднем на 20%. Причем неважно, что защищаем: удаленный доступ, данные клиентов или самой организации. Именно поэтому при формулировке состава и функционала средств и комплексов предотвращения НСД все больше внимания в современных условиях уделяется вопросам многофакторной аутентификации (МФА) АСУ ТКС [6-10]. Под аутентификацией понимается процедура проверки подлинности субъекта доступа – пользователя АСУ ТКС, позволяющая достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует. Пользователь АСУ ТКС должен подтвердить факт обладания некоторой информацией, которая может быть доступна только ему одному [6].

Другими словами, система защиты от НСД в АСУ ТКС должна требовать от пользователей идентифицировать себя при запросах на доступ. Система защиты от НСД в АСУ ТКС должна подвергать проверке подлинность идентификации – осуществлять аутентификацию. Для этого она должна обладать необходимыми данными для идентификации и аутентификации. Более того, система защиты должна препятствовать доступу к защищаемым ресурсам АСУ ТКС неидентифицированных пользователей и пользователей, идентификация которых не подтвердилась, она должна надежно и однозначно связывать идентификатор со всеми действиями пользователя АСУ ТКС [3, 6]

Под МФА принято понимать особый метод контроля доступа пользователя к ресурсам АСУ ТКС и рабочему месту. Это, так называемая, расширенная аутентификация должностного лица АСУ, при которой пользователю для получения доступа к информации необходимо предъявить более одного «доказательства» своей подлинности и своих прав [6, 8]. Иными словами, необходимы два и более механизма аутентификации конкретного пользователя, применяемые в комплексе.

При этом механизмами аутентификации могут быть пароль или PIN-код (категория «знание», которым обладает субъект доступа – пользователь АСУ ТКС); электронная или магнитная карта (смарт-карта), токен или флеш-память – USB-ключ (категория «владение», т.е., вещь, которой обладает субъект доступа – пользователь АСУ ТКС); отпечатки пальцев, радужная оболочка глаз, капиллярные узоры, последовательность ДНК (категория «свойство», которым обладает субъект доступа – пользователь АСУ ТКС с точки зрения, например, биометрии) [9].

Построение АСУ ТКС с функцией МФА предопределяет наличие у пользователя такой системы клиентского программного обеспечения, которое может быть разнообразным и многофункциональным. Например, примером средств МФА могут служить отдельно устанавливаемые на рабочие места пользователей АСУ ТКС специализированные пакеты прикладных программ (ППП). Они позволяют входить в сеть управления ТКС, осуществлять идентификацию данных Web-доступа и VPN-подключения [10].

Чтобы использовать с этими ППП МФА электронные или магнитные карты (смарт-карты), токены или флеш-память (USB-ключ), необходимо, чтобы на рабочих местах должностных лиц АСУ ТКС были установлены несколько (иногда, четыре-пять) пакетов специального программного обеспечения. Чаще всего это пакеты специального программного обеспечения для контроля версии или пакеты для проверки конфликтов с иными приложениями, используемыми в рамках АСУ ТКС [9].

Существуют иные формы и способы реализации МФА. При этом имеется много факторов и особенностей (аспектов) отдельных процессов, которые необходимо учитывать при выборе, разработке, тестировании, внедрении и поддержке целостной системы управления идентификацией безопасности в АСУ МФА, включая все релевантные механизмы аутентификации и сопутствующих технологий:

Заключение. Таким образом, задача исследования состоит в реализации способности различных средств МФА пользователей АСУ ТКС к эффективному взаимодействию с учетом того факта, что многофакторные решения требуют инженерных расчетов, оценки рисков, а также дополнительных затрат на установку и оплату эксплуатационных расходов.

Тем не менее, проблема МФА актуальна, поскольку реализация угроз безопасности АСУ ТКС в современных условиях становится лишь вопросом времени. Если игнорировать риски, заранее не принять мер защиты подключений пользователей АСУ ТКС к ресурсам системы, это может привести не только к финансовым

потерям, ущербу репутации, но и к краже интеллектуальной собственности, государственной или коммерческой тайны.

СПИСОК ЛИТЕРАТУРЫ

1. Ермолаева В.В., Калашников Д.А. Автоматизированные системы управления // Молодой ученый. №11. 2016. С. 166-168.
2. Башкирцев А.С., Митрофанов Е.А., Паращук И.Б. Автоматизированные системы управления телекоммуникационными сетями: обзор и анализ современных требований // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020 г.: Материалы конференции. Часть 1. \ СПОИСУ. – СПб.: 2020. С. 63-65.
3. Приказ ФСТЭК России от 14 марта 2014 года №31. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. (с изменениями на 9 августа 2018 года). – М.: ФСТЭК. 2014. – 28 с.
4. Паращук И.Б., Малофеев В.А., Пронин А.А., Башкирцев А.С. Обзор базовых требований по кибербезопасности в автоматизированных системах управления критических информационных инфраструктур // Перспективные направления развития отечественных информационных технологий. Материалы круглых столов VI межрегиональной научно-практической конференции. – Севастополь: 2020. С. 56-57.
5. Михайличенко Н.В. Проблемы и перспективы обеспечения безопасности центров обработки данных // Региональная информатика и информационная безопасность. – СПб.: СПОИСУ. 2017. С. 137-138.
6. Национальный стандарт РФ ГОСТР 58833-2020. Защита информации. Идентификация и аутентификация. Общие положения. – М.: Стандартинформ. 2020. – 32 с.
7. Авраменко В.С., Маликов А.В. Подход к аутентификации пользователей инфокоммуникационных систем с применением машинного обучения // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). Сборник научных статей IX Международной научно-технической и научно-методической конференции. В 4-х т. – СПб.: ГУТ им. Бонч-Бруевича. 2020. С. 13-17.
8. Скородумов А.В. Многофакторная аутентификация – лучше меньше, да лучше // Information Security / Информационная безопасность. №6, 2015. С 52-54.
9. Юрьев Д.Р., Рогова О.С. Сравнительный анализ двухфакторной аутентификации // Технические науки – от теории к практике. №6 (66), 2017. С. 46-51.
10. Карманов А.Г., Галимов Т.А. Средства многофакторной аутентификации в современной инфраструктуре безопасности информационных систем // Info Security. №1, 2012. С. 94-97.

УДК 004.45

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ТРЕБОВАНИЙ ПО ДОСТОВЕРНОСТИ ДАННЫХ ПРИ ПРИМЕНЕНИИ БЕСПРОВОДНЫХ КАНАЛОВ И ЛИНИЙ СВЯЗИ С ВЫСОКИМ УРОВНЕМ ПРЕДНАМЕРЕННЫХ ПОМЕХ

Титов Владимир Степанович, Апарина Елена Юрьевна Панин Роман Сергеевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: titov856@yandex.ru

Аннотация. В статье рассмотрены особенности обеспечения требований по достоверности данных при применении беспроводных каналов и линий связи с высоким уровнем преднамеренных помех.

Ключевые слова: достоверность данных; беспроводные каналы и линии связи; преднамеренные помехи.

DESIGN AND SIMULATION OF SPECIAL-PURPOSE DATA CENTERS

Titov Vladimir, Aparina Elena, 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-mail: titov856@yandex.ru

Abstract. The article considers the features of ensuring the requirements for data reliability when using wireless channels and communication lines with a high level of interference.

Keywords: data availability; wireless channels and communication lines; intentional interference.

В беспроводных каналах и линиях связи для передачи информации различного вида используются электромагнитные волны различных диапазонов частот. Условное разделение на диапазоны частот и их применение приведены в [1].

Самым низким считается диапазон сверхдлинных волн (СДВ)на крайне низких частотах (КНЧ) менее 30 кГц. Далее следуют ультранизкие (УНЧ), очень низкие (ОНЧ), низкие (НЧ), средние (СЧ), высокие (ВЧ), очень высокие (ОВЧ), ультравысокие (УВЧ), сверхвысокие (СВЧ), крайне высокие (КВЧ) частоты до 300 гГц.

Следует отметить возможность использования радиоканалов и линий связи в метровом, дециметровом, сантиметровом, миллиметровом диапазонах на частотах от 20 мГц и выше. В настоящее время более всего загружены радиодиапазоны L (390-1550 мГц), S (1550-5200 мГц), C (5,85 - 8,20 гГц) и диапазон $К_у$ 12,4-18,0 гГц).

Беспроводные средства сетей связи с подвижными объектами являются составной частью стационарных и полевых пунктов управления. Они обеспечивают предоставление инфокоммуникационных услуг должностным лицам органов военного руководства, других силовых структур и государственной властей при нахождении их в специально оборудованных транспортных средствах, а также при пешем перемещении в мирное и военное время,

в особых условиях, при чрезвычайных ситуациях, в ходе локальных конфликтов в районах при отсутствии других родов связи, а также для резервирования или наращивания емкости сетей стационарной и полевой системы связи.

Применение сети связи с подвижными объектами повышает эффективность управления подразделениями при нахождении их вне пунктов управления, а также в движении [2].

Беспроводные средства и сети в целом, по сравнению с проводными, имеют ряд преимуществ. К ним относятся повышенная мобильность, живучесть, а также незначительные ограничения по доступности оконечных и сетевых средств, которые в основном определяют степень их боевой готовности.

К недостаткам, несколько ограничивающим применение беспроводных каналов и линий связи, можно отнести их низкую помехоустойчивость, так как реализованные протоколы обработки, передачи и приема не учитывают особенностей функционирования в условиях повышенного уровня помех и, тем более, при воздействии преднамеренных помех.

При исследовании проблемы помехозащищенности каналов и линий беспроводного доступа необходим учет современного уровня и основных направлений развития и модернизации средств и способов радио подавления (РЭП). Комплексы РЭП могут быть стационарными, полевыми, а также забрасываемыми малогабаритными. Учитывая относительно большое удаление средств РЭП от радиосредств и диапазон рабочих частот современных систем беспроводного доступа (единицы – десятки ГГц), можно сделать вывод о том, что наибольшая опасность для систем беспроводного доступа, развернутых на ПУ, вероятнее всего, будет исходить от забрасываемых передатчиков помех (ЗПП).

Современный парк средств РЭП в основном рассчитан на подавление линий радиосвязи КВ, УКВ и нижней части СВЧ диапазона. Однако в США и других странах ведутся активные разработки перспективных комплексов РЭП на более высокие рабочие частоты. Основными достоинствами нового комплекса будут высокая эффективность вскрытия радиоэлектронной обстановки, оптимальное подавление линий радиосвязи целенаправленными маломощными помехами без задействования традиционных средств РЭП, возможность использования в режиме противодействия средствам радио и радиотехнической разведке противника.

При решении задач вскрытия и отслеживания изменений в радиоэлектронной обстановке комплекс будет обеспечивать: перехват сигналов типовых средств радиосвязи в диапазоне от 20 мГц до 15000 мГц и радиолокации в диапазоне от 100 мГц до 15000 мГц) с вероятностью, близкой к 100%; классификацию и идентификацию сигналов всех известных радиоэлектронных средств при скорости программной перестройки рабочей частоты 1400 и более скачков в секунду; определение менее чем за 2 с местонахождения радиостанций и радиолокационных станций с круговой вероятной ошибкой не более 10 м при условии установки средств на удалении 3 – 5 км от источников радиоизлучения.

С учетом многообразия различных типов средств беспроводной связи в качестве примера рассмотрим вариант модификации протокола обеспечения достоверности в средствах, реализующих широкополосную сеть на базе стандарта 802.16e на уровне дискретного канала и канала передачи данных.

Одним из путей решения данной проблемы может быть модификация протокола обратной связи обеспечение гибридной обратной связи. Исходными данными являются результаты оценки параметров достоверности на уровне дискретного канала по вероятности ошибочного приема единичных элементов, которая, в основном, зависит от вида модуляции полезного сигнала, вида помехи и соотношения «сигнал/шум»

Для описания дискретного канала могут быть использованы различные модели: двоичный симметричный канал без памяти, варианты канала с памятью на основе простой марковской цепи, модель Гилберта, модель Беннета-Фройлиха, модель Пуртова, Захарова, Замрия.

Данная модель является наиболее простой и широко используется. Для двоичного симметричного канала без памяти вероятность появления ошибок в пакете длины n можно определить по формуле Бернулли [65].

Особенностью использования высокочастотного диапазона является многолучевое распространение радиоволн, которое ведет к группированию ошибок в дискретном канале.

Модель ДСК БП этого не учитывает и необходимо использовать другие модели. В качестве наиболее простой, но достаточно точной, рассмотрим модель канала Пуртова – Замрия – Захарова.

Группирование ошибок приводит к увеличению числа кодовых комбинаций, пораженных ошибками большей кратности, но уменьшается число не пораженных кодовых комбинаций. Эффективность обратной связи на уровне канала передачи данных определяется следующими положениями:

1. Возможна передача пакетов различной длины с одинаковыми служебными полями.

2. Ориентация на использование в асинхронных каналах связи. Именно такие каналы имеют место при подключении оконечного оборудования данных к модему CDE по стыку Ethernet.

3. Более высокая достоверность передачи данных по сравнению с системами помехоустойчивого кодирования. Корректирующая способность любого помехоустойчивого кода в режиме обнаружения ошибок больше, чем в режиме исправления.

4. Способностью адаптации к изменениям характеристик канала. При увеличении коэффициента ошибки снижается скорость передачи информации по каналу и наоборот.

5. Более высокая скорость передачи информации по сравнению с системами помехоустойчивого кодирования в каналах с высоким группированием ошибок, имеющих место в рассматриваемой системе (группирование ошибок вызывает наличие частотно-селективных замираний). Это обусловлено тем, что избыточность (переспросы) используется не постоянно, как в системах помехоустойчивого кодирования, а только при возникновении ошибок. Большее группирование требует меньшего числа переспросов.

Существует три основные способа обработки ответов на положительные и отрицательные подтверждения: стартстопный (передача с остановкой и ожиданием) с блочным методом передачи; с возвращением на *N* кадров (потоковый метод передачи; метод выборочного (селективного) повтора.

Наиболее перспективными, на сегодняшний день, являются системы, которые используют гибридную обратную связь (ГОС). Данные системы занимают промежуточное положение между системами с переспросом и системами с исправлением ошибок, комбинируя лучшее этих двух подходов.

Сущность ГОС заключается в следующем: передаваемая информационная последовательность разбивается на кадры длиной *k* элементов; каждый информационный кадр защищается корректирующим кодом с обнаруживающей способностью; Информационный кадр вместе с заголовком и проверочными разрядами кода, обнаруживающего ошибки, образуют блок; блок, в свою очередь, защищается кодом, исправляющим ошибки с определенной исправляющей способностью. В результате данной операции получается дополнительная группа проверочных разрядов, которая является корректирующей группой. В общем случае к информационному кадру может быть добавлен заголовок.

Первоначально передается пакет. Если на приеме в нем обнаружена ошибка, то запрашивается передача корректирующей группы. После исправления ошибок информационный кадр повторно проверяется на наличие ошибок. При отсутствии ошибок кадр выдается получателю. В другом случае пакет повторяется.

Результаты оценки позволяют сделать вывод, что в системах с ГОС время доставки пакета будет меньше. Это достигается тем, что при перезапросе будет передаваться меньшее число бит. Что касается эффективности такой системы, то в дискретных каналах высокого качества (с низкой вероятностью ошибки на бит) доставка пакета происходит, как правило, на первом или втором переспросе. Вследствие этого ГОС нет заметного выигрыша по времени доставки. Однако в каналах низкого качества (радиоканалах) системы повышения достоверности с гибридной обратной связью обеспечат сокращение времени передачи пакетов до 30%.

СПИСОК ЛИТЕРАТУРЫ

1. Олифер В, Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное изд. - СПб.: Питер, 2020. - 1008 с.
2. Пикалов Е.Д., Иванов Ю.Н., Паращук И.Б. Классификация и сравнительный анализ беспроводных технологий для построения радиосетей специальной связи. 2010. –14 с. Деп. в ЦВНИ МО РФ № 2 (107), 16.03.2010, №А30516.
3. Компьютерные сети: Нисходящий подход \ Джеймс Куроуз, Кит Росс.–6-изд.–Москва: изд. «Э», 2016. – 912с.

УДК 004.054

ПОВЫШЕНИЕ КАЧЕСТВА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Федоров Андрей Евгеньевич, Гурьев Сергей Николаевич
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mails: fedorofff4312@mail.ru, sguryev@mail.ru

Аннотация. Статья посвящена вопросу повышения качества программного обеспечения автоматизированных систем управления. Определены основные проблемные вопросы и представлены направления повышения качества программного обеспечения современных автоматизированных систем управления.

Ключевые слова: автоматизированная система управления; программное обеспечение; качество программного обеспечения; требования к качеству программного обеспечения; реализация требований качества программного обеспечения.

IMPROVING THE QUALITY OF SOFTWARE FOR AUTOMATED CONTROL SYSTEMS

Fedorov Andrey, Guryev Sergey
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mails: fedorofff4312@mail.ru, sguryev@mail.ru

Abstract. The article is devoted to the issue of improving the quality of software for automated control systems. The main problematic issues are identified and the directions of improving the quality of software for modern automated control systems are presented.

Keywords: automated control system; software; software quality; software quality requirements; implementation of software quality requirements.

Введение. Значительный рост конкуренции на отечественном рынке производственных предприятий обусловлен экономической ситуацией и высокими требованиями заказчиков. Для того, чтобы удерживать свои позиции на рынке и производить продукцию высокого качества современное предприятие должно особое внимание уделять автоматизации технологических процессов. Автоматизация технологических процессов предполагает внедрение автоматизированной системы управления (АСУ), которая реализует функцию управления технологическим процессом, оперативное управление производством и сокращение цикла управления в деятельности предприятия. Составной частью АСУ предприятия является программное обеспечение.

Автоматизированная система управления представляет собой комплекс аппаратных и программных средств, предназначенный для управления различными процессами в рамках технологического процесса, производства, предприятия.

Компонентами АСУ являются программно-аппаратные комплексы, включающие в себя общее, общесистемное и специальное программное обеспечение, систему управления базами данных и базы данных.

Программное обеспечение включает в себя совокупность программ на машинных носителях и программных документов, используемых для их отладки, проверки работоспособности и функционирования. Состав программного обеспечения определяется тремя главными факторами [1, 2]:

- совокупностью решаемых задач;
- характером циркулирующей информации;
- составом комплекса технических средств.

В настоящее время в организациях и компаниях ведется целенаправленная работа по созданию и внедрению систем и комплексов средств автоматизированного управления. При этом эффективность их использования во многом определяется уровнем профессиональной подготовки кадров, наличием у пользователей знаний, умений и навыков в применении современных программных и аппаратных средств.

Актуальность вопроса повышения качества определяется тем, что [3]:

- программное обеспечение, используемое в некоторых АСУ, разработано более 10 лет назад и не отвечает современным требованиям;
- в случаях изменения принципов управления и его организационно-штатной структуры приходится в ручном режиме проводить большое количество настроек, уточнять адресную книгу комплексов средств автоматизации, что требует привлечения представителей промышленности и дополнительных издержек;
- отсутствует возможность использовать полученные результаты ранее проведенных расчетов в качестве входных данных для последующих расчётов для дальнейшего применения;
- частично организован учет входящих и исходящих документов, оповещение должностных лиц об их получении, а также защищенный удаленный доступ к документам, находящимся в автоматизированной системе управления;
- отсутствует внедрение в программное обеспечение возможности формирования шаблонов документов;
- отсутствует возможность трехмерной визуализации пространства, что не позволяет проводить демонстрацию объекта (интерьер, жилой комплекс и т.д.) на всех стадиях жизненного цикла.

Качество программного обеспечения определяется способностью программного продукта при заданных условиях удовлетворять установленным или предназначенным потребностям. Для удовлетворения потребностей пользователей необходимо обеспечить выполнение следующих требований [4]:

- функциональной пригодности;
- уровня производительности;
- совместимости;
- удобству использования и сопровождения;
- надежности;
- безопасности;
- мобильности;
- эффективности;
- удовлетворенности.

Для повышения качества ПО требуется усовершенствованное ПО. Для обеспечения требуемого качества программного обеспечения необходимо спланировать и осуществить комплекс мероприятий, выполняемых для удовлетворения потребностей пользователей, а именно:

- обеспечить автоматизированную конфигурацию и реконфигурацию АСУ при изменении структуры системы управления;
- сформировать единое пространство результатов решения информационно-расчетных и кризисных задач;
- реализовать функцию автоматизированного документооборота между органами управления;
- обеспечить коллективную разработку текстовых и графических документов;
- предоставить возможность трехмерной визуализации пространства;
- обеспечить выполнение других функциональных возможностей в части автоматизации процессов, связанных с системой защиты информации, контроля и управления функционированием автоматизированной системы.

Заключение. Таким образом, повышение качества программного обеспечения в значительной мере позволит реализовать выполняемые АСУ функции, определит направление технического прогресса организации, обеспечит внедрение инноваций, а также экономию всех видов ресурсов организации.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р ИСО/МЭК 25051-2017 «Требования и оценка качества систем и программного обеспечения (SQuaRE)»
2. ГОСТ 24.103-84 «Автоматизированные системы управления. Основные положения»
3. Гурьев С.Н. Повышение качества программного обеспечения комплексов средств автоматизации. Материалы VI межрегиональной научно-практической конференции, Науч.ред. Соколов. Севастополь, 2020 г. с.170-171
4. Паращук И.Б., Михайличенко Н.В. Особенности построения и анализа качества дата-центров как базовых элементов IT-инфраструктуры // Перспективные направления развития отечественных информационных технологий: материалы IV Межрегиональной научно-практической конференции. – Севастополь: Севастопольский государственный университет, 2018. – 352 с., С. 28-29

УДК 004.451.87

ОСНОВНЫЕ МЕТОДЫ ЗАЩИТЫ СИСТЕМЫ ОТ LKM ROOTKIT

Фёдорова Ольга Вячеславовна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mail: olagfedorova666@gmail.com

Аннотация. В ходе выполнения выпускной квалификационной работы были разработаны методы обнаружения LKM RootKit в системе Linux, благодаря чему можно вовремя заметить нахождение вредоносного ПО.

Ключевые слова: ядро Linux; Модуль ядра системы Linux; RootKit; права суперпользователя; системные вызовы; аппаратные прерывания; механизм защиты; виртуальный лабораторный стенд.

THE MAIN METHODS OF PROTECTING THE SYSTEM FROM LKM ROOTKIT

Fedorova Olga
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: olagfedorova666@gmail.com

Abstract. During the completion of the final qualification work, methods for detecting LKM RootKit in the Linux system were developed, thanks to which it is possible to notice the presence of malware in time.

Keywords: linux kernel; Linux kernel module; RootKit; superuser rights; system calls; hardware interrupts; protection mechanism; virtual laboratory stand.

Существуют следующие способы сокрытия руткита в ядре:
- Перехват системных вызовов и функций.
- Маскировка файлов и их содержимого.
- Маскировка процессов.
- Маскировка сетевых соединений и модификация трафика.

На их основе и будут строиться методы их обнаружения. Основная идея заключается в поиске аномалий в системе. Единственным способом поиска является анализ памяти ядра. Чтобы спрятать файлы и папки, руткиты проверяют листинг директории на заданные заранее имена и при совпадении убирают их. При этом они не всегда перехватывают обращения к скрытым папкам, и, зная эти имена, можно туда зайти и оперировать файлами в них.

Второй и третий руткиты работают с таблицей системных вызовов. Информацию о местонахождении кода системных функций и вызовов ядро берет из двух таблиц: символьной таблицы ядра System.map (откуда при загрузке экспортируемые функции ядра отображаются в псевдофайл /proc/kallsyms) и таблицы syscall'ов sys_call_table, адрес которой есть в System.map. Когда найден адрес нужной функции, руткит заменяет его адресом своей функции. Таблица системных вызовов находится в защищенной области памяти, помеченной только для чтения в регистре CR0 (x86), но это ограничение — легко исправимо для руткита уровня ядра, ведь есть функция write_cr0(), с помощью которой оно легко обходится. Так же возможна замена адреса самой таблицы, но в рассмотренных руткитах не использовалась. Таким образом отследив изменение в регистре CR0, можно судить о наличии руткита в системе.

Есть еще возможный вариант обнаружения руткита в ядре поиск в памяти ядра дескриптор модуля, отвязанного от списка загруженных модулей. Найдя его, можно вернуть его в список, чтобы затем использовать команду rmmod (если, конечно, руткит не подменил и ее). Существует решение, позволяющее обнаружить в памяти объекты, похожие на дескрипторы LKM, но оно работает на уже очень старых и только 32-битных ядрах. Перебор же памяти современных систем затруднен из-за огромного адресного пространства. Проверка памяти ядра на предмет наличия объектов, похожих на дескрипторы модулей ядра, - довольно сложная задача, интересное решение, для которого описано в журнале Phrack и реализована как антируткит LKM module_hunter.o. Метод brute force (грубой силы) может использоваться для перебора содержимого памяти ядра. Память, выделенная модулю, должна быть выровнена по размеру страницы памяти ядра, которая составляет 4 КБ и уменьшает количество попыток перебора. Чтобы избежать ошибок «сбой страницы памяти» во время полного перебора, необходимо обращаться только к отображаемым страницам, информацию о которых можно получить из таблиц соответствия адресов виртуальных и физических.

Чтобы эффективно противодействовать LKM-руткитам, антируткит должен работать тоже в режиме ядра, в нулевом кольце защиты. Необходимо написать модуль ядра Linux, который бы обнаруживал присутствие описанных в главе 2 руткитов по их характерным признакам (хотя в некоторых случаях может быть достаточно доступа к памяти ядра через устройство /· dev/kmem из программы пространства пользователя, но это не всегда надёжно).

Разрабатываемый антируткит должен обнаруживать исключённые из списка module_list структуры-описатели модулей, как наиболее часто используемый LKM-руткитами механизм маскировки. Ещё обнаружить присутствие руткита поможет выявление факта перехвата некоторых существенных для пользовательских

программ функций (функции VFS для основных операций с файлами, системные вызовы для работы с сетью), поэтому данный функционал тоже важен.

СПИСОК ЛИТЕРАТУРЫ

1. Долгих Д. Учимся писать модуль ядра (Netfilter) или Прозрачный прокси для HTTPS: [Электронный ресурс] URL: https://habr.com/ru/post/138328/
2. Кирилова К.С., Цветков А.Ю. Анализ существующих методов реализации rootkit [Текст] В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференция: в 4 т.. 2019. С. 492-497.
3. Кирилова К.С., Цветков А.Ю., Волкогонов В.Н. Проблема обезвреживания руткитов уровня ядра в системах специального назначения [Текст] I-methods. 2020. Т. 12. № 3. С. 1-9.
4. Матвейчиков И.В. Простая маскировка модуля ядра Linux с применением DKOM [Электронный ресурс] URL: https://habr.com/ru/post/205274/
5. Фёдорова О.В., Цветков А.Ю. // Инновации. Наука. Образование. 2021. №31. С. 118-124.
6. Цилюрик О. Практикум: модули ядра Linux. Конспект с примерами и упражнения с задачами: [Электронный ресурс], URL: https://losst.ru/wp-content/uploads/2016/08/BOOK_PRACTIS_245.pdf
7. Щербакова Т. Фишинговые письма — самый распространенный способ взлома почты: [Электронный ресурс] URL: https://www.kaspersky.ru/blog/email-account-stealing/23433/
8. Alavoor Vasudevan The Linux Kernel HOWTO: [Электронный ресурс] URL: http://www.faqs.org/docs/Linux-HOWTO/Kernel-HOWTO.html
   Andreas Bunten UNIX and Linux based Rootkits. Techniques and Countermeasures: [Электронный ресурс] // DFN-CERT Services GmbH, 2004. URL: http://repository.root-me.org/Virologie/EN%20-20UNIX%20and%20Linux%20based%20Rootkits%20Techniques%20and%20Countermeasures%20-%20Andreas%20Bunten.pdf
9. Кирилова, К.С. Анализ существующих методов реализации rootkit / К.С. Кирилова, А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 492-497.
10. Таргонская, А.И. Разработка защищенного веб-интерфейса для управления устройствами в сети / А.И. Таргонская, А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно- методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 734-739.
11. Темченко, В.И. Проектирование модели информационной безопасности в операционной системе / В.И. Темченко, А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 740-745.
12. Цветков, А.Ю. Исследование существующих механизмов защиты операционных систем семейства Linux / А.Ю. Цветков // Актуальные проблемы инфотелекоммуникаций в науке и образование. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 4-х т. СПб.: СПбГУТ, 2018. С. 657-662.
13. Цветков А.Ю. Обеспечение безопасности в клиент-серверном Java приложении для учета и автоматической проверки лабораторных работ / А.Ю. Цветков, М.Е. Шалаева, М.А. Юрченко // Актуальные проблемы инфотелекоммуникаций в науке и образование. VIII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. СПб.: СПбГУТ, 2019. С. 756-761.
14. Багомедова А.Р., Ушаков И.А., Цветков А.Ю. Разработка методов проверки соответствия серверов виртуализации требованиям безопасности согласно стандарту ГОСТ Р 56938-2016 // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): сборник статей VII Международной научно-технической и научно-методической конференции. 2018. С. 58-63.

УДК 004.7: 621.39

ПРОТОКОЛ МАРШРУТИЗАЦИИ ДЛЯ ГЕТЕРОГЕННЫХ БЕСПРОВОДНЫХ ЯЧЕИСТЫХ СЕТЕЙ

Хазиев Нугаян Нурутдинович, Григорьев Артем Александрович, Зятинин Александр Александрович, Коростень Александра Олеговна

Военная академия связи им. Маршала Советского Союза С.М. Буденного,
Тихорецкий пр-т, д. 3, Санкт-Петербург, 194064, Россия
e-mail: grigorev.artem-x@yandex.ru

Аннотация. Внедрение гетерогенных беспроводных сетчатых технологий дает возможность повысить пропускную способность сети, расширить охват и повысить качество обслуживания (QoS). Каждое беспроводное устройство использует различные стандарты, форматы данных, протоколы и технологии доступа. Однако разнообразие и сложность таких технологий создают проблемы для традиционных систем контроля и управления. В данной статье предлагается гетерогенная архитектура столичной сети, которая сочетает в себе беспроводную ячеистую сеть IEEE 802.11 (WMN) с сетью LTE. Кроме того, предлагается новый гетерогенный протокол маршрутизации и алгоритм маршрутизации, основанный на усилительном обучении, называемый когнитивной гетерогенной маршрутизацией, для выбора соответствующей технологии передачи данных на основе параметров каждой сети. Предлагаемая гетерогенная сеть преодолевает проблемы отправки пакетов по длинным путям, островным узлам и помехам в WMNs и увеличивает общую пропускную способность комбинированной сети за счет использования нелицензионных частотных полос вместо покупки большего количества лицензионных частотных полос для LTE. Результаты моделирования показывают, что предлагаемая сеть достигает увеличения пропускной способности до 200% по сравнению с сетями только Wi-Fi или сетями только LTE.

Ключевые слова: интернет-трафик; гетерогенная сеть; гетерогенные узлы; пропускная способность; метрика; интероперабельность.

PROTOCOL ROUTING ALGORITHM IN PACKET MOBILE DATA NETWORKS

Haziev Nugayan, Grigorev Artem, Zatinin Aleksandr, Korosten Aleksandra

Military Academy of Communications Marshal of the Soviet Union S.M. Budyonny
Tikhoretsky Ave., 3, St. Petersburg, 194064, Russia
e-mail: grigorev.artem-x@yandex.ru

Abstract. The introduction of heterogeneous wireless mesh technologies provides the opportunity to increase network capacity, expand coverage and improve quality of service (QoS). Each wireless device uses different standards, data formats, protocols, and access technologies. However, the variety and complexity of such technologies creates problems for traditional monitoring and control systems. This article proposes a heterogeneous metropolitan network architecture that combines an IEEE 802.11 wireless mesh network (WMN) with an LTE network. In addition, a new heterogeneous routing protocol and a learning-based routing algorithm called cognitive heterogeneous routing are proposed to select the appropriate transmission technology based on the parameters of each network. The proposed heterogeneous network overcomes the problems of sending packets over long paths, island nodes and interference in WMNs and increases the overall capacity of the combined network by using unlicensed frequency bands instead of buying more licensed frequency bands for LTE. Simulation results show that the proposed network achieves a throughput increase of up to 200% compared to Wi-Fi-only or LTE-only networks.

Keywords: internet traffic; heterogeneous network; heterogeneous nodes; bandwidth; metric; interoperability.

Введение. Интернет-трафик, как ожидается, увеличится в три-пять раз в течение следующих трех лет из-за роста числа подключенных мобильных устройств. Количество подключенных устройств и машинно-машинной связи, как ожидается, увеличится в 2 раза. Прогнозируется, что в течение следующего десятилетия для поддержки этого роста интернет-трафика потребуется более развитая интернет-инфраструктура. Беспроводные сети [1] следующего поколения должны решать несколько задач, включая затраты на покрытие районов с высокой плотностью населения, многолюдных мероприятий, больших площадей или на временные изменения где будут востребованы, например, крупные спортивные мероприятия. Оценка стоимости зависит от количества необходимых базовых станций и стоимости аренды полос частот. Интероперабельность - это еще одна проблема, поскольку многие устройства используют различные операционные системы, протоколы и технологии доступа. Надежность сети также является важным вопросом, который необходимо решить, чтобы гарантировать, что системы способны функционировать без сбоев в сложных и изменяющихся условиях. Интернет-взаимодействие различных беспроводных технологий, в частности LTE и беспроводных локальных вычислительных сетей, является одной из ключевых возможностей для развития беспроводных сетей следующего поколения. LTE - это эволюция стандарта третьего поколения, который обеспечивает широкий охват и пиковую скорость передачи данных.

Однако в сетях LTE используются лицензированные полосы частот [2], и поэтому для обеспечения большей пропускной способности вводятся дополнительные затраты либо на покупку большего количества полос частот (которые могут быть доступны не во всех регионах), либо на инвестиции в более высокую плотность базовых станций. Еще одной перспективной беспроводной архитектурой для следующего поколения беспроводных сетей являются беспроводные ячеистые сети (WMNs). WMN - это парадигма, разработанная для обеспечения широкого покрытия сети без использования централизованной инфраструктуры. Таким образом, WMNs - это реальный выбор для обеспечения магистральной сети для крупномасштабных сетей. В таких сетях для обеспечения интернет-соединения с ячеистой сетью используются шлюзы (беспроводные узлы с высокоскоростным проводным подключением к внешнему интернету). Эта архитектура обеспечивает экономичное повсеместное беспроводное подключение к интернету [3] на больших площадях через многопоточную передачу к шлюзу и наоборот. Обширное моделирование при различных сценариях и требованиях к сетям позволяет получить прирост пропускной способности до 200% в предлагаемой гетерогенной сети по сравнению с сетями только LTE и Wi – Fi.

Существуют два типа протоколов маршрутизации в WMNs. Первый тип состоит из реактивных протоколов маршрутизации, в которых маршрут создается по требованию путем заполнения сети маршрутными запросами. Выбор маршрута поддерживается только для узлов, передающих трафик в определенный пункт назначения. Примерами такого типа маршрутизации являются ad hoc on-demand distance vectors и dynamic source routing. Реактивная маршрутизация вызывает некоторую задержку из-за того, что маршрут создается только тогда, когда есть данные, готовые к отправке. Второй тип протокола маршрутизации состоит из проактивных или табличных протоколов маршрутизации. Они поддерживают таблицу всего назначения в сети, периодически распространяя обновление таблицы маршрутизации на все узлы. Примерами такого типа протокола маршрутизации являются целевой секвенированный вектор расстояния и оптимизированная маршрутизация состояния канала связи.

Наиболее широко используемые метрики в протоколах маршрутизации WMN выбирают кратчайший путь к шлюзу на основе количества переходов, то есть количества узлов между источником и пунктом назначения.

Также особенностью этой статьи является создание алгоритма маршрутизации, который называется CHR, который определяет требования к выбору передающего устройства на узлах, имеющих как LTE, так и Wi-Fi устройства. Обучение с подкреплением используется для того, чтобы извлечь уроки из предыдущих действий и оптимизировать производительность сети.

Гетерогенная сеть (HetMeshNet) [3] рассматривает сосуществование нескольких беспроводных технологий, а также проводной сети. Он использует следующие типы узлов: гетерогенные узлы (HetNode)—узлы с поддержкой Wi-Fi и LTE; узлы mesh шлюзов—узлы с Wi-Fi и проводным соединением; базовые станции LTE—также известные как развитый NodeB (eNodeB или eNB); узлы Internet gateway—узлы, которые соединяют все сети с интернетом с помощью высокоскоростной проводной сети; и клиентские узлы-используемые конечными пользователями или датчиками. HetMeshNet. Он включает в себя несколько типов сетевых компонентов. Во-

первых, сеть LTE состоит из множества ячеек, распределенных в регионе. Базовая станция LTE расположена в каждой ячейке. Во-вторых, в сети развернуто несколько Гетнодов, каждый из которых может быть использован в различных технологиях. Гетерогенные узлы (HetNodes) оснащены сетевыми интерфейсными картами Wi-Fi и LTE. Узлы mesh gateway - это узлы третьего типа, которые соединяют WMN с интернет-шлюзом. Интернет-шлюз действует как сервер; он обеспечивает подключение к интернету как LTE, так и WMN сети. Наконец, клиентскими узлами могут быть люди, использующие мобильный телефон, ноутбук или любое другое устройство, подключенное к интернету (например, датчик, отправляющий данные в интернет).

Рассмотрим протокол маршрутизации гетерогенного WMN. Предлагаемый новый протокол маршрутизации использует метрики двух сетей для динамического переключения между технологиями передачи. Предлагаемый протокол состоит из двух основных компонентов: гетерогенных таблиц маршрутизации и алгоритма маршрутизации.

В гетерогенных таблицах маршрутизации каждый тип узла использует различные технологии передачи, и каждая технология передачи использует другой сетевой адрес. Для маршрутизации пакетов между этими различными сетями каждый тип узлов поддерживает таблицу маршрутизации для пересылки пакетов данных из разных сетей так же, как если бы они поступали из одной и той же сети. Во-первых, узел интернет-шлюза нуждается в таблице маршрутизации для пересылки пакетов данных в интернет и из интернета для сетей WMN и LTE. Во-вторых, каждый гетерогенный узел поддерживает таблицу маршрутов к другим гетерогенным узлам сети, а также список доступных сетчатых шлюзов и сетчатый шлюз по умолчанию для пересылки гетерогенных узловых данных. Для создания этой таблицы используется протокол маршрутизации OLSR, используемый для определения таблицы маршрутов для ячеистой сети Wi-Fi и использует счетчик ретрансляций в качестве метрики. Затем добавляется расширение инструментов для поддержки использования сетки шлюза в WMN. Расширенный OLSR использует две метрики для выбора mesh-шлюза: количество переходов к mesh-шлюзу и количество подключенных к нему узлов. Для достижения этой цели управляющее сообщение передается соседним узлам от каждого шлюза для объявления его нагрузки с точки зрения количества узлов, связанных с ним. Каждый узел выбирает шлюз [4] с кратчайшим путем, и если более чем один шлюз имеет одинаковое количество переходов, то узел выбирает шлюз с меньшей нагрузкой. Использование кратчайшего пути для выбора маршрута к шлюзу с помощью OLSR позволит избежать возникновения проблемы колебания маршрута, поскольку узел использует только кратчайший путь к шлюзу без переключения к неоптимальным маршрутам.

Гетерогенная WMN оценивается с помощью симулятора NS-3, который является широко используемым инструментом для оценки и валидации беспроводных сетей. Для оценки и валидации предлагаемой сети используются два типа сценариев. Первый сценарий состоит из топологий сетки, в которых гетноды распределены в сетке. Второй сценарий состоит из случайных топологий, в которых все узлы случайным образом распределены в области 1000 м×1000 м. В обоих сценариях есть пять шлюзов, распределенных в сети, и LTE eNB выделяется в центре. Для анализа производительности предлагаемой сети применяются различные нагрузки на сеть, использующую 19 и 30 узлов, передающих одновременно информацию как в одноуровневой сети, так и осуществляет передачу информации на базовые станции.

HetMeshNet сравнивается с сетями LTE, использующие различное количество блоков радиоресурсов (RBs), а также сетями Wi-Fi. Для оценки предлагаемой системы используются два типа сценариев: один для тестирования линии связи с шлюзами и один для тестирования одноранговой сети. В сценариях связи с шлюзами линии связи узлы (за исключением узлов mesh gateway) генерируют трафик протокола пользовательских дейтаграмм (UDP) с одинаковой скоростью, и единственным назначением является интернет. Это имитирует «восходящий» трафик от клиентских терминалов к интернету. В моделировании используются сеточная и случайная топологии, и к сети прикладываются две различные нагрузки, используя 19 и 30 узлов, одновременно передающих данные в интернет. Второй сценарий используется для того, чтобы показать, как алгоритм адаптируется к изменению величины нагрузки во время моделирования. Результаты моделирования для сценариев «восходящей» линии связи указывают на значительное улучшение пропускной способности системы для предлагаемой гетерогенной системы по сравнению с базовыми сетями.

В данной статье представлен новый подход к построению гетерогенной сетевой архитектуры, в которой беспроводные устройства [4] LTE и Wi-Fi используются для получения преимуществ в пропускной способности каждой технологии передачи. Кроме того, был разработан новый протокол маршрутизации для гетерогенных WMNs, который динамически выбирает технологию передачи для увеличения общей пропускной способности сети и повышения средней пропускной способности. Кроме того, для нужд протокола маршрутизации был предложен новый алгоритм маршрутизации, который оценивает стоимость передачи трафика через каждую сеть. Предлагаемый алгоритм рассматривает нагрузку трафика на сеть LTE в качестве метрики для оценки стоимости передачи по LTE и использует скорость передачи в качестве метрики для ячеистой сети Wi-Fi. Результаты моделирования показывают, что предлагаемая сеть обеспечивает до 200% большую пропускную способность по сравнению с сетями только Wi-Fi и сетями только LTE. Гетерогенная сетевая архитектура управляет различными беспроводными устройствами как частью единой виртуальной сети. Сеть LTE используется для того, чтобы избежать перегруженных узлов Wi-Fi и пути высокой интерференции в WMN, в то время как WMN разгружает нагрузку сети LTE, снижает стоимость использования большего количества лицензированных частотных диапазонов и вперед, когда пропускная способность LTE ухудшается. Эта работа обеспечивает основу для будущих исследований развития гетерогенных ячеистых сетей Wi-Fi/LTE и использования других беспроводных технологий в составе гетерогенных сетей.

Заключение. Предлагаемый протокол маршрутизации потенциально может быть расширен для поддержки других беспроводных технологий за счет использования их параметров в алгоритме обучения. Предлагаемая архитектура обеспечивает простой способ расширения покрытия и пропускной способности мобильной сети и может внести свой вклад в инфраструктуру пятого поколения. Кроме того, гетерогенные сети могут использоваться для подключения сетей интернета вещей и использоваться для обеспечения инфраструктуры умных домов и умных городов.

СПИСОК ЛИТЕРАТУРЫ

1. Чуднов А. М., Кирик Д. И., Курашев З. В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений. // Радиотехнические и телекоммуникационные системы. 2017, №2, с.41-49.
2. Чуднов А. М., Курашев З. В. Принципы формирования маршрутных таблиц на основе оптимизации распределения потоков в сети передачи данных. // Наукоемкие технологии в космических исследованиях Земли. 2017. Т.9, № 6, с. 46–51.
3. Маркин В. Г., Рыжкова А. Г. Протоколы маршрутизации в мобильных самоорганизующихся сетях. // Теория и техника радиосвязи, 2013, №4, с.48-56. Siachalou S. Efficient QoS routing.// The International Journal of Computer and Telecommunications Networking. 2003. vol. 43. iss. 3. p. 351-367.
4. Toh C. K. Wireless Atm and Ad-Hoc Networks: Protocols and Architectures.// Kluwer Academic Publisherb Group. 1997. – 313 p.

УДК 004.7: 621.39

ОПТИМИЗАЦИЯ АЛГОРИТМОВ ГИБКОЙ МАРШРУТИЗАЦИИ В СЕТИ ПЕРЕДАЧИ ДАННЫХ БПЛА

Хазиев Нугаян Нурутдинович, Волков Вадим Вагифвич. Зятинин Александр Александрович, Чекалина Елена Анатольевна
Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия
e-mail: zyatinin@rambler.ru

Аннотация. Ресурсные ограничения и динамический характер роя беспилотных летательных аппаратов (БПЛА) создают проблемы при разработке протоколов маршрутизации. Большинство традиционных схем произвольной маршрутизации не интеллектуальны и не могут адаптироваться к динамической природе сетей БПЛА. С другой стороны, некоторые схемы маршрутизации на основе искусственного интеллекта (ИИ) могут потреблять значительные вычислительные ресурсы в беспилотных летательных аппаратах. Предлагается адаптивный протокол маршрутизации, а именно маршрутизация роя на основе структур, которые использует интеллектуальный алгоритм онлайн-обучения и особенности топологии управляемого полетом БПЛА для распределения трафика по оптимальным маршрутам.

Ключевые слова: беспилотный летательный аппарат; рой; геометрическая адресация; адаптивная маршрутизация; скелет; каркас; маршрутизация роя; геоадрес.

COMPLEX ROUTING ALGORITHM IN PACKET MOBILE DATA NETWORKS

Haziev Nugayan, Volrov Vadim, Zatinin Aleksandr, Chekalina Elena
The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia
e-mail: zyatinin@rambler.ru

Abstract. A swarm of unmanned aerial vehicles (UAVs) requires the transmission of data related to a data transmission task over a network. Resource constraints and the dynamic nature of the swarm create problems when developing UAV routing protocols. Most traditional random routing schemes are not intelligent and cannot adapt to the dynamic nature of UAV networks. On the other hand, some artificial intelligence (AI) - based routing schemes can consume significant computing resources in unmanned aerial vehicles. An adaptive routing protocol is proposed, namely skeleton-based swarm routing (SSR), which uses an intelligent online learning algorithm and features of the UAV's flight-controlled topology to distribute traffic along optimal routes.

Keywords: unmanned aerial vehicle; swarm; geometric addressing; adaptive routing; skeleton; wireframe; swarm routing.

Введение. Сеть беспилотных летательных аппаратов имеет специфические характеристики с точки зрения мобильности, вычислительной мощности, энергопотребления и распространения радиосигнала, которые делают ее отличной от других типов специальных сетей.

Сети связи, состоящие из БПЛА [1], были развернуты в различных гражданских, коммерческих и военных целях, таких как борьба со стихийными бедствиями, пограничное наблюдение, поисково-спасательные операции, доставка грузов и т. д. В таких сетях часто требуется передавать данные (например, видео наблюдения высокого разрешения) между БПЛА или на станцию управления. Таким образом, установление надежных сквозных маршрутов между беспилотными летательными аппаратами имеет решающее значение для многих применений, требующих высокого качества обслуживания (*QoS*).

Схема *SSR* направлена на достижение интеллектуальной роевой адаптивной [2], сбалансированной по нагрузке и высокой пропускной способности маршрутизации. Он строит листовидную маршрутную трубу (от

источника к месту назначения), состоящую из взаимосвязанных путей. Основываясь на обратной связи, узлы постепенно регулируют частоту передачи данных по этим путям.

Когда исходный узел p решает отправить пакеты в пункт назначения q, он сначала ищет соответствующую запись в своей таблице маршрутизации и извлекает ее $G(q)$ из таблицы геоадресов. Если есть соответствующий набор (*SSR* может найти это, сравнив $G(q)$ и его отметка времени с теми, что указаны в таблице маршрутизации), он начинает отправлять пакеты между точками на основании соответствующей ценности. В противном случае он сначала обновляет пути и соответствующие им значения.

Кроме идентификаторов источника и назначения, заголовок пакета данных также включает в себя, отметку времени, когда источник обновился. Когда узел ретрансляции получает пакет, он обновляет $G(p)$ в своей геоадресной таблице. Если узел имеет более новый $G(q)$ по сравнению с пакетом, он вставляет обновленный в заголовок пакета и уведомляет источник об изменениях в $G(q)$. В общем, каждый узел, который слышит новый геоадрес, обновит свою таблицу. При значительных изменениях геоадреса узла или назначения q, набор узлов следующего перехода, $PF(q)$, обновляется и Q -инициализируются значения вновь добавленных узлов.

Сетчатая архитектура, вдохновляет нас сформулировать задачу маршрутизации [3] на основе скелета как стохастическую задачу кратчайшего пути, которая может быть решена с использованием подхода динамического программирования. Стоимость (или вознаграждение) назначается каждому звену внутри листовидной трубы, и совокупная стоимость рассчитывается методом обратной рекурсии. Однако, стоимостные значения заранее не известны и подвержены изменениям из-за динамического характера роевой сети. Таким образом, используется онлайн-подход, основанный на динамическом программировании, который может быстро адаптироваться к изменениям условий сети. Он имеет два основных преимущества:

Чтобы отправить совокупную стоимость (или вознаграждение) по пути в обратном порядке, можно воспользоваться сообщениями, которые обычно используются в протоколах маршрутизации. Мини-канал инициируется от каждого узла ретрансляции к месту назначения q. “Ожидаемая” стоимость (или вознаграждение) отправки пакетов с узла g через мини-трубу, обозначается как $V(g)$, который может быть привязан к g ’это сообщения. После его получения отправитель обновляет значение, соответствующее узлу пересылки г в таблице маршрутизации.

Проблема может быть смоделирована как Марковский процесс принятия решений, в котором каждый узел является состоянием.

Узел может стать следующим экспедитором на основе функции распределения вероятностей. Существуют различные стратегии выбора действий в схемах обучения на основе подкрепления, такие как случайный выбор действий и жадные подходы. Здесь используется подход Больцмана, который выбирает действия на основе функции распределения вероятностей, так что более полезные действия выбираются с более высокой вероятностью.

Основное преимущество подхода Больцмана перед ϵ -жадный подход [4] заключается в том, что неоптимальные действия не выбираются с равной вероятностью. Вместо этого они принимаются с частотой, соответствующей их предполагаемому вознаграждению. Следовательно, на этапе исследования можно получить больше наград. При таком подходе функция вероятности представляется функцией *Softmax* (или нормализованной экспоненциальной функцией) с температурным параметром τ. Здесь правильный выбор τ это очень важно. Более высокие значения приводят к почти равновероятным действиям, как при случайном подходе, в то время как более низкие значения могут иметь большое значение в вероятности выбора действия.

Определение понятия является специфичным для конкретного приложения и зависит от требований *QoS*. Это может быть взвешенная комбинация нескольких показателей. Например, потоковое видео требует высокой скорости передачи данных и очень низкой задержки. Контрольные пакеты содержат конфиденциальную информацию и, следовательно, требуют своевременной доставки. Некоторые приложения *IPv4* и автономная передача текстов или документов могут быть классифицированы как наиболее эффективные сервисы.

Для наиболее эффективного трафика пакеты данных могут быть направлены по путям с более высокой остаточной энергией в промежуточных узлах, хотя они могут не обеспечивать связь с низкой задержкой. Например, в работе была предложена энергетически осознаваемая функция вознаграждения, которая применительно к нашей проблеме.

Чтобы *SSR* поддерживал связь с высокой пропускной способностью и низкой задержкой для высокоприоритетного трафика [5], задержка обслуживания за один переход определяется как стоимость, то есть продолжительность времени с момента поступления пакета в очередь до момента его успешной доставки. Он представляет длину очереди и использование канала (т. е. среднюю задержку доступа в протоколах, основанных на конкуренции) и, следовательно, приводит к решению с балансировкой нагрузки. Он также косвенно рассказывает о других ситуациях, таких как радиочастотные помехи, столкновения каналов и передача связи. Если узел испытывает высокие помехи или плохой *SINR* (из-за большого расстояния), скорость передачи пакетов увеличивается, что приводит к увеличению задержки доставки пакетов. Узел может найти ожидаемую задержку обслуживания через статистику прошлых опытов.

Заключение. *SSR* может быть объединен со схемами обнаружения преднамеренных помех для обхода данных вокруг зон помех. Если БПЛА способны обнаруживать преднамеренные помехи и оценивать себя на основе вероятности вмешательства, эта оценка может быть отражена в Q значение узлов. Следовательно, в вероятность переадресации потенциальному экспедитору увеличивается, если мини-труба инициируется

и имеет более низкий шанс быть вовлеченным в преднамеренные действия вмешательства. В этом случае, *SSR* может направлять пакеты через “безопасные” области в трубе. Обратите внимание, что пограничные узлы, т. е. узлы, близкие к зоне помех, более уязвимы для преднамеренного вмешательства в ближайшем будущем из-за мобильности. Таким образом, им следует присвоить более низкий балл.

СПИСОК ЛИТЕРАТУРЫ

1. Маркин В. Г., Рыжкова А. Г. Протоколы маршрутизации в мобильных самоорганизующихся сетях. // Теория и техника радиосвязи, 2013, №4, с.48-56. Siachalou S. Efficient QoS routing. // The International Journal of Computer and Telecommunications Networking. 2003. vol. 43. iss. 3. p. 351-367.
2. Чуднов А. М., Курашев З. В. Принципы формирования маршрутных таблиц на основе оптимизации распределения потоков в сети передачи данных. // Наукоемкие технологии в космических исследованиях Земли. 2017. Т.9, № 6, с. 46–51.
3. Шварц М. Сети связи: протоколы, моделирование и анализ, Ч. 1, 2. М.: Наука. 1992.
4. Toh C. K. Wireless Atm and Ad-Hoc Networks: Protocols and Architectures. // Kluwer Academic Publisherb Group. 1997. – 313 p.
5. Овсянников С.Н., Панин Р.С., Калюка В.И. Принципы обеспечения информационной безопасности в сетях беспроводного абонентского доступа//Региональная информатика и информационная безопасность. 2017. С. 147-149.

УДК 004.7: 621.39

ПОВЫШЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ MESH-СЕТИ С ДЕЦЕНТРАЛИЗОВАННЫМ УПРАВЛЕНИЕМ

Хазиев Нугаян Нурутдинович, Зятинин Александр Александрович, Калайтанова Елена Владимировна, Попов Андрей Иванович

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

Аннотация. Планирование и распределение спектра частот — это задачи, влияющие на производительность сетей когнитивной радиосвязи, где неоднородность в доступности каналов ограничивает производительность и представляет собой серьезную проблему при разработке протоколов управления сетью. С учетом этого предлагается распределенный алгоритм для планирования и распределения спектра с позиции повышения эффективности функционирования всей сети при заданных требованиях к ней. В процессе функционирования mesh-сети проблемы планирования и распределения спектра частот включают так же и выбор подмножества каналов, которые будут задействованы и на основе результатов зондирования спектра распределяет доступные ресурсы по этим каналам. Эта проблема рассматривается с позиции максимизации эффективности функционирования mesh-сети в целом. Поскольку пропускная способность любого потока данных ограничена пропускной способностью самого слабого звена вдоль его сквозного пути, величина каждого потока выбирается в зависимости от пропускной способности этого самого слабого звена. Пропускная способность и время задержки при передаче пакетов в сети рассчитывается с помощью математического аппарата теории систем массового обслуживания, а повышение пропускной способности достигается за счет применения теории лагранжевой двойственности. Структура двойной декомпозиции разделяет проблему на набор подзадач, которые могут быть решены локально, следовательно, это позволяет разработать масштабируемый распределенный алгоритм. Численные результаты демонстрируют быструю сходимость предлагаемого алгоритма, а также значительный выигрыш в производительности по сравнению с традиционными методами проектирования.

Ключевые слова: пропускная способность4 лагранжевая двойственность; децентрализованное управление; mesh-сеть; распределение спектра частот; подмножество каналов.

INCREASING MESH NETWORK THROUGHPUT WITH DECENTRALIZED MANAGEMENT

Haziev Nugayan, Zatinin Aleksandr, Kalaytanova Elena, Popov Andrey

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

Abstract. Spectrum planning and allocation are challenges affecting the performance of cognitive radio networks, where heterogeneity in channel availability limits performance and presents a major challenge in the design of network management protocols. This article proposes a distributed algorithm for scheduling and allocating spectrum from the standpoint of improving the efficiency of the entire network for the given requirements for it. In the process of functioning of the mesh network, the problems of planning and allocating the frequency spectrum also include the choice of a subset of channels that will be involved and, based on the results of spectrum sounding, distributes the available resources over these channels. This problem is considered from the standpoint of maximizing the efficiency of the mesh network as a whole. Since the bandwidth of any data stream is limited by the bandwidth of the weakest link along its end-to-end path, the size of each stream is selected based on the bandwidth of that weakest link. The throughput and delay time for packet transmission in the network is calculated using the mathematical apparatus of the theory of queuing systems, and the increase in throughput is achieved through the application of the theory of Lagrangian duality. The double decomposition structure divides the problem into a set of subproblems that can be solved locally, hence allowing the development of a

scalable distributed algorithm. Numerical results demonstrate fast convergence of the proposed algorithm, as well as significant performance gains compared to traditional design methods.

Keywords: bandwidth; Lagrangian duality; decentralized control; mesh network; frequency spectrum allocation; channel subset.

Введение. Задача повышения пропускной способности mesh-сети с децентрализованным управлением сводится к распределению канальных и временных ресурсов, чтобы максимизировать совокупную полезность для всех потоков трафика в сети. Полагается, что маршруты между источником каждого потока и его пунктом назначения уже установлены.

Прежде чем представить задачу оптимизации и подход к ее решению, необходимо сначала проанализировать влияние решений о распределении ресурсов на производительность сети.

Когнитивное радио — это коммуникационная парадигма, пользователи которой делятся на две категории в зависимости от того, имеют ли они лицензию на использование определенного диапазона спектра (основные пользователи (*PUL*)) или нелицензированные (вторичные пользователи (*SUH*)). НЛП разрешено оппортунистически использовать спектр, пока они не создают вредных помех для активных ЛП. Это достижимо если приемники ЛП находятся достаточно далеко от передатчика НЛН (доступность пространственного канала), либо приемники ЛП не работают во время передачи передатчика НЛП (временное доступность канала). Эта оппортунистическая и динамичная концепция связи ведет к более «плотному» использованию спектра, и обеспечивает НЛП хорошей доступностью услуг и надежностью.

Одна из самых больших проблем в когнитивной радиосети — это совместное использование спектра, которое определяет набор правил и стратегий, регулирующих поведение НЛП относительно мобильности, распределения и доступа к спектру. В целом архитектура совместного использования спектра классифицируется на две категории: централизованные и распределенные. В централизованном случае организация по управлению использованием спектра контролирует как распределение спектра, так и доступ к спектру. С другой стороны, в распределенной архитектуре каждый НЛП отвечает за распределение каналов и принятия решения о доступе. НЛП может принимать решения на основании локального наблюдения за сетью и состоянием спектра или путем сотрудничества с другими пользователями, чтобы иметь более глобальное наблюдение.

Ячеистая сеть с когнитивной радиосвязью — это ячеистая беспроводная сеть (mesh-сеть), которая развертывает когнитивные радио для своих узлов, и полагается на гибкий и динамичный доступ к спектру для его работы. Помимо увеличения спектра частот и преодоления дефицита его ресурса, когнитивные ячеистые радиосети создавались для ряда потенциальных приложений, решающих новые и сложные задачи. Например, когнитивные ячеистые сети могут уменьшить перегруженность традиционных беспроводных сетей за счет поиска доступных каналов в основном спектре, чтобы они могли уменьшить перегрузку рабочего диапазона беспроводной сети, переместив некоторых пользователей на доступные частоты. В некоторых случаях узлы сети необходимо ограничить по мощности передачи, чтобы помехи, которые они вызывают в месте расположения других базовых станций, оставались в пределах предварительно рассчитанного порога, обеспечивающего требуемое качество обслуживания.

Используемая модель беспроводной ячеистой сети на основе когнитивного радио. Когнитивная сетчатая сеть состоит из узлов, которые оппортунистически делят ресурсы спектра с первичной сетью, состоящей из корреспондирующих пар. Каждая первичная пара приемопередатчиков работает по выделенному отдельному каналу, который не накладывается на каналы других пользователей. Таким образом, количество корреспондирующих пар характеризует количество каналов в сети. Кроме того, все первичные каналы имеют одинаковую пропускную способность. Полагаем, что в первичной сети переключение каналов связи происходит в рассчитанные временные интервалы. Поэтому передача пакетов информации может начинаться только в начале временного интервала. Это предположение упростит анализ нашей когнитивной сети, однако разработанная модель и анализ могут быть расширены для включения различных первичных схем передачи [1].

Каждый узел когнитивной сетки будет оппортунистически обращаться к простаивающим первичным каналам для передачи своих пакетов. Доступность локального канала может быть обнаружена с помощью одного из различных методов зондирования спектра, доступных. Когнитивная сетчатая сеть использует гибридный способ *TDMA/FDMA* для доступа к каналу. Поэтому время разбивается на временные интервалы фиксированной длительности, которые далее группируются в рамки временных интервалов. В каждом временном интервале узел выбирает один из доступных частотных каналов для передачи.

Поскольку передача данных в первичной сети также является дискретной, то и когнитивная сеть регулирует границы своих временных интервалов в соответствии с границами первичной сети. В любой практической системе у *PUs* есть служебные каналы, пакеты синхронизации и различные способы кодирования, которые используются приемниками сети для когерентного обнаружения. Например, телевизионный сигнал имеет узкополосный служебный канал для аудио- и видеоносителей, системы *CDMA* имеют выделенные коды (способы модуляции) распространения для служебных каналов и синхронизирующих пакетов; протокол OFDM имеют предусилители для сбора пакетов и служебных потоков для канала управления.

Каждый узел когнитивной ячеистой сети имеет бесконечный буфер для хранения пакетов фиксированной длины. Случай конечных буферов также может быть включен в нашу модель с небольшими модификациями задачи оптимизации, сформулированной в следующем разделе. Время передачи пакета равно длительности одного временного интервала. Поскольку в начале каждого временного интервала вторичные пользователи

тратят время на зондирование канала, у них будет меньше времени на передачу своих пакетов по сравнению с первичными пользователями. Однако *SU* может выбрать схему модуляции и длину пакета таким образом, чтобы полезная часть временного интервала была достаточна для передачи одного полного пакета.

Основная цель при попытке решить задачу оптимизации состоит в том, чтобы найти решение, которое является децентрализованным и масштабируемым. Наличие минимального члена внутри функции полезности значительно усложняет задачу. Чтобы упростить задачу, мы предлагаем преобразовать минимальный член в набор ограничений линейного неравенства. Это преобразование упрощает целевую функцию и позволяет использовать теорию двойственности для поиска децентрализованного решения, как будет показано в следующем разделе.

Решение проблемы распределения ресурсов централизованным способом требует наличия глобальной информации о сети в центральной точке [2], чтобы иметь возможность найти решение. В беспроводной ячеистой сети каждый узел имеет локальную информацию о своей среде. Эта локальная информация должна быть передана в центральную точку со всех узлов сети. Во многих случаях такие коммуникационные накладные расходы нецелесообразны, особенно в сетях с большим количеством узлов. В этом разделе мы предлагаем декомпозицию исходной задачи на более мелкие подзадачи, которые могут быть эффективно решены распределенным способом.

В данной работе задача максимизации пропускной способности в когнитивных радиосвязях на основе *WMN* формулируется как задача максимизации полезности. Используемая функция полезности является функцией минимальной скорости обслуживания вдоль сквозного пути этого потока, что обеспечивает степень справедливости между различными потоками. Кроме того, формулировка задачи максимизации позволяет включать различные сквозные ограничения задержки. Проблема централизованного распределения ресурсов в масштабах всей сети была разложена на ряд подзадач, которые могут быть решены локально. Эффективная и масштабируемая децентрализованная система [3] был предложен протокол решения.

Заключение. Результаты демонстрируют эффективность предложенной схемы децентрализованного решения и ее способность адаптироваться к изменяющимся сетевым нагрузкам. Продемонстрирован прирост производительности предлагаемого протокола по сравнению с равномерным распределением ресурсов и максимальным-минимальным распределением полосы пропускания. Было показано, что при заданном объеме ресурсов предлагаемый протокол [4] может вместить большее количество потоков трафика. Кроме того, он может добиться увеличения пропускной способности до 17% и уменьшения задержки на 20%.

СПИСОК ЛИТЕРАТУРЫ

1. Чуднов А. М., Кирик Д. И., Курашев З. В. Оптимизация распределения информационных потоков в информационной системе по показателю вероятности своевременной доставки сообщений. // Радиотехнические и телекоммуникационные системы. 2017, №2, с.41-49.
2. Чуднов А. М., Курашев З. В. Принципы формирования маршрутных таблиц на основе оптимизации распределения потоков в сети передачи данных. // Наукоемкие технологии в космических исследованиях Земли. 2017. Т.9, № 6, с. 46–51.
3. Маркин В. Г., Рыжкова А. Г. Протоколы маршрутизации в мобильных самоорганизующихся сетях. // Теория и техника радиосвязи, 2013, №4, с.48-56. Siachalou S. Efficient QoS routing. // The International Journal of Computer and Telecommunications Networking. 2003. vol. 43. iss. 3. p. 351-367.
4. Toh C. K. Wireless Atm and Ad-Hoc Networks: Protocols and Architectures. // Kluwer Academic Publisherb Group. 1997. – 313 p.

ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 004.94

ИМИТАЦИОННАЯ МОДЕЛЬ ФОРМИРОВАНИЯ И КОНТРОЛЯ БИЗНЕС-ПРОЦЕССОВ ИНТЕГРАЦИИ ОРГАНИЗАЦИОННЫХ КУЛЬТУР

Абрамова Евгения Александровна
Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mail: vectra4444@mail.ru

Аннотация. Организационная культура является важной характеристикой для разработки квалифицированной стратегии интеграции. В условиях объединения компаний из разных стран своевременность, надежность и эффективность интеграции организационных культур является одной из ключевых задач. В статье описана разработанная имитационная модель, позволяющая по результатам проведения экспериментов с достаточно большой точностью прогнозировать количество сотрудников компании, образованной в результате слияния.

Ключевые слова: имитационная модель; надежность интеграции; своевременность интеграции; слияния; поглощения, сценарии объединения.

A SIMULATION MODEL ENSURING THE TIMELINESS, RELIABILITY AND EFFICIENCY OF THE INTEGRATION OF ORGANIZATIONAL CULTURES

Abramova Evgenia
ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mail: vectra4444@mail.ru

Abstract. Organizational culture is an important characteristic for developing a qualified integration strategy. In the context of the merger of companies from different countries, the timeliness, reliability and efficiency of the integration of organizational cultures is one of the key tasks. The article describes a developed simulation model that allows, based on the results of experiments, to predict the number of employees of a company formed as a result of the merger with a sufficiently high accuracy.

Keywords: simulation model; reliability of integration; timeliness of integration; mergers; acquisitions, unification scenarios.

Основной целью всех сделок слияния и поглощения является успешная интеграция. Интеграция приводит к созданию новой организационной структуры в процессе объединения компаний. Статистические данные показывают, что 70% случаев потенциально выгодных слияний терпят неудачу из-за некачественной подготовки и проведения интеграции [1]. Таким образом, выбор организационной формы для интеграции компаний в соответствии с заявленными критериями, обеспечивающими своевременность, надежность и эффективность интеграции является важным шагом, который может способствовать объединению ресурсов и эффективности. Чтобы избежать ошибок, необходимо разработать план процедур слияний и поглощений, и вопрос об организационной культуре и персонале новых компаний должен быть сформулирован на этапе выбора объекта для слияний и поглощений [2]. На сегодняшний день не существует инструмента, позволяющего достоверно диагностировать совместимость организационных культур и воспроизвести за короткий промежуток времени большое количество возможных сценариев объединения компаний. Используя средства имитационного моделирования, можно за короткий временной промежуток получить большое количество возможных сценариев [3] объединения организационных культур, необходимых для формирования корректной интегрированной культуры. Имитационная модель должна обладать следующими характеристиками: надежность, способность моделировать систему, близкую к реальности; гибкость; возможность изменения параметров модели без изучения сложных зависимостей организационных культур, описываемых в литературе. Любые бизнес-инструменты должны соответствовать определенному уровню своевременности и надежности, позволяющему исключить факторы потери данных или ошибочных расчетов. Данный аспект особенно важно учесть при построении модели. Разработанная имитационная модель содержит много стохастических величин, поэтому для выявления четких тенденций необходимо проводить большое количество экспериментов с одинаковыми значениями изменяемых экзогенных параметров. По результатам проведения имитационных экспериментов с

достаточно большой точностью можно прогнозировать количество сотрудников компании, образованной в результате слияния. Этот фактор успеха является одним из важнейших в сделках слияния и поглощения. Предполагается оценка влияния на исследуемые процессы инфокоммуникационной составляющей [4].

СПИСОК ЛИТЕРАТУРЫ

1. Delong, G., & Deyoung, R. (2007). Learning by observing: Information spillovers in the execution and valuation of commercial bank M&As. // Journal of Finance, 62, p. 181–216.
2. Colombo, G., Conca, V., Buongiorno, M., & Gnan, L. (2007). Integrating cross-border acquisitions: A process-oriented approach. // Long Range Planning 40, p. 202–222
3. Имитационное моделирование: создание терминов // Хабрахабр. [Электронный ресурс]. URL: http://habrahabr.ru/post/246307/
4. Богатырев В.А. Комбинаторно-вероятностная оценка надежности и отказоустойчивости кластерных систем // Приборы и системы. Управление, контроль, диагностика" - 2006. - № 6

УДК 621.391

МОДЕЛЬ КИБЕРКИНЕМАТИЧЕСКОЙ СИСТЕМЫ

Астахова Татьяна Николаевна[1], Колбанёв Михаил Олегович[2]
[1] Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия
[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: ctn_af@mail.ru, mokolbanev@mail.ru

Аннотация. В работе предложено построение модели процесса взаимодействия кибернетической и физической компонент комплексной системы на примере БСС.

Ключевые слова: киберфизические системы; киберкинематические системы; машина Дубинса; оптимальный маршрут; система дифференциальных уравнений; управление; формула Фрииса; энергопотребление.

MODEL OF CYBERMECHANICAL SYSTEMS ON THE EXAMPLE OF USN

Astakhova Tatyana[1], Kolbanev Mikhail[2]
[1] Nizhny Novgorod state University of engineering and Economics
22A Oktyabrskaya St, Knyaginino, 606340, Russia
[2] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: ctn_af@mail.ru, mokolbanev@mail.ru

Abstract. The paper proposes the construction of a model of the process of interaction of the cybernetic and physical components of a complex system using the example of USN.

Keywords: cyber physical systems; cyber-mechanical systems; Dubins car; optimal route; system of differential equations; control; Friis's formula; power usage.

Киберфизические системы представляют огромный интерес для абсолютно любой сферы деятельности: научной, промышленной, экономической и т.д. Киберфизические системы – это цифровая система нового поколения, которая состоит из двух основных функциональных компонентов: расширенные возможности подключения, обеспечивающие сбор данных в реальном времени из физического мира и информационную обратную связь из киберпространства; интеллектуальное управление данными, аналитика и вычислительные возможности, которые создают киберпространство [1].

В качестве элементов киберфизических систем рассматриваются мобильные робототехнические, мобильные клиентские, встроенные, стационарные и облачные компоненты. Их основным подсистемам могут быть поставлены в соответствие четыре процесса (вида функционирования): взаимодействие, функционирование целевых и обеспечивающих технических средств, движение, расход и (или) пополнение ресурсов [2]. Использование моделей киберфизических систем направлено на расширение внедрения крупномасштабных систем за счет улучшения адаптируемости, автономности, эффективности, функциональности, надежности, безопасности и удобства использования таких систем.

В представленной работе даем определение киберкинематической системы и рассматриваем беспроводную сенсорную сеть с подвижными узлами как пример такой системы. Киберкинематические системы – это системы нового поколения с пересекающимися вычислительными и кинематическими возможностями, которые требуют тесной интеграции вычислительных, коммуникационных и управляющих технологий для достижения стабильности, производительности, надежности, устойчивости и эффективности при работе с физическими системами. Это определение полностью подходит и для определение сенсорной сети, т.к. она с одной стороны состоит из физических объектов – сенсорных устройств, которые двигаются в пространстве и занимают определенные полосы частот, потребляют энергия и все это элементы физической системы, потому что физическая система – это совокупность физических объектов, которые описываются непрерывными физическими параметрами: скорость, время и т.д. Эту часть поведения сенсорных устройств можно описать

системой дифференциальных уравнений, системой Дубинса, а потребление энергии, например, формулой Фрииса. Предложенные в работе модели позволяют определить поведение в физическом пространстве в зависимости от того, что происходит в кибернетическом. Например, как кибернетические процессы информационного обмена или обработки влияют на движение. Например, в блок управление пришло сообщение выполнить какое-либо действие в определенном местоположении в пространстве, и физически этот объект направляется в конкретную локацию, где данный объект должен выполнить конкретное действие. И наоборот, законы, по которым они живут в физическом пространстве влияют на то, что происходит в кибернетике, потому что можно по-разному измерять одни и те же параметры.

В работе предложена и построена такая модель, которая позволяет, во-первых, дать представление о влиянии кибернетических характеристик на физические параметры, а также иметь возможность предсказать поведение такой киберфизической системы.

СПИСОК ЛИТЕРАТУРЫ

1. Lee, EA (2015). The past, present and future of cyber-physical systems: A focus on models. Sensors (Switzerland), 15(3), 4837–4869. doi: 10.3390/s150304837
2. Ронжин, А. Л., Басов, О. О., Соколов, Б. В., Юсупов, Р. М. (2016). Концептуальная и формальная модели синтеза киберфизических систем и интеллектуальных пространств. Известия высших учебных заведений. Приборостроение, 59(11).

УДК 004

МОДЕЛЬ УПРАВЛЕНИЯ РЕСУРСАМИ ВЗАИМОДЕЙСТВИЯ КИБЕРТЕХНИЧЕСКИХ СИСТЕМ

Астахова Татьяна Николаевна[1], Колбанев Михаил Олегович[2], Романова Анна Александровна[1,2]

[1] Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия

[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: ctn_af@mail.ru, mokolbanev@mail.ru, anya-romanova-07@yandex.ru

Аннотация. В работе рассмотрена модель управления ресурсами взаимодействия кибертехнических систем.

Ключевые слова: вероятностно-временные характеристики; вероятностно-энергетические характеристики; киберфизическая система; сенсорное устройство.

RESOURCE MANAGEMENT MODEL OF INTERACTION OF CYBER TECHNICAL SYSTEMS

Astakhova Tatyana[1], Kolbanev Mikhail[2], Romanova Anna[1,2]

[1] Nizhny Novgorod state University of engineering and Economics
22A Oktyabrskaya St, Knyaginino, 606340, Russia

[2] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: ctn_af@mail.ru, mokolbanev@mail.ru, anya-romanova-07@yandex.ru

Abstract. The paper considers a model for managing resources of interaction of cybertechnical systems.

Keywords: cyberphysical system; sensor device; probabilistic and energy characteristics; probabilistic-temporal characteristics.

Одним из актуальных направлений научных исследований в наше времена является исследование киберфизических систем, которые по виду реализуемого физического процесса могут быть разделены на: кибербиологические, киберастрономические, киберхимические и другие системы подобного рода.

Кибертехническая система – это созданные людьми инструменты, приспособления, механизмы, машины и устройства, оборудованные средствами формирования, сохранения, распространения и обработки цифровых данных и используемые в процессе некоторой деятельности. Характерной особенностью таких систем является потребность во временных, пространственных и энергетических ресурсах для реализации в процессе деятельности, во-первых, физических процессов, реализуемых техническими компонентами (измерение, передвижение, нагревание) и, во-вторых, кибернетических процессов, реализуемых информационными технологиями работы с цифровыми данными.

Одним из примеров кибертехнических систем является сенсорное устройство беспроводных сенсорных сетей. В процессе работы сенсорного устройства необходимо рассматривать его не только как элемент киберпространства, который передаёт и принимает информацию, но и как элемент, потребляющий энергию.

Можно выдвинуть сложные задачи разработки моделей управления процессами информационного взаимодействия кибертехнических систем, учитывающие ограничения, связанные с энергопитанием. В настоящее время отсутствует комплексное решение таких задач. Предлагаемая модель оценки характеристик сенсорных устройств [1], учитывающие в комплексе такие пространственные, временные и энергетические характеристики сенсорной сети, как геометрический размер и плотность сенсорного поля, частотный диапазон взаимодействия, стратегию выбора ретранслирующего сенсорного устройства при формировании маршрута

передачи сообщений к базовой станции, длину и время передачи сообщений, затраты электроэнергии при передаче сообщений. Модель может использоваться для решения широкого круга задач, возникающих при разработке протоколов функционирования беспроводных сенсорных сетей.

Например, для образования умного сельскохозяйственного объекта необходимо организовать сеть из большого количества сенсорных устройств с автономным питанием. Для сокращения трудозатрат, связанных с заменой электрических батарей, следует обеспечить энергосберегающие режимы работы сенсоров, поэтому разработка модели для оценки соответствующих характеристик для трехмерного пространства сельскохозяйственных угодий является актуальной и имеет практическое значение [2]. Это также влияет на безопасность сети.

В настоящее время разработка и использование кибертехнических систем продолжают активно развиваться. Эти системы эффективны для управления сложными распределенными системами и для решения сложных задач. В работе приведен пример построенной модели для оценки характеристик сенсорных устройств в трехмерном пространстве.

СПИСОК ЛИТЕРАТУРЫ

1. Astakhova T., Kolbanev M., Romanova A. Estimation of the sensor devices characteristics in three-dimensional space of agriculture // В сборнике: The Majorov International Conference on Software Engineering and Computer Systems. 2020. С. 154-157.
2. A. V. Bogatyrev, V. A. Bogatyrev and S. V. Bogatyrev, "Multipath Redundant Transmission with Packet Segmentation," 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), Saint-Petersburg, Russia, 2019, pp. 1-4. doi: 10.1109/WECONF.2019.8840643

УДК 004.7

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ В КИБЕРТЕХНИЧЕСКОЙ СИСТЕМЕ

Верзун Наталья Аркадьевна[1], Колбанёв Михаил Олегович[2], Романова Анна Александровна[2]

[1] Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия

[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия

e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, anya-romanova-07@yandex.ru

Аннотация. Рассматривается имитационное моделирование информационного взаимодействия в кибертехнической системе. Было проведено дискретно-событийное моделирование процесса информационного взаимодействия. При этом кибертехническая система рассматривалась как система множественного доступа, состоящая из множества устройств, которые делят общее время и общую физическую среду передачи.

Ключевые слова: киберфизическая система; кибертехническая стсема; Индустрия 4.0; имитационное моделирование.

IMITATION MODELING OF INFORMATION INTERACTION IN A CYBER-TECHNICAL SYSTEM

Verzun Natalia[1], Kolbanev Mikhail[2], Romanova Anna[2]

[1] Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia

[2] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia

e-mails: verzun.n@unecon.ru, mokolbanev@mail.ru, anya-romanova-07@yandex.ru

Abstract. Simulation modeling of information interaction in a cyber-technical system is considered. Discrete-event modeling of the information interaction process was carried out. At the same time, the cyber-technical system was considered as a multiple access system consisting of a set of devices that share a common time and a common physical transmission medium.

Keywords: cyber-physical system; cyber-technical system; Industry 4.0; simulation modeling.

Ключевыми технологиями доктрины Индустрия 4.0 являются интернет вещей и киберфизические системы, развитие и внедрение которых призвано трансформировать различные области деятельности человека [1, 2]. Прежде всего речь, как правило, идет о кардинальных изменениях в таких сферах как производство, строительство, транспорт, энергоснабжение. Под киберфизической системой понимается совокупность взаимодействующих физических сущностей и компьютеров. Физические сущности могут быть любого вида – это и природные, и искусственно созданные объекты. Встроенные в физические сущности контроллеры, датчики, сенсоры пр. позволяют в реальном времени отслеживать протекающие процессы, обмениваться данными об изменениях в них и окружающей их среде, прогнозировать различные события и адаптироваться под них, оперативно принимать решения без участия человека и реализовывать их (например, посредством исполнительных устройств, актуаторов). Встроенные компьютеры отслеживают и управляют протекающими физическими процессами обычно с помощью циклов обратной связи, где процессы влияют на вычисления и наоборот.

В зависимости от вида физических процессов различают следующие типы систем: кибербиологические, кибермеханические, кибертехническая, киберастрономические, киберхимические, кибергеографические и другие. Примерами кибертехнических систем могут служить всепроникающие сенсорные системы подвижных объектов, беспилотный транспорт, роботы KUKA, системы точного земледелия, рой летательных аппаратов и др. [3-5]. Важным условием эффективного использования кибертехнических систем является способность технической части выполнять свою функцию, а также отлаженное информационное взаимодействие всех компонент системы [6]. Моделирование информационного взаимодействия в кибертехнической системе позволит заранее на этапе её проектирования оценить работоспособность и производительность, принять взвешенные решения по составу, структуре системы, по способу организации информационного взаимодействия в ней.

В работе рассмотрено имитационное моделирование информационного взаимодействия в кибертехнической системе. Было проведено дискретно-событийное моделирование процесса информационного взаимодействия в ходе функционирования системы. При этом кибертехническая система рассматривалась как система множественного доступа [7, 8]: состоит из множества устройств, которые “делят” общее время и общую физическую среду передачи. Была разработана диаграмма процесса взаимодействия, которая представляет собой совокупность взаимосвязанных объектов, участвующих в информационном обмене; проведены имитационные эксперименты и сбор статистики по работе блоков модели. Построены диаграммы, отображающие распределение средней загрузки общего канала, среднее время обслуживания, среднюю длину очереди, гистограмма для оценки времени проведения в очереди. Эксперименты, проведенные на разработанной имитационной модели, позволяют оценить характеристики системы множественного доступа: коэффициент загрузки, длину очереди, вероятность отказа в обслуживании и пр.

СПИСОК ЛИТЕРАТУРЫ

1. Ястреб Н.А. Индустрия 4.0: киберфизические системы, разумное окружение, интернет вещей // Человек в технической среде: сборник научных статей. Вологда: ВоГУ, 2015. Вып. 2. – С. 136–141.
2. Верзун Н. А., Колбанёв М. О., Омельян А. В. Сетевая архитектура цифровой экономики. СПб.: Изд-во СПбГЭУ. 2018. 156 с.
3. Shamin A., Frolova O., Makarychev V. et al. Digital transformation of agricultural industry// IOP Conference Series: Earth and Environmental Science. – 2019. – Vol. 346, № 1. DOI: 10.1088/1755-1315/346/1/012029.
4. Верзун Н. А., Колбанёв М. О., Цехановский В. В. Принципы построения и характеристики цифровых сетей нового поколения. СПб.: Изд-во СПбГЭТУ «ЛЭТИ». 2017. 212 с.
5. Верзун Н. А., Колбанёв М. О., Шамин А.А. Энергетическая эффективность взаимодействия в беспроводных сенсорных сетях \\ Информационные технологии и телекоммуникации. 2017. Том 5. № 1. С. 88–96.
6. Ватаманюк И.В., Яковлев Р.Н. Обобщенные теоретические модели киберфизических систем \\ Известия Юго-Западного государственного университета. 2019. 23(6). – С.161–175. DOI: 10.21869/2223-1560-2019-23-6-161-175.
7. Verzun N., Kolbanev M., Cehanovsky V. Model of Multiple Access in a Super-Dense Network of Smart Things \\ **Conference Proceedings:** 2020 9th Mediterranean Conference on Embedded Computing (MECO). DOI:10.1109/MECO49872.2020.9134364.
8. Верзун Н. А., Колбанёв М. О., Советов Б. Я., Яшин А. И. Методы сбора данных с сенсорных узлов беспроводной сенсорной сети // Изв. СПбГЭТУ «ЛЭТИ». 2018. № 5. – С. 55–60.

УДК 004

ИНТЕРНЕТ ВЕЩЕЙ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ДОБЫВАЮЩЕЙ ПРОМЫШЛЕННОСТИ

Верзун Наталья Аркадьевна, Никулин Никита Сергеевич
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mails: verzun.n@unecon.ru, nikita.nickfake@yandex.ru

Аннотация. Рассматриваются возможности использования технологий интернета вещей в горнодобывающей промышленности для повышения безопасности производственной среды. Реализация на практике подобных решений позволит повысить эффективность и безопасность производственного процесса.

Ключевые слова: интернет вещей; горнодобывающая промышленность; безопасность.

INTERNET OF THINGS FOR SECURITY IN THE EXTRACTIVE INDUSTRY

Verzun Natalia, Nikulin Nikita
Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
e-mails: verzun.n@unecon.ru, nikita.nickfake@yandex.ru

Abstract. The possibilities of using Internet of Things technologies in the mining industry to improve the safety of the production environment are considered. The implementation of such solutions in practice will increase the efficiency and safety of the production process.

Keywords: internet of things; mining industry; security.

Технологии интернета вещей постепенно охватывают различные области человеческой деятельности [1]. Одной из возможных сфер их применения является добывающая промышленность, в частности, в докладе рассматривается горнодобывающая промышленность.

Деятельность в данной сфере зачастую сопряжена с рядом опасностей, угрожающих жизни и здоровью человека [2]. Главная особенность труда в угольных шахтах – неблагоприятные метеорологические условия сопровождающие технологические процессы: отсутствие солнечного света и вентиляции, загрязнение атмосферы рудника опасными для человека газами, шум, вибрации, зачастую высокая влажность, запылённость, сложности водоотведения и пр. [3]. Все это в конечном итоге неблагоприятно сказывается на здоровье горняков и подчас угрожает их жизни. Работа шахтера общепризнана одной из самых сложных, и при этом опасных и вредных. Сегодня задача первостепенной важности горнодобывающей промышленности – это сведение к минимуму рисков на производстве, совершенствование систем обеспечивающих безопасность рабочих и своевременная профилактика травматизма и профессиональных заболеваний.

В [4] отмечается, что “для сохранения безопасности на предприятии желательно внедрение технологий, позволяющих обнаруживать и прогнозировать риски.” Для своевременного прогнозирования проблемных ситуаций и принятия превентивных мер для их устранения и/или минимизации последствий необходимо вести постоянный проактивный мониторинг необходимых параметров (температура, давление, уровень, вибрации и т.д.), производственной среды, а также ключевых показателей деятельности горных рабочих. Применение решений на базе технологий интернета вещей дает возможность: реализовать подобный мониторинг, выполнять сбор и анализ оперативной информации о производственных процессах на месторождении, поддерживать коммуникацию между всеми задействованными в производстве сотрудниками. Датчики, сенсоры, контроллеры и другое периферийное оборудование позволяет проводить регулярные измерения необходимых показателей и передавать эти данных в сеть на облачный сервер [5]. Данные консолидируются, обрабатываются, оперативно анализируются и на их основе принимаются оперативные решения, связанные с безопасностью производственных процессов. Сбор и первичная обработка данных также могут стать основой для создания алгоритмов обработки данных методами машинного обучения и сопутствующего прогнозирования рисков, повышения эффективности стратегического планирования.

В докладе проводится обзор решений на базе технологий интернета вещей для горнодобывающей промышленности, ориентированных на повышение безопасности производственной среды. Реализация их на практике позволит повысить эффективность и безопасность производственного процесса.

СПИСОК ЛИТЕРАТУРЫ

1. Колбанёв М.О., Верзун Н.А., Нестеренко Е.С. К вопросу о сущности и технологиях интернета вещей // Теоретическая экономика. 2020. №5(65). С.36-43.
2. Kubin'ski V., Kubin'ska-Yabtson E., Petrov A., Sala D., Yu D. Savon analysis of hazards in the mining industry // Gornyy informatsionno-analiticheskiy byulleten. 2017. No. 11, pp. 168–176.
3. Вредное воздействие производственных факторов на здоровье рабочих в шахтах при добыче каменного угля. URL: https://www.trudcontrol.ru/press/publications/13875/vrednoe-vozdeystvie-proizvodstvennih-faktorov-na-zdorove-rabochih-v-shahtah-pri-dobiche-kamennogo-uglya (дата обращения: 25.08.2021).
4. Промышленный интернет вещей. URL: https://investmoscow.ru/media/3340535/03-промышленный-интернет-вещей.pdf (дата обращения: 25.08.2021).
5. Марисов Д.А., Зацепин А.Ю., Марин Е.А., Терлеев А.В., Ларионова М.Ю. Интернет вещей в нефтегазовой сфере: анализ технологии LoRaWAN и возможности прикладного применения // PROНЕФТЬ. Профессионально о нефти. 2019, №2(12). С.76-80.

УДК 338

ВЛИЯНИЕ ЦИФРОВИЗАЦИИ ОТНОШЕНИЙ НА БОРЬБУ С ЛЕГАЛИЗАЦИЕЙ (ОТМЫВАНИЕМ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЕМ ТЕРРОРИЗМА

Гилета Евгений Сергеевич[1,2], Разина Анастасия Дмитриевна[2]
[1] Санкт-Петербургский государственный экономический университет
канала Грибоедова наб., 30-32, Санкт-Петербург, 191023, Россия
[2] Межрегиональное управление Росфинмониторинга по Северо-Западному федеральному округу
Воскресенская наб., 10А, Санкт-Петербург, 191123, Россия
e-mails: dept.keb@unecon.ru, nadzor_szfo@fedsfm.ru, anast.razina2015@yandex.ru

Аннотация. Современные реалии обусловлены тем, что процессы всеобщей цифровизации способствуют активным изменениям структур и устройств экономической системы различных государств и характеризуются как положительными, так и отрицательными последствиями.

Ключевые слова: национальная безопасность; цифровая экономика; финансовый мониторинг; финансовая грамотность.

INFLUENCE OF DIGITALIZATION OF RELATIONS ON THE FIGHT AGAINST LEGALIZATION (LAUNDERING) OF PROCEEDS FROM CRIME, AND FINANCING OF TERRORISM

Gileta Evgeny[1,2], Razina Anastasia[2]
[1] Saint-Petersburg State University of Economics
30-32 Griboyedov Canal, St. Petersburg, 191023, Russia
[2] Interregional Department of Rosfinmonitoring for the Northwestern Federal District
10A Voskresenskaya Emb, St. Petersburg, 191123, Russia
e-mails: dept.keb@unecon.ru, nadzor_szfo@fedsfm.ru, anast.razina2015@yandex.ru

Abstract. Modern realities are due to the fact that the processes of universal digitalization contribute to active changes in the structures and devices of the economic system of various states and are characterized by both positive and negative consequences.

Keywords: national security; digital economy; financial monitoring; financial literacy.

Введение. Актуальность выбранной темы обусловлена стремительным внедрением цифровых технологий в деятельность всех без исключения хозяйствующих субъектов от микро- до мегаэкономического уровня. Ни один человек и ни одна страна мира не остались в стороне от данного процесса, что вывело в перечень приоритетных задач, стоящих перед мировым сообществом, противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Процесс формирования в мировой системе хозяйства нового (шестого) технологического уклада, в рамках теории экономических циклов Н. Кондратьева, неразрывно связан с коренной трансформацией отношений как на макро, так и на мега-экономическом уровнях.

Речь идет о дальнейшем развитии робототехники, систем искусственного интеллекта, глобальных информационных сетей, о расширении автоматизации производства, о прогрессе в области исследований мозга и технологий считывания его активности и т.д. [4]. При этом, основным фактором, оказывающим влияние на формирование ядра нового технологического уклада, в последнее десятилетние, стала цифровизация экономических отношений.

Термин «Цифровая экономика» взят нами из практики Всемирного банка и представляет собой систему экономических, социальных и культурных отношений, основанных на использовании информационно-коммуникационных технологий. Это новая парадигма ускоренного экономического развития [6].

Если взглянуть на становление правоотношений, регулирующих данную сферу в государствах ОДКБ, то в Российской Федерации, в декабре 2021 года исполнится 5 лет с начала реализации системной программы развития экономики нового технологического поколения, так называемой «цифровой экономики». В 2017 г. была принята Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы, а также Программа «Цифровая экономика Российской Федерации». 12 декабря 2017 года Постановлением Правительства Республики Казахстан № 827 была утверждена Государственная программа «Цифровой Казахстан», 02 февраля 2021 г. Постановлением Совета Министров Республики Беларусь от № 66 утверждена Государственная программа «Цифровое развитие Беларуси» и др.

Следует подчеркнуть, что стремительное распространение пандемии COVID-19 значительно ускорило внедрение цифровых технологий в деятельность хозяйствующих субъектов во всех странах мира. При этом важно отметить, что цифровизация отношений несет как позитивные, так и негативные последствия.

Если говорить о плюсах «цифровизации», то существенно повышается эффективность деятельности хозяйствующих субъектов микро- и макроэкономического уровня. Например, согласно прогнозу Аналитического центра при правительстве Российской Федерации, цифровизация экономики России позволит увеличить ВВП на 12% к 2030 году [8]. По информации Белорусского государственного университета, при успешном заимствовании зарубежных и создании собственных цифровых технологий потенциальный ежегодный экономический рост Беларуси может составить около 3% до 2050 года [9].

В исследовании «Fast Track to Future-Ready Performance» проведенном международной консалтинговой компанией Accenture (опрошены 1100 крупнейших компаний в 11 странах и 13 отраслях), результат цифровой трансформации компаний и появление новых гибких моделей ведения бизнеса к концу 2020 года оценивается в 5,4 трлн. долларов США, а к 2023 году количество так называемых компаний «Future-Ready» вырастет в промышленности (48%), страховании (42%) и банкинге (37%), эти отрасли выйдут в лидеры цифровизации[10].

Однако внедрение цифровых технологий имеет и серьезные негативные последствия. Так, на протяжении последних лет значительно активизировались субъекты теневого сектора экономических отношений. По данным Cybersecurity Ventures если потери мирового сообщества от киберпреступлений в 2015 году составляли 3 триллиона долларов США, то в 2025 году они достигнут 10,5 триллиона долларов США. В качестве потерь рассматривается: повреждение и уничтожение данных, кража денег, потеря производительности, кража интеллектуальной собственности, кража персональных данных, хищение, мошенничество, нарушение ведения бизнеса после кибератаки, восстановление и удаление взломанных данных и систем, и репутационный ущерб [2].

Процесс цифровизации отношений также оказал существенное влияние и на мировой «черный» рынок наркотиков. Согласно данным *Управления по наркотикам и преступности* ООН, торговые площадки для сбыта наркотиков появились в даркнете всего лет десять назад, однако, уже сегодня годовой оборот крупнейших из них, по самым скромным оценкам, составляет 315 млн долларов США. Хотя это лишь малая часть от совокупного оборота наркотиков, тенденция идет вверх: в период с начала 2010-х годов (2011 — середина 2017 года) по последние годы (середина 2017 — 2020 год) годовой объем продаж увеличился в четыре раза. Проникновение наркоторговли в социальные сети и на популярные электронные торговые площадки позволяет предположить, что доступность наркотиков растет и будет увеличиваться. Согласно прогнозам, к 2030 году численность людей, употребляющих наркотики, во всем мире вырастет на 11% только вследствие демографических изменений [1].

Не остается в стороне от общего криминального тренда и «бело-воротничковая» преступность. Так, Ассоциация сертифицированных исследователей мошенничества («Association of Certified Fraud Examiners» - ACFE) на протяжении нескольких десятков лет изучает опыт различных стран в области противодействия

мошенничеству и коррупции. В последнем отчете «Report To The Nations. 2020 Global Study On Occupational Fraud And Abuse» (2504 преступления, 125 стран) она оценивает общие потери от данного вида преступлений в 3,6 млрд долларов США в год. Эксперты ACFE оценивают средний убыток компании от мошеннических действий собственников/ руководителей оценивается в 600 000 долларов США в год (20% преступлений), а ежегодные потери компании – 5% своего дохода [7].

Важно отметить, что наибольших успехов в области противодействия «бело-воротничковой» преступности добились Сингапур и Южная Корея. Источник успехов этих стран – активное внедрение информационных технологий и построение информационного общества.

Так, например, в Сингапуре, с 2003 года, реализуется система «электронного правительства», в рамках которого, гражданам и гостям страны с помощью современных информационных технологий оказывается более 1600 услуг. За 30 лет, в том числе с помощью «высоких технологий», Lee Kuan Yew смог вывести Сингапур «из третьего мира — в первый».

Вызывает интерес опыт Южной Кореи, где в конце 90-х годов XX в. начала свою реализацию программа борьбы с коррупцией, получившая название - «OPEN». Опыт Южной Кореи нашел свое отражение в материалах IX Международной антикоррупционной конференции, проходившей с 10 по 15 октября 1999 года в Дурбане (Южная Африка), на которой Мэр Сеула Гох Кун сделал доклад о реализации программы «OPEN» [9].

Успехи Сингапура и Южной Кореи в нейтрализации коррупционной угрозы подтверждаются стабильностью и высоким значением Индекса восприятия коррупции «Transparency International» в этих государствах [5].

Таким образом, можно утверждать, что в теневом секторе моровой экономики ежегодно аккумулируются сотни миллиардов долларов и перед всеми государствами, без исключения, стоит важнейшая задача – поставить надежный заслон на пути легализации доходов, полученных преступным путем.

Несомненно, знания в сфере финансовой безопасности, в условиях стремительного внедрения цифровых технологий, с каждым днём становятся обязательным атрибутом культуры жителя земного шара. Так как финансы окружают нас повсюду, базовые правила их безопасного использования необходимо формировать начиная со школьной скамьи.

Например, в Российской Федерации обязательное преподавание финансовой грамотности закреплено в новых федеральных государственных образовательных стандартах начального и основного общего образования. Уже сегодня, благодаря совместной работе Министерства просвещения, Министерства финансов и Банка России, 86% российских школ включили финансовую грамотность в свои учебные планы, а в каждой пятой школе это обязательный урок [11].

Так, директор Федеральной службы по финансовому мониторингу Ю.А. Чиханчин отмечает, что сегодня ведется активная работа по повышению финансовой грамотности населения совместно с Центральным банком и Министерством финансов. Повышение уровня информированности граждан о потенциальных финансовых угрозах является одним из приоритетных направлений работы Международного учебно-методического центра Росфинмониторинга, где происходит обучение иностранных коллег, в первую очередь из стран Евразийской группы и СНГ: Белоруссии, Индии, Казахстана, Китая, Кыргызстана, Таджикистана, Туркменистана, Узбекистана (40 учебных заведений из 7 стран)[3].

Таким образом, повышение финансовой грамотности становится исходным пунктом в сфере обеспечения финансовой безопасности личности, общества и государства.

Для эффективного функционирования национальной экономики в частности и мировой экономики в целом необходимы профессиональные кадры. Так, финансовая безопасность помимо личных финансов, включает меры защиты интересов хозяйствующих субъектов как микро-, так и макроэкономического уровня.

Для эффективного развития национальной экономики, в частности и мировой экономики в целом необходимы профессиональные кадры и решению этой задачи, на наш взгляд, будет способствовать Международная олимпиада по финансовой безопасности, проводимая при поддержке Президента Российской Федерации к 20-летию Финансовой разведки России Росфинмониторингом совместно с Минпросвещения России, Минобрнауки России, образовательными и научными организациями - участниками международного сетевого института в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Первый этап олимпиады успешно прошел в мае 2021 года на площадках образовательных и научных центров - участников международного сетевого института ПОД/ФТ из Беларуси, Казахстана, Кыргызстана, России, Таджикистана, Туркменистана, Узбекистана. В первом этапе приняло участие более 3 тыс. школьников и 4 тыс. студентов. Победители олимпиады будут определены в ходе второго этапа, который запланирован к проведению в октябре 2021 года на территории образовательного центра «Сириус».

Заключение. Не вызывает сомнений, что работа по нейтрализации ПОД/ФТ должна быть системной и включать как карательные меры (срок заключения под стражей, штрафы и т.д.), так и превентивные. По мнению авторов, важнейшей превентивной мерой в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, должна стать работа национальных органов финансового мониторинга, совместно с образовательными учреждениями, с нынешними школьниками и студентами. С одной стороны, через 5-10 лет они будут являться активными производителями ВВП своих государств, с другой стороны, те, кто придёт на работу в органы финансового мониторинга, станут защитниками своих национальных экономик, в частности и мирового сообщества в целом, что позволит поставить надёжный заслон криминальному капиталу на пути из теневого в легальный сектор экономики.

СПИСОК ЛИТЕРАТУРЫ

1. Всемирный доклад о наркотиках за 2021 год. Управление по наркотикам и преступности ООН. – 2021.
2. Гилевская М. Анализ антикоррупционной программы Сеула «OPEN» // Проблемы преступности: традиционные и нетрадиционные подходы. - М.: Российская криминологическая ассоциация. 2003. С. 247–254.
3. Журнал «Финансовая безопасность» №30/2021 [Электронный источник] https://www.fedsfm.ru/content/files/%D0%B6%D1%83%D1%80%D0%BD%D0%B0%D0%BB/2021/%D0%B6%D1%83%D1%80%D0%BD%D0%B0%D0%BB%20%D0%BC%D0%B0%D0%B9%202021.pdf (дата обращения: 30.08.2021).
4. Кондратьев Н.Д., Яковец Ю.В., Абалкин Л.И. Большие циклы конъюнктуры и теория предвиденья. Избранные труды. – М.: Экономика, 2002. — 550 с.
5. Центр антикоррупционных исследований и инициатив «Трансперенси Интернешнл - Р». Индекс восприятия коррупции 2020.
6. Цифровые дивиденды: доклад о мировом развитии – 2016. Вашингтон: Всемирный банк, 2016.
7. Report To The Nations On Occupational Fraud And Abuse 2014 Global Fraud Study. Association of Certified Fraud Examiners, Inc. 2014. Report To The Nations On Occupational Fraud And Abuse 2020 Global Fraud Study. Association of Certified Fraud Examiners, Inc. 2020.
8. https://ac.gov.ru/news/page/cifrovizacia-ekonomiki-mozet-obespecit-znacitelnyj-rost-vvp-26952 (дата обращения: 30.08.2021).
9. https://rce.by/articles/article36.php (дата обращения: 30.08.2021).
10. https://www.accenture.com/_acnmedia/PDF-149/Accenture-Fast-Track-Insurance-Report-3-31-21-Final.pdf (дата обращения: 30.08.2021).
11. https://www.cbr.ru/press/event/?id=11018 (дата обращения: 30.08.2021).
12. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/# (дата обращения: 30.08.2021).

УДК 004.056

КИБЕРПРОТИВОСТОЯНИЕ МИРОВЫХ ДЕРЖАВ: АКТУАЛЬНЫЕ УГРОЗЫ

Графов Александр Александрович
Санкт-Петербургский государственный экономический университет
канала Грибоедова наб., 30-32, Санкт-Петербург, 191023, Россия
e-mail: grafov_aa@mail.ru

Аннотация. В статье рассматриваются проблемы современных аспектов кибербезопасности в мире в контексте глобальных угроз. Предлагается видение по комплексному изучению элементов глобальных угроз в киберпространстве и Интернет-сети в мире, и рассматривается важность разработки и осуществления максимально эффективных механизмов по противодействию киберугрозам.

Ключевые слова: кибербезопасность; глобальные угрозы в мире; защита системы кибербезопасности; надёжность системы киберпространства; эффективность инфраструктур ИКТ.

CYBER-CONFRONTATION OF THE WORLD POWERS: CURRENT THREATS

Grafov Aleksandr
Saint-Petersburg State University of Economics
30-32 Griboyedov Canal, St. Petersburg, 191023, Russia
e-mail: grafov_aa@mail.ru

Abstract. The article deals with the problems of modern aspects of cybersecurity in the world in the context of global threats. A vision is proposed for a comprehensive study of the elements of global threats in the cyber space and the Internet network in the world, and the importance of developing and implementing the most effective mechanisms for countering cyber threats is considered.

Keywords: cybersecurity; global threats in the world; protection of the cybersecurity system; reliability of the cyberspace system; efficiency of ICT-infrastructures.

Введение. В условиях глобальных угроз обеспечение безопасности в мире требует координации и урегулирования многих политических и экономических вопросов. В частности, это очаги гражданских, межэтнических конфликтов и войн, продовольственные угрозы, негативные последствия изменения климата, загрязнение окружающей среды, истощение природных ресурсов и замедление их повторного возобновления, необходимость обеспечения экономного режима энергоносителями, развития зеленой экономики, рационального использования природных ресурсов и человеческого потенциала, и прочее. Однако среди всех компонентов обеспечения безопасности появился новый и одновременно сложный элемент безопасности – кибербезопасность [1].

Кибербезопасность – это реализация мер по защите систем, сетей и программных приложений от цифровых атак. Проблемы кибербезопасности осложнены тем, что в пространстве кибербезопасности осуществляются хакерские атаки на государственные органы, международные структуры, идёт киберпротивостояние между отдельными государствами, и проч. Для противостояния этого вызова необходимо изучение основных причин кибер-преступлений, правонарушений в киберпространстве, взлома компьютерной сети, распространения вредоносных программ и вирусов с дальнейшей разработкой адекватных механизмов и государственной политики по минимизации их влияния. Необходимо расширение международного сотрудничества и взаимодействия кибердержав по обеспечению превентивных и неотложных мер по противодействию киберпреступлениям. Требуется совершенствование системы управления по обеспечению кибербезопасности и активного применения новых технологий в данной сфере. Актуальным становится обновление международных механизмов и критерий по противодействию с киберпреступниками, хакерами и киберзлоумышленниками.

Особо нуждаются в системном изучении причины киберпреступлений, так как киберпреступность в современном мире объявлена глобальной проблемой, где больше всего отмечены такие правонарушения, как мошенничество, неправомерный доступ к компьютерной информации, распространение вредоносных программ. Для расследования преступлений, совершенных в киберпространстве, требуются как технические, так и теоретические познания. На международном уровне следует рассматривать такое понятие как кибервойна.

Кибервойна [3] – это использование цифровых атак - таких как компьютерные вирусы и взломы - одной страной, чтобы разрушить жизненно необходимые компьютерные системы другой с целью причинения ущерба, разрушения и даже смерти. В перспективе возможны такие сценарии, в которых в будущих войнах хакеры будут использовать компьютерный код для атаки на инфраструктуру противника, сражаясь вместе с войсками, используя обычное оружие и ракеты.

Почти каждая система, которую мы используем, каким-то образом связана с компьютерами, что означает, что практически каждый аспект нашей жизни может быть уязвим для кибервойны в какой-то момент [2].

Правительства стран осознают, что современные общества настолько зависят от компьютерных систем, что они могут управлять всем: от финансовых услуг до транспортных сетей, соответственно использование хакеров, вооруженных вирусами или другими инструментами для отключения этих систем, может быть столь же эффективным и разрушительным, как и традиционная военная кампания с использованием вооруженных войск.

Новые и более сложные международные угрозы в лице кибер-террористов, хакеров и злоумышленников нуждаются в построении сильной и системной конструкции по защите киберпространства, чтобы обеспечить полноценную и эффективную кибербезопасность в мире.

Заключение. Кибербезопасность, таким образом, обеспечивает защищенность киберпространства путем сохранения конфиденциальности, целостности и доступности информации в нем, где есть сетевая безопасность, бесперебойные и безопасные передачи Интернет-ресурсов, и прочих системообразующих компонентов. При эффективности системы кибербезопасности минимизируется возможность киберпреступников по проникновению их в киберпространство. Формирование элементов киберпреступлений в киберпространстве обуславливает более четкий механизм и средства по их нейтрализации и ликвидации, чтобы уменьшить убытки и причиненный ущерб.

Вопрос обеспечения кибербезопасности мира требует разработки и осуществления более эффективных механизмов функционирования и обеспечения работы киберпространства, повышения надежности основных механизмов и компонентов глобальной Интернет-сети и прочих устройств, комплексного и системного подхода в определении методических принципов и инструментариев формирования государственной политики по кибербезопасности в нынешних условиях, и т.д.

СПИСОК ЛИТЕРАТУРЫ

1. Джаббарова К.Ф. Современные аспекты кибербезопасности в мире в контексте глобальных угроз//АНИ: экономика и управление – 2017 - №2(19) – С. 323 – 326.
2. Источник подтвердил попытки иностранных спецслужб взломать системы управления инфраструктурой РФ [Режим доступа] URL: https://www.interfax.ru/russia/665518 (Дата обращения 14.07.2019).
3. Кибервойна России [Режим доступа] URL: https://en.wikipedia.org/wiki/Cyberwarfare_by_Russia (Дата обращения 09.09.2021).

УДК 331.1; 339.9

ВЛИЯНИЯ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ НА ПОДГОТОВКУ СПЕЦИАЛИСТОВ В СФЕРЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Дронов Роман Владимирович[1], Разина Анастасия Дмитриевна[2]
[1] Санкт-Петербургский государственный экономический университет
канала Грибоедова наб., 30-32, Санкт-Петербург, 191023, Россия
[2] Межрегиональное управление Росфинмониторинга по Северо-Западному федеральному округу
Воскресенская наб., 10А, Санкт-Петербург, 191123, Россия
e-mails: dept.keb@unecon.ru, nadzor_szfo@fedsfm.ru, anast.razina2015@yandex.ru

Аннотация. Авторы исследуют влияние процесса цифровизации национальной экономики на подготовку студентов в рамках Федерального государственного образовательного стандарта высшего образования по специальности 38.05.01 «Экономическая безопасность».

Ключевые слова: безопасность; специалист; цифровизация; экономическая безопасность; национальная безопасность.

THE INFLUENCE OF THE DIGITALIZATION OF THE ECONOMY FOR TRAINING SPECIALISTS IN THE FIELD OF ECONOMIC SECURITY

Dronov Roman[1], Razina Anastasia[2]
[1] Saint-Petersburg State University of Economics
30-32 Griboyedov Canal, St. Petersburg, 191023, Russia
[2] Interregional Department of Rosfinmonitoring for the Northwestern Federal District
10A Voskresenskaya Emb, St. Petersburg, 191123, Russia
e-mails: dept.keb@unecon.ru, nadzor_szfo@fedsfm.ru, anast.razina2015@yandex.ru

Abstract. The authors investigate the impact of the process of digitalization of the national economy on the training of students within the framework of the Federal State Educational Standard of Higher Education in the specialty 38.05.01 "Economic Security".

Keywords: security; specialist; digitalization; economic security; national security.

Стремительное распространение COVID-19 способствовало активизации процесса реализации поставленных Президентом России целей в сфере внедрения цифровых технологий в деятельность хозяйствующих субъектов как на макро, так и микроэкономическом уровне в 2020 и 2021 гг., что отразилось и на профессиональной деятельности выпускников программы ФГОС ВО по специальности 38.05.01 «Экономическая безопасность», утвержденной Приказом Минобрнауки России № 20 от 16 января 2017.

Следует отметить, что Санкт-Петербургский государственный экономический университет с 2014 г. осуществляет подготовку студентов по специализации «Экономико-правовое обеспечение экономической безопасности» в рамках следующих видов профессиональной деятельности: расчетно-экономическая; проектно-экономическая; информационно-аналитическая; организационно-управленческая.

Вручение диплома «специалиста» подразумевает, что выпускник программы успешно освоил общекультурные, общепрофессиональные, профессиональные, профессионально-специализированные компетенции. В числе ключевых общекультурных компетенций, на наш взгляд, можно назвать следующие: способность понимать и анализировать мировоззренческие, социально и личностно значимые философские проблемы; способность к логическому мышлению, аргументированно и ясно строить устную и письменную речь, вести полемику и дискуссии и т.д. Среди основных профессиональных компетенций можно выделить такие как: способность на основе типовых методик и действующей нормативно-правовой базы рассчитывать экономические показатели, характеризующие деятельность хозяйствующих субъектов; осуществлять планово-отчетную работу организации, разработку проектных решений, разделов текущих и перспективных планов экономического развития организации, бизнес-планов, смет, учетно-отчетной документации, нормативов затрат и соответствующих предложений по реализации разработанных проектов, планов, программ; анализировать показатели финансовой и хозяйственной деятельности государственных органов и учреждений различных форм собственности и др.

Опыт профессиональной деятельности наших выпускников показывает, что освоение широкого комплекса компетенций позволяет не только сформировать гармонично развитую личность с устойчивым «иммунитетом» к совершению противоправных действий, но и успешно работать на четырех основных направлениях обеспечения безопасности хозяйствующих субъектов, которые условно можно назвать: «Кадры» (подбор, расстановка и увольнение кадров, внутренняя безопасность организации и пр.), «Касса» (финансово-хозяйственная деятельность, бухгалтерский учет и пр.), «Контрагенты» (подбор и анализ деятельности деловых партнеров и пр.), «Конкуренты» (анализ конкурентной среды).

Внедрение высоких технологий в нашу повседневную жизнь, ускоряемые COVID-19, безусловно, способствуют глобальному прогрессу – продвижению к шестому технологическому укладу, в рамках теории длинных волн. Здесь речь идет о дальнейшем развитии робототехники, систем искусственного интеллекта, глобальных информационных сетей, о расширении автоматизации производства, о прогрессе в области исследований мозга и технологий считывания его активности и т.д. [3]

Хотелось бы отметить, что мы разделяем точку зрения А. Волож, сооснователя, генерального директора Группы компаний «Яндекс», высказанную на Петербургском международном экономическом форуме – 2019: «…искусственный интеллект не меняет самого человека, а забирает на себя рутинные функции… Что-то рутинное становится гораздо более эффективным, когда это делает машина...» [4].

Кроме того, высокие технологии оказывают существенное влияние на профессиональную деятельность наших выпускников. Так, например, в работе на направлении «Касса» не один десяток лет используются программные продукты фирмы «1С» (1С:Предприятие, 1С:Бухгалтерия, 1С:Консалтинг и пр.), а Корпорация «Парус» успешно автоматизирует процессы в области финансово-хозяйственной деятельности, управления НИОКР и производством. Однако на рынок выходят новые игроки. Уже сегодня можно воспользоваться услугами ПАО «ВТБ», запустившего дистанционный сервис для малого и среднего бизнеса «Цифра», и компании «СБЕР», открывшей онлайн-сервис для индивидуальных предпринимателей «Бухгалтерия для ИП», и т.д.

Если рассматривать работу по направлениям «Контрагенты» и «Конкуренты», то, как показывает практика, наиболее популярными в сфере безопасности являются программы «Глобас» от компании «Credinform» и «СПАРК» от компании «Интерфакс». Следовательно, можно с уверенностью сказать, что значительная часть профессиональных задач, стоящих перед специалистом в области обеспечения экономической безопасности, уже попала под «оцифровку» и успешно решается с помощью высоких технологий. Так большинство профессиональных компетенции ФГОС ВО по специальности 38.05.01 уходят в цифровую сферу и на первый план в работе наших выпускников выходит то, что не поддается процессу цифровизации – «Кадровое» направление.

Отечественный и зарубежный опыт обеспечения экономической безопасности хозяйствующих субъектов показывает, что одновременно основным источником процветания компании и основной угрозой является свой собственный сотрудник.

На наш взгляд, вызывает интерес мнение А. Мордашова, председателя совета директоров ПАО «Северсталь», прозвучавшее на ПМЭФ – 2019, относительно современных требований представителей бизнеса к трудовым ресурсам: «… возрастает значимость «soft skills»: анализировать причины и следствия, способность работать с людьми, открытость мышления, способность воспринимать новые идеи, правду, меняться. Эти способности – фактор успеха. Кто сможет создать возможности для раскрытия творческого потенциала сотрудников будет победителем в конкурентной гонке» [4].

Таким образом, уже сегодня, в условиях жёсткой рыночной конкуренции, усугубляемой COVID-19, существует значительный спрос со стороны работодателей на творческого работника. Как показывает практика, если в организации есть те, кто творит, то есть и те, кто вытворяет. Именно они находятся в зоне особого внимания сотрудников службы экономической безопасности.

Угроза номер один для хозяйствующего субъекта – коррупция и внутрикорпоративное мошенничество давно и подробно исследуется такими компаниями как KPMG, E&Y и др. Последнее исследование Ассоциации сертифицированных специалистов по расследованию мошенничества – ACFE охватило125 стран за период с января 2018 года по сентябрь 2019 года. Оно выявило 2504 преступлений с общим ущербом 3,6 млрд. долларов США. Важно отметить, что ежегодные потери организаций оцениваются в 5% от их дохода, а главную угрозу для организации представляют собственные владельцы и/или топ менеджеры – на них приходится 20% преступлений. Более подробно ознакомиться с угрозой коррупции и внутрикорпоративным мошенничеством можно в отчете ACFE «Report to the Nations on occupational fraud and abuse 2020 Global Fraud Study».

С точки зрения авторов на первый план в работе современного специалиста в сфере экономической безопасности выходит работа с человеческим фактором. Если говорить о мере цифровизации профессиональной деятельности, то на место уходящих в цифру профессиональных компетенций будут приходить современные общекультурные компетенции, а именно: выполнение профессиональных задач в соответствии с нормами морали, профессиональной этики и служебного этикета; способность работать в коллективе, толерантно воспринимая социальные, культурные, конфессиональные и иные различия, предупреждать и конструктивно разрешать конфликтные ситуации в процессе профессиональной деятельности; проявление психологической устойчивости в сложных и экстремальных условиях и т.д. Следовательно, в условиях цифровизации отношений, для выпускника ФГОС ВО по специальности 38.05.01 «Экономическая безопасность» происходит трансформация общекультурных компетенций в профессиональные. Данный процесс должен найти свое отражение в новой редакции образовательного стандарта.

Активное внедрение высоких технологий в нашу повседневную жизнь и продвижение к новому технологическому укладу оказывают существенное влияние на рынок трудовых ресурсов и в этих условиях спрос на качественных специалистов в области обеспечения экономической безопасности хозяйствующих субъектов будет стабильно высок.

СПИСОК ЛИТЕРАТУРЫ

1. Распоряжение Правительства Российской Федерации от 28 июля 2017 г. № 1632-р Программа «Цифровая экономика Российской Федерации». [Электронный ресурс] URL: http://government.ru/docs/28653/ (дата обращения: 30.07.2021).
2. Глазьев С.Ю. О прогнозах динамики мировой экономики в условиях пандемии COVID-19 и возможных стабилизационных мерах в рамках ЕАЭС [Электронный ресурс] URL: http://eec.eaeunion.org/ru/covid-19/Documents/1111.pdf (дата обращения: 30.07.2021).
3. Кондратьев Н.Д., Яковец Ю.В., Абалкин Л.И. Большие циклы конъюнктуры и теория предвиденья. Избранные труды. – М.: Экономика, 2002. — 550 с.
4. «Мы не можем тупо копировать Google». О чем говорили Волож, Мордашов и Тиньков на технологической сессии ПМЭФ [Электронный ресурс] URL: https://www.forbes.ru/milliardery/377295-volozh-mordashov-i-tinkov-o-tehnologiyah-i-igre-na-operezhenie-pryamaya (дата обращения: 30.07.2021).
5. Coronavirus: Europe plans full border closure in virus battle // BBC News [Электронный ресурс] URL: https://www.bbc.com/news/world-europe-51918596 (дата обращения: 30.07.2021).

УДК 338

ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОВЕДЕНИИ ЭКСПЕРТИЗЫ НОРМАТИВНО-ПРАВОВЫХ АКТОВ

Елкин Станислав Евгеньевич
Санкт-Петербургский государственный экономический университет
канала Грибоедова наб., 30-32, Санкт-Петербург, 191023, Россия
e-mail: elkin-se@yandex.ru

Аннотация. В статье рассмотрен процесс информационного обеспечения механизма экспертизы нормативно-правовых актов с позиций экономического и юридического подходов. Представлены проблемы оценки эффективности законодательства в экономической сфере, развитие механизмов анализа и оценки последствий нормативных правовых актов. На основе проведенного исследования предлагаются варианты использования современных подходов к применению права в сфере экономических и общественных отношений.

Ключевые слова: законодательство в сфере экспертизы нормативных правовых актов; экономический анализ нормативных актов; экономическая теория права.

LEGAL ASPECTS OF ENSURING INFORMATION SECURITY DURING THE EXAMINATION OF REGULATORY LEGAL ACTS

Elkin Stanislav
Saint-Petersburg State University of Economics
30-32 Griboyedov Canal, St. Petersburg, 191023, Russia
e-mail: elkin-se@yandex.ru

Abstract. The article considers the process of forming a mechanism for the examination of normative legal acts from the standpoint of economic and legal approaches. The problems of evaluating the effectiveness of legislation in the economic sphere are presented. The development of mechanisms for analyzing and evaluating the consequences of regulatory legal acts is presented. Based on the conducted research, measures based on new approaches to the application of law in the field of economic and social relations are proposed.

Keywords: legislation in the field of examination of normative legal acts; economic analysis of normative acts; economic theory of law.

Введение. Безопасность устойчивого развития экономики и общественной сферы определяет необходимость эффективного правового регулирования. Одним из требующих внимания вопросов является механизм анализа и оценки применения нормативных правовых актов. Проблематика экономического анализа права актуализируется необходимостью создания правового обеспечения функционирования рынков. Экономическая теория права достаточно близка к неоинституционализму по своему предмету. Это объясняется тем, что законы и другие правовые нормы представляют собой частный случай необходимых к исполнению правил, т.е. институтов. Используемые в ней методы анализа законов позаимствованы преимущественно из неоклассической экономической теории. Основное противоречие при постановке вопроса об эффективности права заключается в ограничениях в получении экономически полезных результатов. Понятие эффективности закона в рамках позитивистского подхода интерпретируется как фактическая реализация сформулированной законодателем цели правового предписания. Для принятой ранее доктрины было характерно «…понимание эффективности правовых норм как соотношения между действительным результатом и целью, а также между достигнутым результатом и применяемым для его достижения средствами. Цель правовой нормы – эталон оценки ее эффективности» [1].

Для юриспруденции в значительной мере был характерен так называемый «юридический позитивизм», суть которого заключается в том, что любое решение законодателя воспринимается как данность, фактически не подлежащая обсуждению с точки зрения его социальных или экономических функций.

Экономическому стилю мышления, напротив, свойственна альтернативность, стремление к сопоставлению различных вариантов достижения целей, сравнению результатов и издержек и т.п. Тем самым закон не воспринимается как «объективная реальность», он есть не более чем один из возможных альтернативных путей достижения определенной цели [2].

Многие современные авторы считают, что «…цель нормативного правового акта могла бы формулироваться через понятие направленности на социальный эффект, который должен быть достигнут при реализации правового предписания» [3]. Характеризуя экономический и юридический подход к анализу правовых норм отметим, что их различия во многом объясняют критику экономического анализа права. Достаточно сказать, что базовой предпосылкой применения экономического подхода к изучению правовых актов является допущение того, что «…люди, действующие в рамках правовой системы, совершают действия, максимизирующие их функции полезности» [4].

Несомненная актуальность экономико-правовых исследований определяется отношением к праву как инструменту системы управления на основе оценки правовых предписаний с точки зрения их влияния на экономику и общество. В свою очередь, экономические науки обогащаются универсальным инструментом управления и участвуют в формировании нормативного эквивалента экономических отношений. Результативность экономико-правового анализа одних и тех же общественных явлений или правовых актов обеспечивается повышением эффективности управления общественными процессами [1].

В целом следует согласиться с мнением Хабриевой Т.Я. о том, что «…расхождение позиций экономистов и юристов в общем подходе к проблеме изучения эффективности правовых норм заключается в том, что экономисты базируют свою оценку на критерии полезности, который хотя и исходит из сравнения полезностей (например, строительство автострады вызывает протест жителей, по территории участков которых проходит новая дорога, однако в строительстве проявляют заинтересованность жители близлежащих территорий), но не учитывает другие аспекты, влияющие на регулирование избранного круга отношений. В свою очередь, методика определения эффективности права, используемая в юриспруденции, позволяет обратиться к более широкому кругу критериев оценки действия правовой нормы, в основе которых лежит принцип справедливости, и включает систему оценки распределения полученных благ. Таким образом, существует потенциальная возможность более точного измерения эффективности правовых норм» [6].

Вместе с тем, наука еще недостаточно продвинулась не только в общих вопросах методологии, но и в разработке конкретных методик проведения совместных исследований. Нельзя забывать и о специфичности понятийно-категориального аппарата правовой и экономической наук. Соединение методов права и экономики,

предполагающее необходимость комплексных исследовательских подходов, общепризнано проявляется в теме эффективности права.

Основные направления исследования методологии экономико-правовых исследований определяются необходимостью выявления факторов, определяющих степень позитивного влияния нормативно-правовых актов на социально-экономические процессы в обществе. Необходимо завершение построения модели экономического обоснования в законотворческом процессе. В целом речь идет о разработке механизма прогнозирования социально-экономических последствий правовых новаций.

Принципиально важным выводом из исследований, осуществляемых в рамках экономического подхода к праву, является доказанная полезность экономического анализа для осуществления правовых реформ, улучшения как отдельных нормативных актов, так и всей системы, обеспечивающей их проведение в жизнь, т.е. продуктивность нормативного экономического анализа права [6].

В последние десятилетия интенсивно развиваются теории регуляции, институциональной экономики, экономического анализа права и другие, позволяющие обнаружить сложные взаимосвязи этих явлений. С точки зрения экономической теории нормативные правовые акты оцениваются с позиций экономической эффективности. Выделяются различные критерии данной оценки: критерий эффективности по Парето, критерий Калдора-Хикса, критерий максимизации богатства, критерий Ролза и др [8].

Важным этапом повышения качества правового регулирования с точки зрения определения экономической эффективности права стало внедрение в России системы оценки регулирующего воздействия. В практике отдельных стран деятельность по изучению, контролю или оценке эффективности национального законодательства именуется по-разному. Несмотря на имеющиеся различия, в большинстве случаев речь идет о системе оценки, анализа и прогноза состояния, динамики законодательства и практики его применения с целью выявления их соответствия планируемому результату правового регулирования, а также ожиданиям участников законодательного процесса, должностных лиц различных органов власти, институтов гражданского общества [9].

В зарубежном законодательстве отсутствуют общие для всех государств методики, которые применялись бы для проведения оценки регулирующего воздействия. Методика проведения этой процедуры значительно различается в государствах и зависит от тех целей, на которые направлено проведение рассматриваемой процедуры. В Российской Федерации целью оценки регулирующего воздействия является выявление положений, вводящих избыточные административные и иные ограничения и обязанности для субъектов предпринимательской деятельности, а также способствующих возникновению необоснованных расходов как субъектов предпринимательской деятельности, так и бюджетов всех уровней бюджетной системы.

Современный этап развития оценки регулирующего воздействия в Российской Федерации характеризуется активной законодательной деятельностью ее субъектов в данном направлении. Это обусловлено установленной необходимостью закрепления процедуры оценки регулирующего воздействия и экспертизы действующих нормативных правовых актов в отношении органов государственной власти субъектов Российской Федерации и органов местного самоуправления [10].

В случае невозможности оценить количественные показатели целесообразно указать на возможную проблему. В связи с этим уместно сослаться на один из документов Организации экономического сотрудничества и развития, где говорится, что «…самым важным вкладом анализа регулирующего воздействия в обеспечение качества принимаемых решений является не точность проводимых при этом расчетов, а процесс анализа как таковой: рассмотрение возможных вариантов, осмысление реальных эффектов воздействия регулирования и исследование сделанных гипотез» [1].

Немаловажным элементом проведения оценки регулирующего воздействия является правовой мониторинг, позволяющий оценить соответствие последствий нормативного регулирования его целям, заложенным при принятии правового предписания, а также качество процедур оценки регулирующего воздействия, проведенных на стадии разработки и принятия нормативных правовых актов. Институт правового мониторинга можно использовать при оценивании последствий реализации нормативных правовых актов, что позволит повысить их качество и эффективность государственного и муниципального управления.

В законодательстве Российской Федерации широко используется понятие «экспертиза» нормативных правовых актов. В нормативных правовых актах различного уровня предусматривается обязательное проведение экспертизы градостроительной документации, землеустроительной экспертизы, экологической экспертизы и др. Разработан большой массив ведомственных нормативных правовых актов, часть из которых содержит методики проведения конкретного вида экспертизы [1]. В практику экспертной деятельности введены институты оценки регулирующего воздействия и оценки фактического воздействия нормативных правовых актов на регулируемые правоотношения, которые и по форме, и по содержанию, и по порядку их проведения являются видами экономико-правовой экспертизы [1].

Итоги правового воздействия позволяют обнаружить типичные последствия нормативных правовых актов, которые условно различаются по степени соизмерения с целями и задачами и средствами регулированию на планируемые, расчетные, прогнозируемые, возможные, непредвиденные и т.д.

Объективная оценка последствий актов не может быть окончательной, она получает продолжение в юридических действиях и решениях. Это могут быть изменения или меры ответственности для виновных лиц. Должностные лица и служащие несут ответственность по административному, трудовому, гражданскому и

уголовному законодательству. Важно фиксировать именно невыполнение или плохое выполнение правовых актов основанием для привлечения работников к ответственности [1].

Заключение. Основными требованиями к таким разработкам должны являться требования разумной достаточности установления таких критериев, которые позволяли бы оценивать позитивные и негативные последствия их принятия, а с другой стороны - не приводили бы к избыточным ограничениям, сдерживающим развитие конкретной области экономической деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Дементьев А.Н. Экономико-правовые аспекты теории экспертизы правовых актов в сфере реализации промышленной политики в Российской Федерации // Грант РФФИ № 17-03-00181.
2. Карапетов А.Г. Экономический анализ права / А.Г. Карапетов. М.: Статут, 2016. 528 с.
3. Нанба С.Б. Экономическое измерение права // «Адвокат», 2013, № 12.
4. Правовой мониторинг: Научно-практическое пособие / Под ред. Ю.А. Тихомирова, Д.Б. Горохова. М.: Юриспруденция, 2009. С. 86.
5. Правовые акты: оценка последствий: научно-практическое пособие / отв. ред. Ю.А. Тихомиров, «Юриспруденция», 2011, С. 3, 125.
6. Самощенко И.С., Никитинский В.И. Некоторые теоретические вопросы изучения эффективности норм. Варна, 1970. С. 2-10.
7. Степин В.С., Горохов В.Г., Розов М.А. Философия науки и техники. М., 1995
8. Тамбовцев В.Л. Право и экономическая теория: Учеб. пособие, - М.: ИНФРА-М, 2005. - 224 с, - (Учебники экономического факультета МГУ им. М.В. Ломоносова). С. 11-21
9. Указ Президента РФ от 07.05.2012 № 601 «Об основных направлениях совершенствования системы государственного управления» // Российская газета. 09.05.2012.
10. Хабриева Т.Я. Экономико-правовой анализ: методологический подход // «Журнал российского права», 2010, № 12, С.5-26.
11. Эффективность законодательства в экономической сфере / Отв. ред. Ю.А. Тихомиров. М., 2010. С. 133.

УДК 007.2

НЕКОТОРЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ «УМНЫЙ ДОМ»

Емельянов Александр Александрович[1], Завадская Ольга Ивановна[2]
[1] Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
[2] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: S1_Alex2000@mail.ru, zav_olia_com@mail.ru

Аннотация. Рассмотрены общие концепции построения систем «умный дом». Выделены угрозы безопасности, возникающие при эксплуатации данного рода систем. Описана модульная схема аппаратно-программного комплекса для повышения уровня безопасности работы рассматриваемых систем.

Ключевые слова: автоматизация; умный дом; безопасность.

SOME ASPECTS OF INFORMATION SECURITY OF THE SMART HOUSE SYSTEMS

Emelyanov Alexandr[1], Zavadskaya Olga[2]
[1] Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
[2] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: S1_Alex2000@mail.ru, zav_olia_com@mail.ru

Abstract. In this work, various aspects of the Smart House system are considered, security threats of such systems are highlighted, and a modular structure of hardware-software complex increasing the security level of the systems is proposed.

Keywords: automation; smart house; security.

В рамках современной терминологии под подходом «умный дом» подразумевается инфраструктура, включающая в себя вариативные системы сенсоров, исполнительные механизмы, блоки обработки и хранения данных. Подобные решения позволяют обеспечивать необходимые условия для комфортной жизни, сокращать расходы на электроснабжение [1], осуществлять контроль и устранение различных угроз – таких, как возгорание/затопление/проникновение злоумышленников и т.д. Существует множество подходов, воплощающих концепцию «умного дома». От простейших, осуществляющих автоматизированный контроль за микроклиматом внутри помещений – до интеллектуальных систем, реализующих голосовое управление, использующих широкий спектр устройств для взаимодействия (смартфоны, планшеты, ноутбуки, смарт-часы, фитнес-трекеры и пр.)

Однако, чем большей сложностью обладает система, тем большее количество уязвимых элементов имеется в её составе. Одним из важных аспектов работы вышеупомянутых систем является использование радиоканала для передачи данных от сенсорной системы к устройствам обработки и хранения информации, а также осуществление управляющих воздействий с помощью электромеханических блоков. В качестве примера можно привести передачу данных от датчиков температуры и управление устройствами обогрева. В случае, если

входная информация будет искажена (значения температурных показателей искусственно занижены/завышены), управляющий модуль может некорректно задействовать приборы для повышения/понижения температуры с целью удержания таковой в границах комфортного диапазона, и в результате спектр последствий может быть довольно негативным. Аналогичная ситуация может наблюдаться в случае перехвата управления над исполнительными устройствами. Данный вариант представляет ещё более существенную опасность, так как управляющий модуль может включать в себя блоки анализа корректности показателей, а исполнительные механизмы в большинстве случаев используют лишь простейшие алгоритмы, подразумевающие исполнение команд без наличия минимального аналитического блока.

Не менее значимой угрозой информационной безопасности при использовании систем «умный дом» с применением современных механизмов управления и взаимодействия является передача информации между конечными устройствами пользователя – такими, как смартфоны, планшеты, смарт-часы и т.д., и управляющим модулем (ядром) системы. Для данной процедуры обычно применяется глобальная сеть Интернет и облачные системы, облегчающие хранение, анализ и обработку данных [2]. Однако, как и любое решение подобного спектра, данный вариант не застрахован от перехвата/подмены/искажения информации. Это может повлечь за собой как репутационные потери (перехват видеопотока с внутренних камер), так и более материальные угрозы (отключение датчиков сигнализации и проникновение в дом, вывод из строя механизмов защиты от пожара с инициацией такового и т.п.)

Создание какого-либо единого механизма, позволяющего автоматически анализировать происходящие события/учитывать потоки информации/отсекать несанкционированные воздействия, на текущий момент представляется сложнореализуемой задачей в силу ряда противоречащих друг другу факторов. Основным препятствием является отсутствие единой системы унификации сенсорно-исполнительных комплексов, блоков обработки и передачи информации; при этом в большинстве случаев используются универсальные протоколы передачи данных, не имеющие специализированных средств защиты информации в контексте рассматриваемой предметной области.

Решением, позволяющим снизить вероятность возникновения угроз информационной безопасности инфраструктуры «умного дома» может стать программно-аппаратный комплекс, имеющий возможность анализа сетевого трафика. С точки зрения физической реализации в качестве основы подобного комплекса рационально применение интегрированного модуля, включающего в себя высокоуровневую платформу на базе NVidia Jetson или аналога таковой. Программная реализация подразумевает наличие возможности работы со всеми устройствами, входящими в инфраструктуру рассматриваемой предметной области – сенсорными комплексами, исполнительными механизмами, каналами передачи данных. Важным условием является возможность автоматизированной и гибкой адаптации к условиям эксплуатации, подразумевающей формирование разрешительно-запретительных политик безопасности в зависимости от того, как именно настроена и используется система «умный дом». Наиболее эффективным решением с программной точки зрения будет использование в качестве базового аналитического механизма нескольких конволюционных нейросетей (CNN). Подобный подход позволит динамически модифицировать схему правил, подтверждающих или отклоняющих действия по поддержанию обстановки внутри помещения.

Общая модель предлагаемого АПК состоит из нескольких модулей. Первый, сетевой, предназначен для осуществления инфокоммуникационных взаимодействий с системой сенсоров и управляющих механизмов. Решаемые задачи сводятся к приёму и отправке сетевых пакетов с применением широкого спектра проводных и беспроводных технологий – таких, как Wi-Fi, Bluetooth, Z-Wave, ZigBee и т.п. Поступающие пакеты отправляются во второй модуль, предназначенный для декодирования и интерпретации. В рамках данной задачи определяется: что за информация поступила, её источник, конкретные значения. Третий модуль предназначен для валидации поступивших данных. В качестве критериев могут выступать предопределённые диапазоны значений; привязка к разрешённому спектру устройств, идентифицируемых на уровне сетевых интерфейсов; допустимые значения хэш-функций; разрешённые идентификационные и аутентификационные данные. Четвёртый модуль, аналитический, принимает на вход проверенную на предыдущем этапе информацию и решает тактико-стратегические задачи, основными из которых является определение: насколько корректно то или иное воздействие, направленное на поддержание гомеостатического состояния; является действие, заданное пользователем, допустимым с учётом заданных параметров – или же имеется ситуация несанкционированного, вредоносного воздействия [3].

В настоящее время имеется ситуация, когда автоматизация функций жилища становится повсеместным явлением, внедряемым как в рамках частных домов, так и в помещениях предприятий различного масштаба и направлений деятельности. Централизованное управление температурой, влажностью, освещением помещений позволяет не только упростить задачи по поддержанию микроклимата, но и сократить расходы на электроэнергию, водоснабжение, газ и другие энергоносители. Функции, реализующие автоматическую и своевременную реакцию системы в случае возгораний, протечек, иных аварийных ситуаций, позволяют устранить последствия (а в ряде случаев – и предотвратить таковые), а также существенно сократить расходы на пост-аварийное восстановление помещений; порой подобные системы спасают человеческие жизни.

Однако, как и в любой автоматизированной системе, в случае преднамеренных действий со стороны злоумышленников, инфраструктура «умного дома» может представлять существенную опасность для обитателей и/или сотрудников, находящихся в помещениях, управляемых подобного рода системами. С каждым днём

количество потенциальных угроз безопасности существенно возрастает, и разработка методов по их своевременному анализу и устранению является весьма значимой задачей.

СПИСОК ЛИТЕРАТУРЫ

1. Аминов Х.И. Модели цифровизации экономической деятельности: монография. / Аминов Х.И., Емельянов А.А., Коршунов И.Л. и др. – СПб: СПбГЭУ, 2019. - 179 с.
2. Коршунов И.Л. Проблемы информационно-технологической деятельности / И.Л. Коршунов, М.О. Колбанёв, И.М. Лёвкин // Известия высших учебных заведений. Приборостроение. - 2017. - Т. 60. - № 2. - С. 105-109.
3. Левкин И.М. Комплексная оценка эффективности робототехнических систем добывания и обработки информации // Изв. вузов. Приборостроение. - 2017. - Т. 60. - № 2. - С. 110-116.

УДК 004.4

ФОРМИРОВАНИЕ ЦИФРОВОГО ОБРАЗОВАТЕЛЬНОГО ПРОФИЛЯ ОБУЧАЮЩЕГОСЯ

Кирилова Дарья Александровна
Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия
e-mails: dasha.kirilova.96@bk.ru

Аннотация. В работе предлагается концепция формирования цифрового образовательного профиля обучающегося, позволяющая отследить полученные компетенции в процессе обучения и оцифровать базу трудоустройства выпускников.

Ключевые слова: цифровой след; цифровой образовательный профиль; обучающийся; трудоустройство; веб-платформа.

GENERATING DIGITAL EDUCATIONAL PROFILE THE LEARNER

Kirilova Daria
Nizhny Novgorod state University of engineering and Economics
22A Oktyabrskaya St, Knyaginino, 606340, Russia
e-mail: dasha.kirilova.96@bk.ru

Abstract. The paper proposes a concept for the formation of a digital educational profile of a student, which makes it possible to track the acquired competencies in the learning process and digitize the employment base of graduates.

Keywords: digital footprint; digital educational profile; learner; employment; web platform.

В настоящее время происходит повсеместная информатизация образовательной деятельности. С внедрением информационных технологий, технологий онлайн обучения, популяризации образовательных активностей в социальных сетях, большую значимость обретает цифровой след формируемый обучающимся в образовательно пространстве. Все цифровые следы оставляемые обучающимся представляют собой цифровой образовательный профиль.

Формирование цифрового образовательного профиля должно начинаться с момента подачи заявления о поступлении в приемную комиссию образовательного учреждения и продолжаться в течении всего периода обучения.

В соответствии с ФГОС ВО 3++ неотъемлемой составляющей цифровой образовательной среды университета является электронное портфолио студента. Электронное портфолио включает в себя достижения студента в различных направлениях деятельности.

Во время учебы электронное портфолио студента пополняется. Вся его творческая работа в виде рефератов, эссе, курсовых работ, отчетов по практике, статей, результатов научно-исследовательской деятельности формирует цифровое портфолио, сохраняя след образовательной и научной деятельности студента. Обновляется и цифровой профиль образовательных интересов студента, включая в себя набор сформированных компетенций.

После того, как обучающийся закончил обучение, его цифровой профиль переносится на веб-платформу «Выпускник» доступ, к которой имеют и работодатели, и выпускники.

В настоящее время в университете используется электронная информационно-образовательная среда на платформе LMS Moodle. В которую импортируются персональные данные абитуриента, полученные в приемной комиссии, а также формируется электронное портфолио, учитывается успеваемость и профессиональные компетенции. Планируется разработка информационной системы Цифрового образовательного профиля, и разработка веб-платформы «Выпускник».

Подводя итог, следует отметить, что в процессе профессиональной подготовки в вузе так или иначе анализируются следы цифровой активности обучающихся, но в большинстве случае требуется поиск системного решения, позволившего бы студентам наиболее полно реализовать свой образовательный потенциал в цифровой среде университета.

Цифровой образовательный профиль, позволит выпускникам, с дальнейшим трудоустройством, а также поможет работодателям найти себе сотрудника с необходимыми профессиональными компетенциями и

навыками. Для университетов, это упростит работу с базой выпускников и в перспективе с дальнейшим отслеживанием их трудоустройства.

СПИСОК ЛИТЕРАТУРЫ

1. Астахова Т.Н., Кирилова Д.А., Маслов Н.С. Перспективы внедрения технологии блокчейн в современную систему образования // International Journal of Open Information Technologies, 2018. Т. 6. №. 8. С. 31-37.
2. Кирилова Д.А., Маслов Н.С. Технология blockchain как процесс цифровизации образования // Перспективные направления развития отечественных информационных технологий материалы IV межрегиональной научно-практической конференции. Севастопольский государственный университет; науч. ред. Б.В. Соколов. – 2018, С. 74-76.
3. Кирилова Д.А., Маслов Н.С. Цифровая трансформация социальной сферы услуг // Перспективные направления развития отечественных информационных технологий материалы V межрегиональной научно-практической конференции. Севастопольский государственный университет; науч. ред. Б.В. Соколов. – 2019., С.361-363.

УДК 004.056

НЕКОТОРЫЕ АСПЕКТЫ ЦИФРОВОГО СУВЕРЕНИТЕТА

Коршунов Игорь Львович, Микадзе Сергей Юрьевич
Санкт-Петербургский государственный экономический университет
канала Грибоедова наб., 30-32, Санкт-Петербург, 191023, Россия
e-mails: dept.ait@unecon.ru , mik@finec.ru

Аннотация. Понятие цифрового суверенитета. Кибербезопасность и цифровой суверенитет. Нормативно-правовая база в интересах цифрового суверенитета. Импортозамещение и технологическая независимость.

Ключевые слова: ИТ-индустрия; цифровой суверенитет; кибербезопасность; цифровизация.

SOME ASPECTS OF DIGITAL SOVEREIGNTY

Korshunov Igor, Mikadze Sergey
Saint-Petersburg State University of Economics
30-32 Griboyedov Canal, St. Petersburg, 191023, Russia
e-mails: kil53@mail.ru, mik@finec.ru

Abstract. The concept of digital sovereignty. Cybersecurity and digital sovereignty. The regulatory framework in the interests of digital sovereignty. Import substitution and technological independence.

Keywords: IT industry; digital sovereignty; cybersecurity; digitalization.

В настоящее время государство, бизнес и общество едины в понимании, что без цифрового суверенитета, без надежной защиты информационного пространства от кибератак Россия существовать не может [1]. Под цифровым суверенитетом принято понимать право государства определять свою информационную политику, самостоятельно распоряжаться инфраструктурой, ресурсами, обеспечивать информационную безопасность [2]. Цифровой суверенитет предполагает, в частности, и защиту от кибератак. Рассматривая цифровой суверенитет России, следует обратить внимание на ряд аспектов.

Движение в сторону цифрового суверенитета должно быть поступательным, динамичным и разумным. Но принимаемые Правительством решения не всегда являются скоординированными, системными и выполнимыми.

Совершенствование нормативно-правовой базы в сфере информационно-коммуникационных технологий должно быть направлено на поддержку интересов разработчиков и производителей отечественной ИТ-продукции.

Доработка систем безопасности объектов критической информационной инфраструктуры и государственных структур должна проводиться с учетом необходимости эффективного противодействия сложным кибератакам. Необходимо активней создавать горизонтальные системы кибербезопасности.

Без создания собственного программного обеспечения, собственной элементной базы цифрового суверенитета у России не будет. Если первоначально государством ставилась задача импортозамещения, то сейчас она формулируется как движение к технологической независимости, а это предполагает разработку не просто отечественного, но и качественного продукта, который может стать конкурентоспособным на международном рынке.

В ИТ-сфере имеется большой дефицит квалифицированных кадров. Количества выпускаемых ИТ-специалистов недостаточно. Нужны специалисты со средним и средним специальным образованием. Необходима планомерная работа с молодежью, начиная со школы.

Для достижения цифрового суверенитета в России должен быть создан культ информационных технологий, работа в этой области должна быть престижна.

СПИСОК ЛИТЕРАТУРЫ

1. Программа Петербургского международного экономического форума «ПЭФМ-2021». [Электронный ресурс]. Режим доступа: https://forumspb.com/programme/business-programme/ (дата обращения: 23.08.2021).
2. Ашманов И. Информационный суверенитет России: новая реальность//Россия навсегда. 13.05.2013. [Электронный ресурс]. URL: http://rossiyanavsegda.ru/read/948/ (дата обращения 3.08.2021).

УДК 004

КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ И ЦИФРОВЫЕ ДВОЙНИКИ КАК КОНЦЕПЦИЯ ПОСТРОЕНИЯ МИРА ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ: СРАВНЕНИЕ И ВЗАИМОСВЯЗЬ

Краснова Анна Сергеевна[1], Колбанёв Михаил Олегович[2], Астахова Татьяна Николаевна[1]

[1] Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия

[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Инструментальная ул., 2, Санкт-Петербург, 197022, Россия
e-mails: shochina96@mail.ru, mokolbanev@mail.ru, ctn_af@mail.ru

Аннотация. В статье представлены описания понятий киберфизических систем и цифровых двойников, которые привлекли большое внимание среди исследователей. Данные концепции позволяют создать оптимальные условия и наделить системы большей эффективностью за счет своей обратной связи, которая позволяет физическим процессам влиять на цифровой мир и наоборот. Киберфизические системы и цифровые двойники включают в себя такие свойства как взаимодействие в реальном времени, взаимосвязь физического и виртуального мира, интеграцию организаций. Но с различных точек зрения они во многом не идентичны. Для того, чтобы показать различия и корреляцию этих двух концепций, в данной статье рассматриваются киберфизические системы и цифровые двойники с различных точек зрения.

Ключевые слова: интеллектуальные технологии; киберфизические системы; концепция; цифровая трансформация; цифровой двойник.

CYBER–PHYSICAL SYSTEMS AND DIGITAL TWINS A CONCEPT OF BUILDING THE WORLD OF INTELLECTUAL TECHNOLOGIES: COMPARISON AND INTERCONNECTION

Krasnova Anna[1], Kolbanyov Mikhail[2], Astakhova Tatyana[1]

[1] Nizhny Novgorod state University of engineering and Economics
22A Oktyabrskaya St, Knyaginino, 606340, Russia

[2] Saint Petersburg State Electrotechnical University
2 Instrumental St., St. Petersburg, 197022, Russia
e-mails: shochina96@mail.ru, mokolbanev@mail.ru, ctn_af@mail.ru

Abstract. The article describes the concepts of cyberphysical systems and digital twins, which attracted a lot of attention among researchers. These concepts allow you to create optimal conditions and give the system more efficiency at the expense of its feedback, which allows you to influence the physical processes in the digital world and vice versa. Cyberphysical systems and digital twins include in themselves such properties as interaction in real time, interconnection of physical and virtual worlds, integration of organizations. But with different points of view they are in many ways not identical. In order to show the difference and correlation of these two concepts, in this article cyberphysical systems and digital twins with different points of view are considered.

Keywords: intellectual technologies; cyberphysical systems; concept; digital transformation; digital twin.

Человечество вступает в новую эпоху, эпоху интеллектуальных технологий. Все то, что нас окружает, стремительно изменяется и эволюционирует. Мы вступаем в эпоху, где интеллектуальные системы способны выполнять функции оптимизации, принятия решения, автоматического анализа и многих других функций, взаимодействуя при этом с реальным миром в режиме реального времени. Взаимодействие человека и машины становится все более тесным, что приводит к построению новых моделей управления. Эффективность рабочих процессов будет намного выше благодаря онлайн-работе и тесной связи с машинами для решения сложных задач. Сейчас мы стоим на пути цифровизации всех существующих процессов, что влечет к глобальным проблемам, связанным с быстрым развитием цифровых технологий.

Современная промышленность так же переживает изменение существующих бизнес-процессов благодаря цифровым технологиям. Производство переходит к интеллектуальному производству, где роль киберфизических систем и цифровых двойников занимает центральное место. Интеллектуальное производство благодаря данным концепциям (киберфическим системам и цифровым двойникам) контролирует состояние производства в режиме реального времени на протяжении всего жизненного цикла продукта, тем самым в реальном времени они могут:

- получать информацию об объектах;
- определять изменение характеристик;
- делать умозаключение в рамках ранее установленных правил;
- принимать решения на основе полученной информации и выдать определенные команды.

Киберфизические системы представляют собой централизованную и/или распределенную аппаратно-программную систему, реализующую физические и инфокоммуникационные процессы сбора, обработки, накопления, хранения, поиска, защиты, распространения и использования данных и информации и взаимодействующую с объектами реального мира через физические процессы [1].

Цифровой двойник, согласно классическому определению – это цифровая копия живого или искусственного физического объекта [2].

Термин цифровой двойник относится к цифровой копии потенциальных и реальных физических активов (физический двойник), процессов, людей, мест, систем и устройств, которые могут использоваться для различных целей. Цифровые двойники призваны облегчать средства контроля, понимания и оптимизации функций всех физические активов, обеспечивая беспрепятственную передачу данных между физическим и виртуальным миром [3].

В связи с переходом к цифровому обществу любая деятельность стала задаваться путем моделирования процессов нового типа, особенностью которых является конвергенция материального и информационного потоков, которые не могут быть отделены друг от друга по принципу кибернетических систем [4, 5].

Киберфизические системы и цифровые двойники включают в себя схожие характеристики, и описывают взаимодействие двух миров физического с «киберпространством». Сейчас киберфизические системы приравнивают больше к научной категории, а цифровые двойники в свою очередь к технической категории.

Цифровые двойники, как и киберфизические системы, включают в себя киберфизическое и физическое пространства. При помощи киберфизического мира они осуществляют контроль, взаимодействие и управление физическим миром в режиме реального времени. Однако существуют определенные расхождения в отношении киберпространства: цифровой двойник больше основывается на виртуальных моделях, которые являются идентичной копией физического объекта, а киберфизические системы делают упор на интеграцию и сотрудничество вычислительных систем, коммуникаций и управления.

Рассматривая цифровые двойники и киберфизические системы с точки зрения их функций, датчики и исполнительные механизмы обеспечивают взаимодействие между физическим и кибер- мирами для обмена данными и управлением в обеих концепциях. Таким образом, датчики и исполнительные механизмы можно рассматривать как основные элементы в киберфизических систем, в то время как модели и данные являются основными элементами для цифровых двойников.

Если рассматривать с иерархической точки зрения, то важно отметить, что данные концепции имеют различные компоненты на каждом уровне. Оба элемента можно разделить на единичный уровень, системный уровень и уровень SoS.

Согласно иерархической структуре, киберфизические системы и цифровые двойники могут быть реализованы в три этапа. На первом уровне необходимо построить модульный уровень, в основе которого лежит интеллектуальный мониторинг, интеллектуальное управление и управление состоянием оборудования. На втором шаге необходимо построить системный уровень. И на третьем шаге по средствам 1 и 2 уровней реализуется уровень SoS.

21 век – век четвертой промышленной революции, или как мы ее привыкли называть Индустрия 4.0, в которой облачные вычисление, 5G, интернет вещей (IoT), искусственный интеллект и другие технологии, являются большим шагом к созданию мира интеллектуальных технологий. Киберфизические системы и цифровые двойники привлекли большое внимание среди исследователей. Данные концепции позволяют создать оптимальные условия и наделить системы большей эффективностью за счет своей обратной связи, которая позволяет физическим процессам влиять на цифровой мир и наоборот. Киберфизические системы и цифровые двойники включают в себя такие свойства как взаимодействие в реальном времени, взаимосвязь физического и виртуального мира, интеграцию организаций. Но с различных точек зрения они во многом не идентичны. В данной работе представлены сравнение и взаимосвязь таких концепций как киберфизические системы и цифровые двойники, концепции рассматриваются и анализируются с разных точек зрения. Сравнение с разных точек зрения, представленное в этой работе, позволяет лучше понять киберфизические системы и цифровые двойники, которые кажутся концептуально похожими. Это также помогает выявить сходства и различия между перспективными технологиями, которые подчеркивают киберфизическую интеграцию.

СПИСОК ЛИТЕРАТУРЫ

1. Захаров В.В. Динамическая интерпретация формального описания и решения задачи модернизации сложных объектов // Приборостроение. 2019. № 10. С. 914–920.
2. El Saddik A. Digital twins: The convergence of multimedia technologies // IEEE multimedia. Vol. 25, 2018, No 2. P. 87–92.
3. Khajavi S. H. et al. Digital twin: vision, benefits, boundaries, and creation for buildings // IEEE access. Vol. 7, 2019. P. 147406-147419.
4. Колбанёв М.О., Коршунов И. Л. Информационно-технологическое обеспечение цифровой экономики // Информационные технологии цифровой экономики. 2017. С. 5-9.
5. Колбанёв А.М., Колбанёв М.О., Цехановский В.В. Модели информационного взаимодействия. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2016, 172 с.

УДК 681.3.06

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОМОЩИ НЕЙРОННЫХ СЕТЕЙ

Мещеряков Евгений Евгеньевич
Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия
e-mail: leonile5@mail.ru

Аннотация. Рассматриваются аспекты защиты различных информационных систем при помощи нейронных сетей.

Ключевые слова: информационная безопасность; информационные системы; нейронные сети.

ENSURING INFORMATION SECURITY USING NEURAL NETWORKS

Meshcheryakov Evgeniy
Nizhny Novgorod state University of engineering and Economics
22A Oktyabrskaya St, Knyaginino, 606340, Russia
e-mail: leonile5@mail.ru

Abstract. The aspects of protection of various information systems using neural networks are considered.

Keywords: information security; information systems; neural networks.

Для обеспечения защиты и оперативного реагирования на события информационной безопасности требуется построение единой системы защиты информации, обладающей адаптивными свойствами.

Кроме того, при построении защищенных систем необходимо придерживаться базовых принципов [1]:

1. Принцип толерантности – средства защиты должны действовать в строгом соответствии с формальной моделью безопасности для всех без исключения взаимодействий в системе.

2. Принцип абсолютности – средства защиты должны быть встроены в систему обработки информации таким образом, чтобы исключить возможность любого взаимодействия, не попадающего под их контроль.

3. Принцип инвариантности – средства защиты должны функционировать исходя из представления всех типов информационных взаимодействий в виде операций доступа субъектов к объектам и контролировать их с помощью универсальных алгоритмов, инвариантных к типу воздействия.

4. Принцип унификации – должно существовать однозначное соответствие между контролируемыми операциями доступа субъектов к объектам и отношениям доступа, описываемыми моделями безопасности.

5. Принцип разрешимости – безопасность системы должна быть формально доказана в рамках используемой модели. Должен существовать механизм, позволяющий решить вопрос о безопасности настоящего состояния системы и оценить ее безопасность в будущем.

Для обеспечения информационной безопасности информационных систем предполагается использование нейронных сетей.

Нейронные сети представляют собой систему соединённых и взаимодействующих между собой простых процессоров (искусственных нейронов) [2].

Нейронные сети необходимо обучать. Возможность обучения – одно из главных преимуществ нейронных сетей перед традиционными алгоритмами. Технически обучение заключается в нахождении коэффициентов связей между нейронами. В процессе обучения нейронная сеть способна выявлять сложные зависимости между входными данными и выходными, а также выполнять обобщение.

Нейронная сеть способна производить классификацию известных угроз безопасности. Входной вектор либо будет отнесен к одному из известных классов угроз, либо будет произведено расширение классификации за счет добавления нового нейрона-прототипа с параметрами предъявленного вектора. Обучение производится в режиме адаптации системы при непосредственном участии и под контролем доверенных лиц. Процесс обучения завершается блокировкой режима адаптации и переводом сформированной системы в режим работы. На начальном этапе происходит минимальная активация потенциальных механизмов защиты и максимальное наполнение поля известных угроз. Целью этапа эксплуатации жизненного цикла системы является корректное исполнение системой заданных функций.

Таким образом, нейронные сети могут быть эффективно использованы для обеспечения безопасности информационных систем.

СПИСОК ЛИТЕРАТУРЫ

1. Зегжда Д.П. Принципы и методы создания защищенных систем обработки информации : дис. ...доктора технических наук : 05.13.19. СПб., 2002.380 с.
2. Каллан Р. Основные концепции нейронных сетей: пер. с англ. – М.: Издательский дом «Вильямс», 2001. 287 с.
3. Малыш В.Н., Федерякин А.В., Обеспечение информационной безопасности научно-методического портала при помощи искусственных нейронных сетей [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-nauchno-metodicheskogo-portala-pri-pomoschi-iskusstvennyh-neyronnyh-setey (Дата обращения: 28.07.2021).
4. Левкович С.С., Жидков Е.А., Левчук К.Э., Соловьев Д.В., Искусственные нейронные сети в вопросах информационной безопасности [Электронный ресурс]. URL: https://openbooks.itmo.ru/ru/file/5037/5037.pdf (Дата обращения: 28.07.2021).

УДК 338.2

ЭВОЛЮЦИЯ ПРОЦЕССА ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Прокопец Наталья Николаевна
Санкт-Петербургский государственный экономический университет (СПбГЭУ)
Прилукская, ул., 3, Санкт-Петербург, 194064, Россия
e-mail: nataly_prokopets@mail.ru

Аннотация. В статье представлен авторский подход к периодизации процесса обеспечения экономической безопасности интеллектуальной собственности и охарактеризованы основные этапы его эволюции.

Ключевые слова: экономическая безопасность; интеллектуальная собственность; эволюционные процессы в развитии систем экономической безопасности.

EVOLUTION OF THE PROCESS OF ENSURING THE ECONOMIC SECURITY OF INTELLECTUAL PROPERTY

Prokopets Natalia
The St. Petersburg State University of Economics (UNECON)
3 Prilukskay St, St. Petersburg, 194064, Russia
e-mail: nataly_prokopets@mail.ru

Abstract. The article presents the author's approach to the periodization of the process of ensuring the economic security of intellectual property.

Keywords: intellectual property; economic security; evolutionary processes in the development of economic security systems.

Обеспечение экономической безопасности интеллектуальной собственности является ключевым вопросом, связанным с эффективным управлением интеллектуальной собственностью в современных условиях хозяйствования. Вместе с тем, процесс обеспечения экономической безопасности интеллектуальной собственности подвергался определенной эволюции с точки зрения изменения подходов к характеристике и специфическим особенностям организации управленческих действий. Основные этапы эволюции процесса обеспечения экономической безопасности интеллектуальной собственности.

Этап 1 – Защита и обеспечение авторских прав на объекты интеллектуальной собственности (античность-50-е гг. XX века).

Этап 2 – Формирование и развитие автономных систем экономической безопасности интеллектуальной собственности на уровне отдельных корпораций (50-е гг. XX века - 80-е гг. XX века).

Этап 3 – Формирование и развитие национальных систем экономической безопасности интеллектуальной собственности и обеспечение их взаимодействия с корпоративными системами безопасности (90-е гг. XX века – начало XXI века).

Этап 4 – Формирование и развитие интегрированных систем экономической безопасности интеллектуальной собственности на основе использования цифровых технологий и обеспечения социальной ответственности участников инновационного процесса (в стратегической перспективе).

На первом и самом значительном, с точки зрения временного периода, этапе экономическая безопасность интеллектуальной собственности ограничивалась вопросами обеспечения и защиты отдельных прав на объекты интеллектуальной собственности [6]. Начало данного этапа соответствует периоду Античности, когда проводились первые судебные разбирательства относительно права владения тем или иным произведением нематериального искусства.

К числу наиболее значимых исторических примеров данного этапа следует отнести такие общеизвестные факты как:

1421 г – впервые городской управой Флоренции выдан патент на изобретение на имя Филиппо Брунеллески, который изобрел корабельный поворотный кран [2],

1624 г – принятие в Англии прообраза современных патентных законов – нормативного акта «Статут Якова I» (или Статут о монополиях) [1],

1828 г – принятие впервые в российской истории нормативного акта, регламентирующего авторские права - Цензурного устава, с которого и начинается развитие российского авторского права [4],

1883 г – принятие международной Парижской Конвенции по охране прав интеллектуальной собственности [1] и т.д.

Как видно из представленных примеров, можно говорить об определенной унификации подходов к экономической безопасности – от локальных и национальных нормативных актов до принятия международных положений, и конвенций. Вместе с тем, область экономической безопасности представляет собой лишь узкий сегмент действий, связанных с интеллектуальной собственностью, а именно- разграничение, обеспечение защиты и соблюдения авторских прав как на произведения искусства, так и на иные объекты интеллектуальной собственности, прежде всего, изобретения и ноу-хау [5].

Второй этап развития исследуемого процесса связан с постепенным формированием и развитием обособленных комплексных систем экономической безопасности интеллектуальной собственности на уровне отдельных корпораций и предприятий. Рассматриваемый этап соответствует постепенному началу формирования мирового рынка интеллектуальной собственности и отражает тенденции постепенного роста инновационной активности различных хозяйствующих субъектов. Именно в данный момент времени в странах Запада появляются первые технопарки, бизнес-инкубаторы, инновационные предприятия при поддержке не только органов государственной власти, но, прежде всего, крупнейших корпораций различного отраслевого характера [3].

На втором этапе происходит трансформация систем экономической безопасности интеллектуальной с точки зрения встраивания объектов интеллектуальной собственности в общую систему корпоративной безопасности. При этом, одним из ключевых вопросов становится оптимизация соотношения уровня прямых расходов на обеспечение экономической безопасности объектов интеллектуальной собственности к результативности их создания, реализации и внедрения в условиях реального производства. Таким образом, наблюдается окончательных переход от номинальной ценности возможного объекта интеллектуальной собственности к его фактической стоимости на основе достижения равновесного состояния между спросом и предложением на формирующемся мировом рынке интеллектуальной собственности.

С началом 90-х гг. и разрушением сложившихся социально-политических и экономических устоев мирового хозяйства, экономическая безопасность интеллектуальной собственности становится объектом не только корпоративного управления, но и стратегическим ресурсом для развития отдельных национальных экономических систем. Данное обстоятельство было обусловлено целым рядом взаимосвязанных проблем общего развития в новых экономических условиях:

– значительным ростом потребления в различных частях земного шара, в том числе в развивающихся странах и странах с переходной экономикой, что требовало неуклонного повышения уровня производственных мощностей при одновременном достижении генеральной цели снижения общей себестоимости производимой продукции,

– повышением уровня конкурентной борьбы между различными производителями при одновременной высокой скорости оборота и неуклонного роста сделок по передаче прав на объекты интеллектуальной собственности, что привело к увеличению расходов на обеспечение экономической безопасности и повысило требования к уровню соблюдения коммерческой тайны на уровне отдельных предприятий и отраслевых рынков,

– возникновением и последующей трансформацией новых, прежде всего технологических, угроз для развития рынка интеллектуальной собственности, что также повысило внимание к вопросам экономической безопасности уже в условиях постепенно формирующейся цифровой среды ведения бизнес-процессов и т.д. [7].

Наконец, формирование и развитие интегрированных систем экономической безопасности интеллектуальной собственности на основе использования цифровых технологий и обеспечения социальной ответственности участников инновационного процесса является перспективным направлением трансформации существующих принципов экономической безопасности в исследуемой сфере.

СПИСОК ЛИТЕРАТУРЫ

1. Арутюнов Э.К., Цыганкина Е.А. История развития права интеллектуальной собственности в зарубежном и отечественном законодательствах// В сборнике: Новые парадигмы общественного развития: экономические, социальные, философские, политические, правовые, общенаучные тенденции и закономерности. Материалы международной научно-практической конференции: в 4 частях. 2016. С. 64-66.
2. Асмандияров В.М. История возникновения института интеллектуальной собственности//В книге: Интеллектуальное право. Кондратовская С.Н., Асмандияров В.М., Валькова Е.В., Миронов А.В., Мухтарова Е.А., Ускова Т.Н., Шелепина Е.А. учебное пособие. ФКОУ ВО «Вологодский институт права и экономики Федеральной службы исполнения наказаний». Вологда, 2020. С. 27-38
3. Гехаев М.Д. Современные проблемы по защите прав интеллектуальной собственности/Инновационная наука. 2019. № 1. С. 100-103.
4. Кабай М. История становления института интеллектуальной собственности/Интеллектуальный потенциал XXI века: ступени познания. 2013. № 19. С. 169-173.
5. Маясова К.С. Защита интеллектуальной собственности и экономическая безопасность// Сборники конференций НИЦ Социосфера. 2020. № 25. С. 104-107.
6. Тактарова С. Институт интеллектуальной собственности в условиях глобализации/ Интеллектуальная собственность. Промышленная собственность. 2020. № 10. С. 56-61.
7. Чунаев С.Ю., Сергеев А.Ю. Инновационный фактор обеспечения устойчивого экономического развития предприятия // Проблемы и перспективы развития Российской экономики: сборник материалов VI научно-практической конференции. – Прага: Vědecko vydavatelské centrum «Sociosféra-CZ», 2017. - С. 22-25.

УДК 343.37

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ЛОГИСТИЧЕСКОЙ СИСТЕМЫ В УСЛОВИЯХ ПАНДЕМИИ: ПРОБЛЕМЫ И РЕШЕНИЯ

Смирнова Ольга Александровна[1], Челак Светлана Васильевна[2]

[1] Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
[2] Санкт-Петербургский государственный экономический университет
канала Грибоедова наб., 30-32, Санкт-Петербург, 191023, Россия
e-mails: o.saraf@mail.ru, sv1135@mail.ru

Аннотация. Статья посвящена выявлению факторов, оказывающих влияние на эффективное обеспечение логистической системы предприятий, рассмотрены основные проблемы, возникающие при внедрении и реализации системы экономической безопасности логистических систем.

Ключевые слова: система безопасности; логистическая система; экономическая безопасность; риски.

ENSURING THE ECONOMIC SECURITY OF THE LOGISTICS SYSTEM IN THE CONTEXT OF A PANDEMIC: PROBLEMS AND SOLUTIONS

Smirnova Olga[1], Chelak Svetlana[2]

[1] Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
[2] Saint-Petersburg State University of Economics
30-32 Griboyedov Canal, St. Petersburg, 191023, Russia
e-mails: o.saraf@mail.ru, sv1135@mail.ru

Abstract. The article is devoted to the identification of factors that influence the effective provision of the logistics system of enterprises, the main problems that arise during the introduction and implementation of the economic security system of logistics systems are considered.

Keywords: security system; logistics system; economic security; risks.

В условиях пандемии глобальные цепочки поставок были нарушены в результате сокращения производственных мощностей из-за снижения глобального потребления и прекращения деятельности производственных компаний в Китае, странах Дальнего Востока и Европы. Эксперты указывают, что прекращение производства промежуточных и конечных товаров в Китае оказывает двустороннее влияние на глобальную цепочку поставок. Во-первых, из-за проблем с поставками конечной продукции и промежуточных товаров компании, конечная продукция которых поступает из Китая, были вынуждены закрыть свои торговые точки. Компании-производители, которые не могли закупить необходимое сырье и детали для своего производства, были вынуждены либо прекратить производство, либо искать альтернативных поставщиков из разных географических регионов. Из изложенного материала следует, что любая логистическая система является сложным элементом и подвержена постоянному риску.

Общества и предприятия по всему миру столкнулись с беспрецедентными проблемами из-за сбоев, вызванных вспышкой коронавируса и, как следствие, большой изоляцией.

По результатам анализа девяти международных поставщиков логистических услуг с использованием тематических исследований и литературного обзора, были выявлены препятствия на пути успешной адаптации поставщиков логистических услуг к цифровой трансформации. В результате исследования определены пять критериев, препятствующих цифровой трансформации поставщиков логистических услуг, и восемь критериев, которые обеспечат успешную реализацию цифровой трансформации.

Создание устойчивой цепочки поставок требует разработки четырех принципов: проектирование цепочки поставок; сотрудничество в цепочке поставок; гибкость цепочки поставок; культура управления рисками цепочки поставок. Все перечисленные принципы нуждаются во внешней поддержке иных составляющих экономической деятельности, и в первую очередь, обеспечения ее безопасности.

Нужно отметить, что у пандемии есть и плюсы. Возникающие проблемы стали импульсом к изменению структуры цепочки поставок и ее большей цифровизации. Благодаря внедрению цифровых технологий можно более эффективно управлять своими запасами [1]. Необходимо отметить, что сегодня за технологическую безопасность должно отвечать каждое звено логистической системы, а вопросы решения экономической безопасности должна решать управляющая логистическая компания.

Цифровые технологии позволили, внедрены следующие системы:

1. Технологии обеспечения безопасной социальной дистанции. Все подвержены риску заражения коронавирусом, включая водителей грузовиков, сотрудников складов и распределительных центров, а также сотрудников магазинов. Руководители логистических компаний должны сделать все возможное, чтобы использовать современные технологии для максимальной безопасности всех участников цепочки поставок.

2. Повышение безопасности за счет внедрения телематических решений. После пандемии правительственные учреждения во многих странах ввели временные стимулы, которые позволяют им увеличить максимальное количество часов в день, которое водители могут проводить за рулем.

3. Адаптация маршрутов и перераспределение активов. Переадресация звонков может применяться на любом этапе доставки: от первой до последней мили. Когда дело доходит до основных грузов, планы могут быть скорректированы, и грузовики могут направляться прямо в розничный магазин, а не в распределительный центр.

4. Повышение эффективности за счет автоматизации. Многие западные логистические компании уже борются с нехваткой водителей, что создает определенные барьеры для бизнеса. Был автоматизирован не только транспорт, но и склады, и распределительные центры. Сегодня Amazon удалось реализовать полную автоматизацию склада, и остальным компаниям ничего не остается, как последовать примеру лидера.

5. Отслеживание движения товаров в реальном времени. С их помощью сотрудники филиала видят движение грузовиков в режиме реального времени и быстро выгружают товар по прибытии, используя средства индивидуальной защиты. Упреждающие оповещения также полезны для конечных пользователей. Вы точно знаете, на каком этапе доставки находится ваш заказ и когда приедет курьер. Мониторинг снижает риск потери груза и не позволяет водителям покинуть свой первоначальный маршрут, что помогает снизить расходы [2].

Цифровизация логистики связана с переходом на электронный документооборот при управлении грузоперевозками, т. е. вместо бумажных транспортных накладных используются электронные транспортные накладные. Преимуществами данных накладных являются: отсутствие затрат на печать и доставку документов; отсутствие потери документов; обмен такими документами занимает считанные минуты.

Цифровая логистика должна функционировать на основе IT поддержки производственных, торговых и экономических процессов по движению потоков (материальных, товарных).

Таким образом, на данный момент уже внедрены и активно используются следующие информационные технологии и устройства: штриховое кодирование; сканеры, которые позволяют считывать информацию со штрихкодов; метки – портативныые устройства, содержащее данные о товаре и передающее их считывающему устройству с помощью радиоволн; ридеры – приборы, принимающие информацию с меток.

Далее речь пойдет о технологиях, которые на данный момент активно набирают популярность, переходя от стадии развития в стадию зрелости: интеллектуальное извлечение контента; визуализация; совместные порталы; кибернетическое отслеживание. Еще одними немаловажными технологиями необходимыми для внедрения в логистических процесс являются: блокчейн и искусственный интеллект [3].

Применение новых технологий позволит избавиться от существующих проблем, увеличит скорость документооборота, позволит создать структуру управления системой безопасности, так как эффективное управление позволяет в целом повысить уровень защищенности компании.

СПИСОК ЛИТЕРАТУРЫ

1. Прусова В.И., Тимофеева А.О., Буликина А.С. Проблемы логистических компаний в условиях нестабильной экономики // Экономика и бизнес: теория и практика. 2020. № 12. С. 238-242.
2. Казанцев А.А. Влияние пандемии коронавируса на цепи поставок // Скиф. Вопросы студенческой науки. 2020. № 6. С. 48-52.
3. Смещение технологических приоритетов индустрии логистики после пандемии // URL: https://vc.ru. (дата обращения 05.04.2021).

УДК 004.056

ОЦЕНКА ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ УПРАВЛЕНИЯ ПРОИЗВОДСТВЕННОЙ КОМПАНИЕЙ

Соколов Роман Владимирович
Санкт-Петербургский государственный экономический университет
наб. канала Грибоедова, д. 30-32, Санкт-Петербург, 191023, Россия
e-mail: rsok7@rambler.ru

Аннотация. Рассматривается нахождение баланса между экономическими потерями и затратами на информационную защищенность. Дана классификация уровней информационной защищенности в соответствии с экономическими потерями от информационных атаки и их отражение.

Ключевые слова: информационная защищенность; производственная компания

ASSESSMENT OF INFORMATIONAL-ECONOMICAL SECURITY IN MANAGEMENT SYSTEMS OF A MANUFACTURING COMPANY

Sokolov Roman
Saint-Petersburg State University of Economics
30-32 emb. Griboyedov channel, St. Petersburg, 191023, Russia

Abstract. Finding a balance between economic losses and the cost of information security is considered. Is given the classification of information security levels in accordance with economic losses from information attacks and their reflection.

Keywords: information security; manufacturing company.

Введение. Информационно-экономическая безопасность в системах управления производственной компанией зависит от вероятности наступления информационного рискового события в системе управления и величины экономических потерь производственной компании в этом случае. В свою очередь, вероятность наступления информационного рискового события зависит от затрат на информационную защищенность [1].

Нахождение баланса между экономическими потерями и затратами на информационную защищенность представляет собой актуальное направление исследований, в рамках которого находится данный доклад.

Предлагается использовать обобщенный показатель информационной защищенности системы управления производственной компанией [2]. Раскрывается зависимость потерь от информационных атак и затрат на их отражение от величины достигнутого показателя информационной защищенности.

Показана последовательность решения основных задач управления производственной компанией, от составления годовой производственной программы до распределения прибыли от реализации продукции. Анализируются пути влияния информационных атак на результаты решения задач управления производственной компанией.

Заключение. Дана классификация уровней информационной защищенности, содержащая пять уровней. Каждый уровень характеризуется своим соотношением экономических потерь от информационных атак и затрат на их отражение. Выделяется уровень минимальных суммарных потерь и затрат, на котором потери и затраты равны.

СПИСОК ЛИТЕРАТУРЫ

1. Аминов Х.И., Андреевский И.Л., Безрук Г.Г. и др. Модели цифровизации экономической деятельности. – СПб.: СПбГЭУ, 2019. - 179.
2. Стельмашонок Е.В. Информационная инфраструктура поддержки и защиты корпоративных бизнес-процессов: экономико-организационные проблемы. - – СПб.: СПбГИЭУ, 2005. – 151 с

УДК 004

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В LOW-CODE ПЛАТФОРМАХ

Соловей Полина Сергеевна
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mail: polinaa_solovey@mail.ru

Аннотация. Данная работа посвящена возможностям обеспечения информационной безопасности в Low-code платформах. Рассматриваются особенности и способы защиты информации в приложениях с минимальным кодированием.

Ключевые слова: Low-code платформа; безопасность; защита информации; приложение; низкий уровень кода; бизнес-приложение.

ISSUES OF INFORMATION SECURITY OF LOW-CODE PLATFORMS

Solovey Polina
Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
e-mail: polinaa_solovey@mail.ru

Abstract. This work is devoted to the possibilities of ensuring information security in Low-code platforms. The features and methods of information protection in applications with minimal coding are considered.

Keywords: Low-code platform; security; information protection; application; Low-code level; business application.

В современном мире роль информации постоянно повышается, что требует ее защиты от утечки и несанкционированного доступа. В экономической деятельности защита информации позволяет значительно повышать эффективность организации за счет повышения прибыли и конкурентоспособности компании. Современные организации стремятся обеспечить высокую эффективность работы компании, качественную правовую защиту различных видов деятельности компании, защиту коммерческой тайны и информационной среды предприятия [1, 2].

В текущих условиях информационного и экономического развития к современным системам цифровой экономики предъявляются высокие требования, касающиеся обеспечения надежности, отказоустойчивости и информационной безопасности в целом. В последнее время набирают популярность использование Low-code платформ для разработки бизнес-приложений с минимальным применением навыков программирования, которые также должны обеспечивать сохранность данных. Low-code платформы – это способ разработки приложений с помощью визуальных компонентов системы, автоматически сгенерированного кода, готовых компонентов и встроенных конфигураций.

Преимущество Low-code заключается в том, что пользователи получают возможность развивать продукт в компании без поддержки разработчиков и программистов. Данное преимущество ведет к сокращению сроков разработки и реализации проекта по сравнению с традиционной разработкой приложений и снижению затрат на ресурсы компании. Кроме этого, Low-code платформы позволяют улучшить клиентский опыт за счет гибкости разрабатываемого приложения и ускорить цифровую трансформацию организации [3].

В настоящее время множество компаний уже внедрили в свою деятельность Low-code технологии. Low-code платформы используются в таких отраслях, как аутсорсинговые контакт-центры, страхование, строительство, недвижимость, госсектор, транспорт и логистика, фармацевтика, образование, медицинские учреждения и банки и финансы. Например, Low-code платформы могут применяться для автоматизации деятельности документооборота, аналитики и отчетности, HR-процессов, Service Desk, процессов эквайринга, продаж. Кроме этого, они используются в различных подразделениях организаций: «отделе продаж, маркетинга, сервиса, контакт-центре или операционном отделе» [3]. Такие платформы предназначены для корпоративного использования, они способны обеспечить масштабируемость и безопасность сложного приложения, а также обладают развитыми возможностями интеграции со смежными системами.

В связи с активным использованием Low-code платформ в крупных организациях необходимо обеспечить безопасность данных в разрабатываемом приложении. Проблемы безопасности могут быть связаны с неосведомленностью специалистов в области обеспечения безопасности приложения, с доступом пользователей к приложению через браузер, с интеграцией со сторонним программным обеспечением, с наличием доступа у некоторых пользователей к областям баз данных компании, которые могут нанести ущерб безопасности [4].

Для обеспечения защиты информации и безопасности данных организации, в первую очередь, необходимо производить оценку поставщиков Low-code решений. Компаниям следует проводить оценку и аудит платформ, которые они выбирают для внедрения, включая вопросы о мерах обеспечения безопасности на платформе, например, сканирование уязвимостей или тесты на проникновение.

Еще одним важным аспектом обеспечения безопасности приложения является безопасность API – область, раскрывающая данные и цифровые активы организации. При использовании инструментов с низким уровнем кода безопасность API должна иметь первостепенное значение. Для предотвращения угроз безопасности может

быть использована защита вызовов API или REST с помощью аутентификации, токенизации или с помощью шлюза API [5].

Организациям необходимо проводить обучение «citizen developers» – пользователей, которые при помощи Low-code инструментов разрабатывают ИТ-решения (например, бизнес или системные аналитики), так как citizen developers, как правило, не обучаются методам обеспечения безопасности приложений. Обучение может включать упражнения по безопасности, чтобы обучить аналитиков основам, например, прямая атака на приложение для поиска недостатков.

Кроме этого, Low-code платформа должна обладать следующими функциями для обеспечения безопасности: должна быть настроена в защищенном частном облаке; применять передовые методы программирования (соглашения о кодировании, шаблоны проектирования и шифрование данных) для автоматически сгенерированного кода и пользовательского кода, написанного разработчиком; иметь сертификаты, подтверждающие качество и безопасность кода; должна поддерживать несколько поставщиков аутентификации (база данных, протокол LDAP, служба каталогов AD, механизм единого входа SSO, язык разметки SAML, стандарт передачи данных OpenID, многофакторные, биометрические) для создания приложения с высокой безопасность пользователей [4].

Также в Low-code платформах защита информации обеспечивается с помощью разграничения прав доступа и контроля за внесением изменений в программе. В приложении настраиваются роли с определенным действиями, которые может совершать пользователь, после чего пользователю выдаются необходимые роли. Кроме этого, в разработанном с помощью Low-code приложении ведется аудит действий пользователей, позволяющий отследить историчность их действий.

Современные платформы требовательны к защите программ и хранящейся в них информации, поэтому содержат необходимые инструменты администрирования, контроля доступа и оценки угроз. Это позволяет легко настраивать и контролировать безопасность системы. Таким образом, команды разработчиков могут использовать технологии Low-code, соблюдая при этом передовые методы безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Модели цифровизации экономической деятельности: [монография] / [Х.И. Аминов, И.Л. Андреевский, Г.Г. Безрук и др.]; [редкол.: Андреевский И.Л. и др.]. – СПб.: Изд-во СПбГЭУ, 2019. – 179 с.
2. Колбанев М. О., Коршунов И. Л., Левкин И. М. Информатизация и информационно-экономическая безопасность //Россия и Санкт-Петербург: экономика и образование в XXI веке. – 2016. – С. 159-163.
3. Реализация Low-code концепции в системе Creatio // Террасофт: сайт. – URL: https://www.terrasoft.ru/our-technologies/low-code (дата обращения: 17.06.2021 г.).
4. Is Low-Code Development a Security Risk? - DevOps.com [Электронный ресурс]. – Режим доступа: https://devops.com/is-low-code-development-a-security-risk/. – Заглавие с экрана. – (Дата обращения: 19.06.2021).
5. 3 Tips to Lower the Security Risk of Low-Code Developer Tools [Электронный ресурс]. – Режим доступа: https://www.reworked.co/digital-workplace/are-no-code-and-low-code-developer-tools-a-security-risk/. – Заглавие с экрана. – (Дата обращения: 22.06.2021).

УДК 004.946

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Степанов Константин Сергеевич
Нижегородский государственный инженерно-экономический университет
Октябрьская ул., 22а, Княгинино, 606340, Россия
e-mail: kostj1997@mail.ru

Аннотация. В работе рассматриваются основные возможности и особенности технологий виртуальной реальности, способные оказать поддержку при обеспечении необходимой степени информационно-экономической защищенности организации.

Ключевые слова: виртуальная реальность; защита информации; информационная безопасность.

VIRTUAL REALITY AS A TOOL FOR PROVIDING INFORMATION AND ECONOMIC SECURITY OF THE ORGANIZATION

Stepanov Konstantin
Nizhny Novgorod state University of engineering and Economics
22A Oktyabrskaya St, Knyaginino, 606340, Russia
e-mail: kostj1997@mail.ru

Abstract. The paper discusses the main capabilities and features of virtual reality technologies that can provide support while ensuring the required degree of information and economic security of the organization.

Keywords: information security; protection of information; virtual reality.

В настоящее время обеспечение информационной безопасности любой организации является очень важной составляющей ее деятельности наряду с постоянной оптимизацией бизнес-процессов и повышением квалификации кадров. Все эти процессы позволяют сохранять конкурентоспособность и привлекательность организации на рынке.

В свою очередь, информационная безопасность на сегодняшний день неразрывно связана с экономической безопасностью и с данной точки зрения представляет собой защищенность деятельности организации и ее информационной среды от негативного влияния дестабилизирующих факторов, которая обеспечивает сохранность основных свойств информации и достижение определенных экономических целей [3].

Важно отметить, что обеспечение безопасности информации – это непрерывный процесс, так как постоянно изменяющиеся информационные ресурсы, средства и системы информатизации и деятельность злоумышленников приводят к возникновению различных угроз безопасности [2].

Таким образом, ставится задача, заключающаяся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования и развития системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий [1].

Одним из инструментов, помогающих в решении данной задачи, может являться применение технологий виртуальной реальности. Актуальность данных технологий будет заключаться в очень высоком уровне их иммерсивности, то есть способности к созданию эффекта присутствия или погружения. При этом можно выделить несколько сценариев использования данных технологий в процессе создания или использования системы информационной безопасности.

Во-первых, с помощью VR-технологий возможно воссоздать деятельность определенного отдела организации и проследить за всеми внутренними перемещениями информационных потоков. Такая визуализация в перспективе может помочь в выявлении потенциальных слабых мест системы защиты.

Во-вторых, с помощью технологий виртуальной реальности появляется возможность произвести анализ существующей системы защиты информации, к примеру, ее аппаратного обеспечения. То есть, у администраторов системы появляется возможность визуально отслеживать области покрытия камер видеонаблюдения, местонахождение и состояние различных охранных датчиков и устройств.

В-третьих, текущий уровень развития VR-устройств позволяет сымитировать большинство угроз безопасности и проанализировать их последствия. Так, пользователь VR-системы может почувствовать себя в роли злоумышленника и попытаться произвести взлом системы безопасности или нанести ущерб информационным потокам. Полученные же в ходе эксперимента данные в дальнейшем можно использовать для совершенствования системы защиты.

Таким образом, VR-технологии являются эффективным инструментом, имеющим неоспоримые достоинства, и они могут быть использованы как в роли одного из способов совершенствования системы защиты информации в организации, так и в качестве составной части данной системы.

СПИСОК ЛИТЕРАТУРЫ

1. Гомалеев А. О. Информационная безопасность как составляющая экономической безопасности организации // Научно-практический электронный журнал Аллея Науки. 2018, № 10(26). С. 993-998.
2. Злыгостев Д. Д, Зарипова Р. С. Информационная безопасность как инструмент обеспечения экономической безопасности предприятий // Инновации в информационных технологиях, машиностроении и автотранспорте. 2017. С. 23-25.
3. Колбанев М.О., Коршунов И. Л, Левкин И. М., Микадзе С. Ю. К вопросу об информационно-экономической безопасности общества // Геополитика и безопасность. 2015, № 3(31). С. 87-91.

УДК 334.02

DLP-СИСТЕМА КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

Филатова Татьяна Александровна
Санкт-Петербургский государственный экономический университет
Садовая ул., 21, Санкт-Петербург, 191023, Россия
e-mail: werck@rambler.ru

Аннотация. Рассматривается применение DLP-систем как инструмента обеспечения информационной безопасности компании для потенциальной защиты информации и эффективности работы персонала в период удаленной работы.

Ключевые слова: DLP-система; удаленная работа; информационная безопасность; защита данных.

DLP-SYSTEM AS A TOOL FOR ENSURING INFORMATION SECURITY OF A COMPANY

Filatova Tatiana
Saint-Petersburg State University of Economics
21 Sadovaya St, St. Petersburg, 191023, Russia
e-mail: werck@rambler.ru

Abstract. The article considers the use of DLP systems as a tool for ensuring information security of a company for the potential protection of information and the effectiveness of personnel during the period of remote work.

Keywords: DLP system; remote work; information security; data protection.

В российской экономике наметился новый тренд - массовый переход на удаленную деятельность компании. После окончания пандемии формат дистанционной работы не потеряет свою актуальность, так как модернизируется процесс труда и усиливается влияние инноваций, повышающие эффективность результата.

Эти утверждения косвенно подтверждают исследования в различных секторах экономики, проведенные на территории России [1].

В связи с этим защита данных любой организации имеет огромную ценность, так как будет потеряна монополия над ней. Более того, некоторая информация может нанести ущерб репутации компании. Каждый руководитель понимает, что данные необходимо беречь. Утечки случаются как случайно, так и намеренно, поэтому должен быть способ их предотвратить. Один из таких способов - настроить DLP-систему (Data Leak Prevention).

Руководство компаний решает внедрить систему по нескольким причинам: она предотвращает утечку конфиденциальных данных, показывает рабочий процесс сотрудников и косвенно рекомендована властями [2].

Есть разные типы DLP-систем, и к выбору нужно отнестись предельно серьезно. Лучший способ понять, удобна ли система в использовании и эффективна в работе - это протестировать ее. Многие производители предоставляют потенциальным клиентам такую возможность. Это помогает объективно оценить преимущества продукта.

С 2020 года компании по всему миру перевели своих сотрудников на работу удаленно. В этих условиях стало сложно контролировать рабочий процесс сотрудников. Именно поэтому возрос спрос на DLP-системы.

Домашняя среда менее безопасна и менее контролируема, поэтому риск утечки данных возрастает. Информирование сотрудников о настройке DLP-системы влияет на эффективность их работы. Персонал перестает тратить время на посторонние вопросы, чтобы больше работать. Участились случаи увольнения персонала, потому что проверка DLP-системы показала, что часть сотрудников тратит время на просмотр фильмов, чтение статей, не связанных с работой, игры, общение в соцсетях [3]. Внедрение системы и информирование об этом персонала привело к повышению эффективности работы персонала и снижению потерь времени.

DLP-систему нельзя считать щитом, исключающим утечку конфиденциальных данных, система сводит к минимуму риск утечки. Она отслеживает и предоставляет функцию запрета, например, печати документов, копирования текстов или открытия записей. Однако это не панацея, ведь способы обхода системы все еще существуют.

Есть утверждение, что использование DLP-системы неэтично, так как она вторгается в личную переписку сотрудников, перехватывает их аудио- и видеосообщения, поисковые запросы. Каждый имеет право на тайну переписки. Но сотрудник работает на территории предприятия, пользуется его ресурсами, поэтому в рабочее время нет места для личной переписки. Работодатели уведомляют сотрудников, что их рабочий процесс будет отслеживаться. Они также предоставляют им согласие на обработку данных и закон регулирует ситуации общего характера. Остальные вопросы регулируются исходя из особенностей сферы деятельности компании.

В 2020 году появились усовершенствованные DLP-систем с обновленным функционалом, позволяющий переводить сотрудников на удаленную работу без проблем с контролем и защитой данных, которые применяются в настоящее время.

СПИСОК ЛИТЕРАТУРЫ

1. Пандемия COVID-19: кризис офлайн и рост онлайн [Электронный ресурс] // Режим доступа: https://stakhanovets.ru/blog/pandemiya-covid-19-krizis-i-rost-onlajn/ (дата обращения: 10.09.2021)
2. Аналитика систем предотвращение утечек данных [Электронный ресурс] / Блог компании МИПКО – Режим доступа: https://www.mipko.ru/blog/2020/02/dlp-sistems/ (дата обращения 10.09.2021).
3. Утечки информации ограниченного доступа [Электронный ресурс] / Отчет экспертно-аналитического центра InfoWatch – Режим доступа: https://d-russia.ru/wp-content/uploads/2020/12/infowatch_2020_9_monts_data_leak.pdf (дата обращения 10.09.2021).

УДК 004.056

ОБ УГРОЗАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Шарафанова Елена Евгеньевна
Санкт-Петербургский государственный экономический университет
канала Грибоедова наб., 30-32, Санкт-Петербург, 191023, Россия
e-mail: el_siver@mail.ru

Аннотация. Представлены угрозы информационной безопасности дистанционного образования и факторы, обусловливающие их влияние на учебный процесс.

Ключевые слова: дистанционное обучение; угрозы; информационная безопасность; несанкционированный доступ.

ABOUT THE THREATS TO THE INFORMATION SECURITY OF DISTANCE LEARNING

Sharafanova Elena
Saint-Petersburg State University of Economics
30-32 Griboyedov Canal, St. Petersburg, 191023, Russia
e-mail: el_siver@mail.ru

Abstract. The article presents the threats to the information security of distance education and the factors that determine their impact on the educational process.

Keywords: distance learning; threats; information security; unauthorized access.

Пандемия новой коронавирусной инфекции, ставшая причиной шокового сжатия мировой экономики, породила резкий рост спроса на интернет-услуги. Заметное увеличение объемов продаж показали компании, предлагающие цифровые решения для удаленной работы, электронная коммерция, телемедицина, виртуальный туризм, видеосервисы и он-лайн кинотеатры, IT-решения в сфере доставки, производство и продажа робототехники и дронов, управление поставками на основе больших данных, облачных вычислений, интернета вещей и блокчейна, 3-D печать, системы он-лайн платежей, обеспечивающие бесконтактную оплаты, технология 5G [1]. В числе лидеров – услуги онлайн (дистанционного) образования. Рост количества и интенсивность использования интернет-услуг, в том числе неопытными пользователями, сопровождался не только активизаций мошеннических действий, но и появлением различных угроз, связанных со спецификой удаленной работы, а именно: дискретизация работника в результате несанкционированного подключения, действий и высказываний злоумышленников к мероприятиям, проводимым в режиме видеоконференции; утечка личных или корпоративных данных вследствие отсутствия двухфаторной аутентификации, ненадежных паролей, вирусных и фишинговых атак [2]; рост психических расстройств в результате распространения в сети панических слухов о течении пандемии. По данным исследования, проведенного «Лабораторией Касперского» количество атак на платформу Zoom только в первом полугодии 2020 г. увеличилось в 1400 раз. Популярный мессенджер Whatsapp, широкого используемых для коммуникаций преподаватель-студент, преподаватель-преподаватель, администрация-преподаватель, в числе прочих уязвимостей, позволял при отправке подготовленного стикера узнать IP-адрес компьютера отправителя. [3] Фактором, снижающем возможности преподавателя противодействовать угрозам кибербезопасности, является высокая вероятность ухудшения здоровья вследствие увеличения продолжительности времени работы на компьютере (по субъективным оценкам преподавателей до 8-10 часов в день) и вытекающего из этого снижения концентрации внимания, пренебрежения стандартными средствами защиты, уменьшения критичности восприятия писем, рассылок и сообщений. Кроме того, усиливать или провоцировать угрозы несанционированного доступа в онлайн-аудиторию могут обучающиеся, не справляющиеся с изолированностью от преподавателя и студенческого социума и передающие пароли доступа пранкерами и троллям. Отсутствие полноценного общения и воспитательного процесса приводит к «стайному» объединению молодых людей в сетях, целью которого может стать троллинг как учебных заведений, так и конкретных преподавателей. Опасность представляет также все более распространяющийся зумбомбинг, представляющий собой атаку конференции в режиме онлайн несанционированными видеороликами, в том числе содержащими порноконтент. Вынужденный опыт дистанционного обучения позволил определить границы его конструктивного применения, который можно и нужно будет использовать по окончании пандемии. Но навыки противодействия выявившимся угрозам должны войти в перечень необходимых компетенций преподавателей с учетом рациональных требований к режиму труда и отдыха при работе на компьютере.

СПИСОК ЛИТЕРАТУРЫ

1. 10 ИТ-отраслей, которым пандемия дала мощный импульс к развитию [Электронный ресурс]. URL: https://hightech.fm/2020/11/06/ten-it-pandemic (Дата обращения 11.09.2021).
2. Об угрозах безопасности информации, связанных с пандемией коронавируса (COVID-19.) [Электронный ресурс]. URL: https://safe-surf.ru/upload/ALRT/ALRT-20200320.1.pdf (Дата обращения 12.09.2021).
3. Security Week 37: атаки на системы дистанционного обучения [Электронный ресурс]. URL: https://habr.com/ru/company/kaspersky/blog/518140/ (Дата обращения 11.09.2021).

УДК 004

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ АСПЕКТЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ СИСТЕМ ЭЛЕКТРОННОЙ ТОРГОВЛИ

Шилков Владимир Ильич, Аденин Семен Михайлович
Уральский федеральный университет имени первого Президента России Б.Н. Ельцина
Мира ул., 19, Екатеринбург, 620002, Россия
e-mails: shilkov-urfu@yandex.ru, semen.dustov@urfu.me

Аннотация. Предлагаются трактовки терминов электронная торговля, электронная коммерция, интернет-магазин, электронная торговая площадка (ЭТП). Предлагается для обсуждения формулировка термина информационно-экономическая безопасность электронной торговли. Обсуждаются организационно-технологические, экономические и информационные риски электронной торговли, связанные с новыми проблемами, целями, задачами и информационно-технологическими решениями. Обсуждаются проблемы управления информационно-экономической безопасностью систем электронной торговли. Предлагаются возможные организационно-технические мероприятия по повышению информационно-экономической безопасности электронной торговли.

Ключевые слова: цифровизация; электронная торговля и коммерция; электронная торговая площадка (ЭТП); риски; информационно-экономическая безопасность.

ORGANIZATIONAL AND TECHNICAL ASPECTS OF MANAGEMENT INFORMATION AND ECONOMIC SECURITY E-COMMERCE SYSTEMS

Shilkov Vladimir, Adenin Semyon
Ural Federal University named after the first President of Russia B.N. Yeltsin
19 Mira St, Yekaterinburg, 620002, Russia
e-mails: shilkov-urfu@yandex.ru, semen.dustov@urfu.me

Abstract. Interpretations of the terms e-commerce, e-commerce, online store, electronic trading platform are proposed. The wording of the term information and economic security of electronic commerce is proposed for discussion. The organizational, technological, economic and information risks of e-commerce related to new problems, goals, tasks and information technology solutions are discussed. The problems of managing the information and economic security of e-commerce systems are discussed. Possible organizational and technical measures to improve the information and economic security of electronic commerce are proposed.

Keywords: digitalization; electronic commerce; electronic trading platform; risks; information and economic security.

Одним из направлений повышения качества управления сложными социально-экономическими системами является цифровая трансформация процессов за счет широкого внедрения информационных технологий и искусственного интеллекта. Развитие информационно-коммуникационных технологий (ИКТ) сделало возможным к возникновение специфических форм торговли, которые могут быть отнесены к электронной коммерции и электронной торговле и, которые используя различные онлайн-сервисы, предполагают покупку или продажу товаров через сети Интернет. Следует отметить, что по мнению авторов данной статьи, вопросы применения дефиниций электронная коммерция (от лат.commercium - торговля) и электронной торговля нуждаются в дальнейшем обсуждении.

Как правило, под термином интернет-магазин, понимают сайт в сети Интернет, с помощью которого осуществляется торговля товарами в розницу. В этом смысле, интернет-магазин представляет собой правовую организационно-техническую форму, с помощью которой клиенты совершают покупки, а продавцы реализуют товары и получают прибыль. Под термином электронная торговая площадка (ЭТП) часто понимают интернет-ресурс, являющийся виртуальным рабочим местом, где не только заключаются сделки купли-продажи между предприятиями, но и могут быть организованы различные конкурсы и аукционы различных типов. Торговые операции на ЭТП обеспечивают организаторам площадки получение дохода, как правило, за счет комиссии от проведенных сделок.

К функциям электронной торговли, в широком смысле этого термина, могут быть отнесены, например, электронный маркетинг, связанный не только с рекламированием товаров и услуг, но и с выполнением задач по поиску покупателей, посредников и поставщиков комплектующих элементов; сбор данных на основе автоматизированных систем; управление цепочками поставок; управление запасами; электронный обмен информацией и анализ эффективности торговых операций; электронные денежные операции, включающие онлайн-обработку транзакций и электронные переводы средств.

Информационно-экономические функции, реализуемые в ходе торговых бизнес-процессов, поддерживаются компьютерными сетями, построенными на основе соответствующих программно-аппаратных средств. Как отмечено в работах [1, 2], в электронной коммерции электронный сетевой обмен данными связывают с электронной почтой, а также с информационными и финансовыми транзакциями, которые с учетом необходимости обеспечения гарантированного уровня информационной безопасности являются дорогостоящими операциями.

Можно утверждать, что электронная торговля представляет собой сложную динамическую систему с большим количеством элементов и связей. Сложность системы в ряде случаев является причиной возникновения различных видов рисков. В частности, организационно-технологические компоненты комплекса, обеспечивающие процесс электронной торговли могут подвергнуться негативному воздействию со стороны третьих лиц. К таким компонентам могут быть отнесены не только традиционные браузеры, но и, например, мобильные и стационарные программные интерфейсы приложений (API), обеспечивающие взаимодействие между различными сервисами внутри компании, а также с сервисами партнеров; биллинговые и процессинговые комплексы, приложения, используемые компаниями для внутренних целей.

В качестве одной из важнейших и актуальных проблем электронной торговли можно считать проблему обеспечения ее информационно-экономической безопасности, что обусловлено не только глобальными процессами цифровизации всей мировой экономики и, в частности, увеличением объемов торговых операций через социальные сети, интернет-магазины, различные сервисы и приложения, но и возрастающими рисками несанкционированных вмешательств в работу компьютерных систем.

В связи с данным обстоятельством в работе [3] отмечены негативные аспекты применения информационных технологий, которые связаны с опасениями пользователей интернета относительно степени защищенности личной информации при проведении деловых операций. Основные опасения могут проявляться, например, в сомнениях относительно эффективности защиты частных сведений и отсутствием гарантий о неразглашении персональных идентификационных данных их сетевыми получателями, а также с рисками

несанкционированных вторжений в частное киберпространство, например, вместе с принудительно навязываемыми рекламными материалами.

Автор работы [4] обращает внимание на то, что при получении третьими лицами персональных данных потенциального покупателя, например, адресов электронной почты, номера телефона или домашнего адреса существуют трудности в последующем установлении вины конкретных лиц, ответственных за дальнейшее несанкционированное распространение персональной информации.

Предлагаем для обсуждения следующую формулировку термина информационно-экономическая безопасность электронной торговли.

Под информационно-экономической безопасностью электронной торговли можно понимать такое состояние совокупности организационно-технических средств, участвующих в обеспечении процессов совершения торговых операций и реализуемых на основе комплекса информационно-коммуникационных технологий, при котором, возможные риски возникновения случайных обстоятельств или несанкционированного вмешательства третьих лиц не могут оказать негативного влияния на результаты, которые предполагается достигать в ходе торговых операций в долгосрочной перспективе с использованием данного информационного ресурса.

Задача управления информационно-экономической безопасностью систем электронной торговли состоит в принятии решений, обеспечивающих оптимальное отношение результатов, достигаемых участниками торговых операций к затратам, необходимым для достижения этих результатов. В [5] отмечено, что если осторожный покупатель не может оценить степень безопасности торговой сделки на рынке электронной торговли или вынужден осуществлять слишком большие затраты по обеспечению безопасности этой сделки, то он, как правило, покидает рынок.

В том случае, если информационная среда рынка электронной торговли не является защищенной и безопасной средой, то конкретный продавец или организатор системы электронной торговли, чтобы не потерять покупателя должны будут понести дополнительные затраты, чтобы обеспечить приемлемый для покупателя уровень информационной безопасности.

Для решения задачи повышения уровня информационно-экономической безопасности электронной торговли рекомендуем принять во внимание, что в дальнейшей проработке нуждаются: модели рынков электронной торговли; концепция построения системы информационно-экономической безопасности электронной торговли; методы тестирования и оценки вероятности возникновения специфических угроз со стороны новых ИКТ, процессов преобразования информации и организационных процедур; методики обучения всех участников электронных торговых операций (покупателей, продавцов и организаторов электронных торговых площадок) правилам информационной гигиены и методам безопасной работы в системах электронной торговли.

СПИСОК ЛИТЕРАТУРЫ

1. Защита систем Интернет-торговли. Халиуллина Э.И. // NovaInfo. 2016. №47-3. С. 12-15.
2. Understanding use of consumer protection tools among Internet gambling customers: Utility of the Theory of Planned Behavior and Theory of Reasoned Action. Procter L., Angus D.J., Gainsbury S.M. // Addictive Behaviors. 2019. Vol. 99. P. 106-125.
3. Основные направления обеспечения качества электронной торговли. И. М. Сафарова, А. С. Акимкина, А. И. Дерябина // Экономика и управление: новые вызовы и перспективы. – 2010. – № 1. – С. 312-316.
4. Ответственность за нарушение правил обработки и хранения персональных данных при осуществлении электронной торговли. Расторгуева А.С. // Актуальные проблемы правоведения. 2018. № 1 (57). С. 20-21.
5. Безопасность рынка электронной торговли с точки зрения трансакционных издержек. Валько Д.В. // Национальные интересы: приоритеты и безопасность. 2012. Т. 8. № 12 (153). С. 59-64.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ИМПОРТОЗАМЕЩЕНИЕ В КРИТИЧЕСКИХ ИНФРАСТРУКТУРАХ

УДК 629.12

ТЕОРИЯ ПРАКТИКИ КВАЛИМЕТРИЧЕСКОГО АНАЛИЗА ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Алексеев Анатолий Владимирович[1], Согонов Сергей Александрович[1], Потехин Владимир Семенович[2], Мусатенко Роман Иванович[2]

[1] Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
[2] Военный учебно-научный центр Военно-Морского флота «Военно-Морская академия им. Н.Г. Кузнецова»
Ушаковская наб., 17/1, Санкт-Петербург, 197045, Россия
e-mail: iapbgks@bk.ru

Аннотация. Обобщены положения теории и практики анализа объектов критической информационной инфраструктуры (КИИ) на основе аппарата квалиметрического оценивания, мониторинга и анализа информационной обстановки. В развитие полимодельного квалиметрического метода системной оптимизации (ПКМ СО) объектов КИИ приведена система критериев и математическая модель оценки, мониторинга и анализа качества управления комплексной безопасностью как меры обеспечения жизненно важных интересов объектов КИИ от внутренних и внешних угроз субъективного и объективного характера. Обоснована целесообразность и пути её реализации в обеспечение требований ФЗ-187 на основе непрерывного системного мониторинга и управления качеством комплексной безопасности объектов КИИ по технологии типа «СПРУ». Приведены основные методические аспекты повышения квалификации специалистов, работающих в области обеспечения безопасности значимых объектов критической информационной инфраструктуры.

Ключевые слова: теория практики; объекты критической информационной инфраструктуры; квалиметрический анализ; математическая модель оценки свойств и качества управления безопасностью.

THEORY AND PRACTICE OF QUALIMETRIC ANALYSIS OF OBJECTS CRITICAL INFORMATION INFRASTRUCTURE

Alekseyev Anatoly[1], Sogonov Sergey[1], Potekhin Vladimir[2], Mussatenko Roman[2]

[1] St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
[2] Military training and research center of the Navy «Naval Academy named after N. G. Kuznetsov»
17/1 Ushakovskaya Emb, St. Petersburg, 197045, Russia
e-mail: iapbgks@bk.ru

Abstract. The provisions of the theory and practice of analyzing objects of critical information infrastructure (CII) on the basis of the apparatus of qualimetric assessment, monitoring and analysis of the information situation are summarized. A system of criteria and a mathematical model for evaluating, monitoring and analyzing the quality of integrated security management as a measure to ensure the vital interests of CII objects from internal and external threats of a subjective and objective nature is presented in the development of the polymodel qualimetric method of system optimization (PCM SO) of CII objects. The expediency and ways of its implementation in ensuring the requirements of FZ-187 on the basis of continuous system monitoring and quality management of integrated safety of CII facilities using the SPRU type technology are substantiated. The main methodological aspects of professional development of specialists working in the field of ensuring the security of significant objects of critical information infrastructure are presented.

Keywords: theory of practice; objects of critical information infrastructure; qualimetric analysis; mathematical model for assessing the properties and quality of security management.

Большая часть современных объектов морской техники и морской инфраструктуры (ОМТИ) в соответствии с Федеральным законом 187 от 26.07.2017 в полной мере относится к объектам КИИ. ОМТИ сфер оборонной техники, военной науки, атомной морской энергетики характеризуются целым рядом уникальных свойств, определяемых внедрением новых технологий в информационно-коммуникационные системы, комплексы автоматизации, обработки, визуализации информации и управления безопасностью ОМТИ [1 - 5].

При этом, высокая информационная критичность систем управления комплексной безопасностью (СУКБ) к внешним и внутренним факторам сегодня обуславливает необходимость особого внимания и высокой

требовательности к проектному качеству (ПК) Q и эффективности управления (ЭУ) W=$Q_{\text{Р}}/Q$ при эксплуатации объектов КИИ ($Q_{\text{Р}}$ - значение ПК, рассчитанное по методике оценки ПК, но при использовании реализованных значений частных показателей (ЧПК) качества), определяемым ключевыми критериями и соответствующими показателями оперативности (своевременности) управления O, достоверности используемых для управления данных D, устойчивости U, скрытности S и непрерывности N управления, а также его ресурсной обеспеченности R при соответствующих индексах критериальной значимости (ИКЗ) o, d, u, s, n, r.

Сегодня информационная критичность СУКБ, как правило, «нейтрализуется» путем внедрения современных организации и технологий защиты информации, повышения надежности используемых средств и ОМТИ в целом, резервирования контуров управления, повышения степени автоматизации решаемых задач, совершенствования и эффективного использования систем поддержки принятия решений в контурах автоматизированного управления, а также соответствующей подготовки и повышения квалификации специалистов, обеспечивающих безопасность значимых объектов КИИ.

В обеспечение безопасности объектов КИИ, по нашему мнению, наряду с отработанными вопросами (категорирования, взаимодействия с системой «ГосСОПКА», своевременным принятием мер по обеспечению безопасности элементов КИИ) каждый ОМТИ должен обладать собственной совершенной СУКБ, включая ситуационный центр управления комплексной безопасностью [5 - 7].

Это позволит в рамках концепции распределённого управления обеспечить главные требования к качеству управления безопасностью –того объекта КИИ $Q \geq Q_{\text{тр}}$ и $W \geq W_{\text{тр}}$ (с учетом специфических условий эксплуатации) в соответствии с математической моделью оценки качества СУКБ в развитие данных [7]

$$Q = C_M^{\text{А}}\{w_m, C_{m,7}^{\text{М}}[w_g, C_{g,N}^{\Gamma}(w_n, q_n)]\}, \quad (1)$$

где: $C_{g,N}^{\Gamma}(w_n, q_n)$, $C_{m,7}^{\text{М}}[w_g, \dots]$, $C_M^{\text{А}}\{w_m, \dots\}$ – соответствующие обобщенные операторы свертки ЧПК СУКБ q_n при их общем числе N (как правило, не менее 30, включая конфиденциальность, доступность, целостность используемой при управлении информации) в g - ый групповой показатель качества (ГПК) при их общем числе $G = 7$ (включая в дополнение к выше приведенным ГПК O, D, U, S, N, R, отражающим свойства управления, также субъективные (позитивные и негативные) свойства операторов СКУБ F с соответствующим значением ИКЗ f). Соответственно свертки ГПК в модельный показатель качества (МПК) при принятом их общем числе M и МПК в АПК по алгоритму типа (указан верхним индексом у оператора свертки) для: аддитивного (линейного) алгоритма (А), впервые предложенного А.Н. Крыловым; мультипликативного алгоритма (М), предложенного Д. Нэшем; гармонического алгоритма (Г) и возможных других алгоритмов свертки.

Наличие системного показателя (1) позволяет обоснованно решать основную задачу исследовательского обоснования структуры, функциональных задач, свойств и характеристик СУКБ на всех этапах жизненного цикла известными современными методами системного анализа, вариантного синтеза технологического развития объектов КИИ ОМТИ, включая представленные в [8 - 9].

Опыт исследовательского проектирования разнородных ОМТИ [3-6] показывает, что принципиально важным требованием в обеспечение заданных требований по качеству управления КИИ является наличие и непрерывное эффективное использование автоматизированных систем мониторинга (непрерывного наблюдения) за состоянием СУКБ по системным показателям типа (1). А также - информационно-аналитическая и интеллектуальная поддержка принятия решений и управления по технологии типа «СПРУ» [2 -6], основные свойства и преимущества которой приведены на рис. 1 в [4]. Еще более значимым системным аспектом циклического управления развитием критическими ОМТИ является минимизация их структурной, функциональной избыточности за счет научно обоснованной полимодельной системной оптимизации СКУБ, например, путем вариантной максимизации функционала (1). Таким образом, в современных условиях развития объектов КИИ первостепенное внимание при наращивании их возможностей и качества следует уделять именно системным показателям качества типа (1) на основе количественного измерения, оценивания, системного анализа и вариантного синтеза проектного качества и эффективности функционирования СУКБ.

Это позволяет адекватно оценивать ситуационную обстановку на объекте и принимать рациональные (безошибочные, эффективные, оптимальные) управленческие решения, в том числе минимизировать влияние негативных субъективных свойств операторов, включая тренажерную подготовку в процессе подготовки и повышения квалификации специалистов, обеспечивающих безопасность значимых объектов КИИ. Приведены основные методические аспекты подготовки, переподготовки кадров, повышения квалификации специалистов.

Обоснована целесообразность и пути реализации теории практики анализа объектов КИИ в обеспечение требований ФЗ-187 на основе мониторинга и управления качеством СКУБ по технологии типа «СПРУ» [3 - 6].

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В., Воробьев В.И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с. 153 – 159.
2. 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). XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2021 г.: Материалы конференции / СПОИСУ. – СПб., 2021.
3. Алексеев А.В., Тычинин И.Ю., Худобородов Е.Ф. Теория практики системного обоснования требований и путей обеспечения военно-технического превосходства ВМФ / Актуальные проблемы морской энергетики: материалы восьмой международной НТК в рамках Третьего Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». - СПб., 2019, с.251–357.
4. Алексеев А.В., Тычинин И.Ю., Мусатенко Р.И., Потехин В.С., Худобородов Е.Ф. Системный анализ и вариантный синтез технологического развития объектов критической информационной инфраструктуры / Актуальные проблемы морской энергетики:

материалы девятой международной научно-технической конференции в рамках Четвертого Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2020, с. 359 - 363.
5. Волков В.И., Тычинин И.Ю., Алексеев А.В. Системные аспекты управления развитием современных критических объектов морской техники и морской инфраструктуры / XIV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2014)». Санкт-Петербург, 29-31 октября 2014 г.: Материалы конференции \ СПОИСУ. – СПб, 2014. С. 447–448.
6. 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). Изд. ФГБУ «РАРАН». Москва – 2018. С. 344 - 347.
7. Алексеев А.В., Мусатенко Р.И., Тычинин И.Ю. Системный мониторинг при интеллектуальной поддержке управления критических объектов / Материалы конференции «Информационные технологии в управлении». – СПб.: ЦНИИ «Электроприбор», 2018, с. 161- 165.
8. Алексеев А.В., Тычинин И.Ю., Мусатенко Р.И., Согонов С.А., Потехин В.С., Худобородов Е.Ф. Концепция роботизации управления как средства гарантированной поддержки качества функционирования критических объектов / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 5. – СПб., 2018, с. 442 – 446.
9. Алексеев А.В., Карпов А.Е., Мусатенко Р.И., Потехин В.С., Худобородов Е.Ф. От мониторинга данных к мониторингу процессов объектов морской техники / Региональная информатика (РИ-2016). Юбилейная XV Санкт-Петербургская международная конференция «Региональная информатика (РИ-2016)». Санкт-Петербург, 26-28 октября 2016 г.: Материалы конференции. \ СПОИСУ. - СПб, 2016, с. 426-427.

УДК 004.41

О КОМПЛЕКСЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОЦЕНКИ ПОКАЗАТЕЛЕЙ ДОЛГОВЕЧНОСТИ СТРУКТУРНО И ФУНКЦИОНАЛЬНО СЛОЖНЫХ СИСТЕМ С ДЛИТЕЛЬНЫМИ СРОКАМИ АКТИВНОГО СУЩЕСТВОВАНИЯ

Волков Александр Владиславович, Острейковский Владислав Алексеевич
Сургутский государственный университет
Ленина пр., 1, Сургут, 628412, Россия
e-mails: volk_234@mail.ru, academicostr@yandex.ru

Аннотация. В статье предлагается использование комплекса программного обеспечения для применения существующих методов оценки показателей долговечности структурно и функционально сложных критически важных систем, учитывающих асимметрию внутреннего времени. Сформулированы основные требования к разрабатываемому программному обеспечению и его структура.

Ключевые слова: информационные системы; долговечность; ресурс; срок службы или остаточные значения; необратимые процессы; асимметрия времени.

ABOUT THE SOFTWARE COMPLEX FOR EVALUATING DURABILITY INDICATORS OF STRUCTURALLY AND FUNCTIONALLY COMPLEX SYSTEMS WITH LONG LIFE

Volkov Aleksandr, Ostreikovskii Vladislav
Surgut State University
1 Lenin Av, Surgut, 628412, Russia
e-mails: volk_234@mail.ru, academicostr@yandex.ru

Abstract. The article proposes the use of software for the use of methods of indicators of durability of structurally and complex critical systems, considering the asymmetry of internal time. The basic requirements for the developed software and its structure are formulated.

Keywords: information systems; durability; resource; service life or residual values; irreversible processes; asymmetry of time.

Обеспечение непрерывной эксплуатации многих структурно и функционально сложных систем (СФСС), таких как ядерные энергетические установки (ЯЭУ), авиационные и космические комплексы, системы транспортировки нефти и газа имеет критически важное значение. Поэтому, на этапе проектирования таких систем важным является определение срока их эксплуатации.

Существующие в настоящее время детерминированные и вероятностные методы оценки показателей долговечности СФСС не учитывают нелинейную траекторию поведения элементов системы, возникшую вследствие внутренних необратимых процессов [1]. Для решения этой проблемы предлагается использовать новый подход к оценке параметров долговечности в модусах «прошлое – настоящее – будущее» [2].

Характер СФСС влечет за собой сложность расчёта её безаварийного срока эксплуатации, а критическая важность такой системы несёт за собой высокие требования к квалификации специалистов. Вследствие тесной взаимосвязанности элементов СФСС, изменение параметров одного из элементов системы влечет за собой пересчет показателей долговечности не только измененного элемента, но и всей системы в целом.

Потребность в создании программного обеспечения для оценки показателей долговечности СФСС вызвана отсутствием существующих программных средств, решающих эти вопросы.

В статье решаются два вопроса:

- Требования к разрабатываемому ПО
- Структура разрабатываемого ПО

Основные требования разрабатываемого ПО:

– ПО должно иметь интерфейс, понятный для использования рядовому пользователю персонального компьютера.

– Формы ввода данных должны проходить предварительную валидацию для исключения ввода неадекватных данных.

– Расчёт параметров долговечности СФСС должен быть произведён в соответствии с выбранным пользователем методом.

– В качестве показателей долговечности рассматриваются следующие показатели: средний ресурс, гамма-процентный ресурс, срок службы, гамма-процентный срок службы [3].

– Выполненный расчёт должен сохраняться в памяти с возможностью последующей его загрузки.

– Так же необходимо предусмотреть возможность печати отчёта по выполненным расчётам.

Структура разрабатываемого ПО:

– Модуль пользовательского интерфейса. Отвечает за ввод начальных данных, выбор метода расчёта и вывод результатов расчёта.

– Модуль валидации данных. Анализ введенных данных и отображения сообщений об ошибках исходных данных.

– Вычислительный модуль. Выполняет конвертацию исходных данных, расчёт среднего ресурса, гамма-процентного ресурса, срока службы и гамма-процентного срока службы СФСС.

– Модуль хранения данных. Реализует операции создания проекта, а также его сохранения и загрузки.

– Модуль отчётов. Генерирует отчёт, в соответствие с выполненной оценкой показателей долговечности. Реализует возможность сохранения отчёта в файл, а также его вывод на печать.

Работа выполнена по гранту РФФИ №18-07-00391.

СПИСОК ЛИТЕРАТУРЫ

1. Острейковский, В. А. Операторы энтропии, преобразования и внутреннего времени в теории долговечности сложных систем/ В.А.Острейковский, Е. Н. Шевченко// Фундаментальные и прикладные проблемы науки. Том 1. – Материалы XIV Международного симпозиума. – М. РАН. – 2019. – С. 91-98.
2. Острейковский, В. А. О возможности использования эффекта асимметрии времени в задачах оценки долговечности сложных технических систем / В.А. Острейковский, С.А. Лысенкова // Надежность и качество сложных систем. – 2019. - №1. – С. 21-34.
3. ГОСТ 27.002-2015 Надежность в технике. Термины и определения. М. - Стандартинформ, 2016. 28 с.

УДК 517.98.519.2.629.039

ИСПОЛЬЗОВАНИЕ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ СТАРЕНИЯ КОНСТРУКЦИОННЫХ МАТЕРИАЛОВ ПРИ ОЦЕНКЕ ДОЛГОВЕЧНОСТИ СЛОЖНЫХ КРИТИЧЕСКИ ВАЖНЫХ СИСТЕМ С ДЛИТЕЛЬНЫМИ СРОКАМИ АКТИВНОГО СУЩЕСТВОВАНИЯ

Острейковский Владислав Алексеевич, Сорочкин Андрей Викторович
Сургутский государственный университет
Ленина пр., 1, Сургут, 628412, Россия
e-mails: academicostr@yandex.ru, sorochkin_av@surgu.ru

Аннотация. В статье рассмотрены вопросы использования современных представлений, математические закономерности оценки и анализа количественных показателей долговечности структурно и функционально сложных критически важных систем с учетом асимметрии внутреннего времени и длительностью активного существования критически важных систем.

Ключевые слова: долговечность; ресурс; срок службы или остаточные значения; неустойчивость; необратимые процессы; асимметрия времени.

USAGE OF MATHEMATICAL MODELING OF AGING OF STRUCTURAL MATERIALS IN ASSESSING THE DURABILITY OF COMPLEX CRITICAL SYSTEMS WITH LONG PERIODS OF ACTIVE EXISTENCE

Ostreikovskii Vladislav, Sorochkin Andrei
Surgut State University
1 Lenin Av, Surgut, 628412, Russia
e-mails: academicostr@yandex.ru, sorochkin_av@surgu.ru

Abstract. The article deals with the issues of using modern concepts, mathematical patterns of assessment and analysis of quantitative indicators of the durability of structurally and functionally complex critical systems, taking into account the asymmetry of internal time and the duration of active existence of critical systems.

Keywords: durability; resource; service life or residual values; instability; irreversible processes; asymmetry of time.

Характерными особенностями современных сложных систем (СС), таких как ядерные энергетические установки (ЯЭУ), авиационные и космические комплексы, системы транспортировки нефти и газа и др. являются: 1) высокая конструктивная сложность, 2) длительные сроки активного существования, 3) чрезвычайная критическая важность. Поэтому для указанных комплексов должны быть обоснованы важные показатели

безотказности и долговечности в течение 40-50 и более лет применения по назначению на всех этапах их жизненного цикла.

Известно [1], что основными факторами ухудшения свойств СС являются процессы естественного старения конструктивных материалов элементов оборудования СС под действием внешней среды и длительного времени применения по назначению.

В современной теории надежности закономерности модели старения принято исследовать на 3 уровнях: субмикроскопическом, микроскопическом и макроскопическом. Эти уровни моделирование старения позволили создать математически строгую теорию, получившую название «физики отказов», которая служит основой теории долговечности для уникальных малосерийных СС. На субмикроскопическом уровне объектом исследования являются строения атомов, молекул и кристаллических решеток конструктивных материалов элементов оборудования СС. Это позволяет моделировать дислокации в кристаллах твердых тел и является основой теории прочности материалов. Микроскопический уровень описания позволяет получить закономерности поведения конструкционных материалов на уровне всего объема твердых тел и получения математических моделей, лежащих в основе теории длительной прочности материалов: диффузионные и химические процессы, «адсорбция», распад твердых растворов, изменение механических, электрических и магнитных свойств твердых тел. Макроскопический уровень описания долговечности, используя математические модели микроскопического уровня, дает возможность получить математические модели сложных деградационных процессов. Эти процессы проявляются при эксплуатации оборудования СС таких как коррозия, эрозия, радиационное охрупчивание, износ, тепловое старение, усталость, ползучесть, рост трещин и деформация. Приведенные виды деградационных процессов позволяют получить математические и физико-статистические модели поведения конструкционных материалов элементов оборудования СС с учетом комплекса факторов внешней среды и эксплуатационных факторов при длительных сроках активного существования структурно и функционально критически важных систем [1, с. 24-127].

В XX веке окончательно сформировались важнейшие достижения в исследовании влияния фактора времени на процессы старения оборудования СС. Их можно сформулировать в виде пяти пунктов:

Неустойчивости, флуктуации, бифуркации необратимых и других диссипативных процессов под действием внешней среды являются источником энтропии и в соответствии со вторым началом термодинамики служат источником появления события, названным стрелой времени (асимметрия времени). Этот факт должен обязательно учитываться в задачах теории долговечности СС.

Развитие теоретических основ операторов современного как раздела функционального анализа позволило математически строго доказать возможности нового описания асимметрии времени в модусах «прошлое, настоящее, будущее» и его применение в задачах долговечности СС.

Появление более тонкой классификации СС на внутренне случайные и внутренне необратимые с применением теории цепей Маркова позволило объединить в единое целое в классические динамику и термодинамику. Это оказало большое влияние на завершенность представления об асимметрии времени.

Содержание пунктов 1-3 позволило строго доказать возможность математического описания состояния СС с помощью оператора внутреннего времени и различия во «внутреннем возрасте» элементов и подсистем СС.

В теории операторов доказано, что если известны значения параметров функций распределения состояния элементов и систем СС, то можно объективно получить значения таких показателей долговечности как ресурс, срок службы и их остаточные значения в будущем. Это кардинально меняет наше представление о возможностях объективного знания о показателях долговечности, полученных по известным теориям длительной прочности [2-5].

Работа выполнена по гранту РФФИ №18-07-00391.

СПИСОК ЛИТЕРАТУРЫ

1. Острейковский, В. А. Старение и прогнозирование ресурса оборудования атомных станций / В. А. Острейковский. – Москва : Энергоатомиздат, 1994. – 288 с.
2. Пригожин, И. Р. От существующего к возникающему: время и сложность в физических науках : пер. с англ. / И. Р. Пригожин ; под ред. Ю. Л. Климонтовича. – Изд. 2-е, доп. – Москва : Едиториал УРСС, 2002. – 304 с.
3. Острейковский, В. А. Операторы энтропии, преобразования и внутреннего времени в теории долговечности сложных систем/ В.А.Острейковский, Е. Н. Шевченко// Фундаментальные и прикладные проблемы науки. Том 1. – Материалы XIV Международного симпозиума. – М. РАН, 2019.- С. 91-98.
4. Острейковский, В. А. О возможности использования эффекта асимметрии времени в задачах оценки долговечности сложных технических систем / В.А.Острейковский, С.А.Лысенкова // Надежность и качество сложных систем. 2019. - №1. С. 21-34.
5. Острейковский, В. А. Онтология необратимости и корней времени в задачах долговечности сложных систем / В. А. Острейковский, Е.Н. Шевченко, А.В. Сорочкин. – Региональная информатика (РИ-2020). Информационные технологии в критических инфраструктурах. Санкт-Петербург, 2020. С. 311-312.

УДК 004.056

ОСОБЕННОСТИ ОЦЕНКИ ПОКАЗАТЕЛЕЙ КРИТЕРИЕВ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Сторожик Виктор Сергеевич
Арктический и антарктический научно-исследовательский институт
Беринга, ул., 38, Санкт-Петербург, 199397, Россия
e-mail: vstorozhik@yandex.ru

Аннотация. Рассматриваются особенности оценки показателей критериев значимости объектов критической информационной инфраструктуры.

Ключевые слова: значимый объект; категория значимости; критерий значимости; критическая информационная инфраструктура; показатель; субъект; угроза безопасности информации.

FEATURES OF EVALUATION OF INDICATORS OF CRITERIA OF SIGNIFICANCE OF OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

Storozhik Viktor
Arctic and Antarctic Research Institute
38 Bering St, St. Petersburg, 199397, Russia
e-mail: vstorozhik@yandex.ru

Abstract. The features of evaluating the indicators of the criteria for the significance of critical information infrastructure objects are considered.

Keywords: significant object; category of significance; criterion of significance; critical information infrastructure; indicator; subject; threat to information security.

В Доктрине информационной безопасности Российской Федерации к основным национальным интересам в информационной сфере отнесено обеспечение устойчивого и бесперебойного функционирования критической информационной инфраструктуры (КИИ) в условиях проведения компьютерных атак [1].

В Стратегии национальной безопасности Российской Федерации указано, что использование иностранных информационных технологий и телекоммуникационного оборудования повышает уязвимость российский информационных ресурсов, включая объекты КИИ, к воздействию из-за рубежа, а также поставлена задача развития системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения их источников и оперативной ликвидации последствий реализации таких угроз [2].

В рамках реализации требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [3] Постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 утверждены Правила категорирования объектов критической информационной инфраструктуры Российской Федерации и перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений [4].

Определение категорий значимости объектов КИИ (КЗ) осуществляется на основании показателей критериев значимости объектов КИИ (ПКЗ) и их значений, предусмотренных перечнем ПКЗ объектов КИИ и их значений. Объекту КИИ по результатам категорирования присваивается в соответствии с перечнем ПКЗ категория значимости с наивысшим значением [4].

В процессе категорирования объекта КИИ комиссией по категорированию оцениваются: социальная, политическая, экономическая, экологическая значимость, а также значимость для обеспечения обороны страны, безопасности государства и правопорядка.

Рассматриваются правила категорирования объектов КИИ, перечень ПКЗ объектов КИИ и их значений, а также особенности оценки показателей критериев значимости объектов [4, 5].

Анализируются социальная, политическая, экономическая, экологическая значимость, а также значимость для обеспечения обороны страны, безопасности государства и правопорядка с учетом требований нормативных правовых актов и методических документов, определяющих порядок оценки каждого из ПКЗ объектов КИИ.

Оценка показателей критериев значимости объектов КИИ позволяет постоянно действующей комиссии по категорированию субъекта КИИ принять решение по присвоению каждому из объектов КИИ одной из категорий значимости либо принять решение об отсутствии необходимости присвоения им одной из категорий значимости. В процессе принятия указанных решений комиссия должна учитывать особенности оценки показателей критериев социальной, политической, экономической, экологической значимости, а также значимости для обеспечения обороны страны, безопасности государства и правопорядка объектов критической информационной инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).
2. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 2 июля 2021 г. № 400).
3. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
4. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «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» (в ред. Постановления Правительства РФ от 13.04.2019 г. N 452).
5. Проект методического документа ФСТЭК России «Рекомендации по оценке показателей критериев экономической значимости объектов критической информационной инфраструктуры Российской Федерации» - Режим доступа: https://fstec.ru/tekhnicheskaya-zaschita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/338-proekty/ - Загл. с экрана.

УДК 004.056

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ПО ОЦЕНКЕ ПОКАЗАТЕЛЕЙ КРИТЕРИЕВ ЭКОНОМИЧЕСКОЙ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Щелокова Екатерина Кристиановна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mail: kece7980@gmail.com

Аннотация. Рассматриваются особенности реализации требований нормативных правовых актов и методических документов, определяющих порядок оценки критериев экономической значимости объектов критической информационной инфраструктуры Российской Федерации.

Ключевые слова: безопасность; значимый объект; категория значимости; критерий значимости; критическая информационная инфраструктура; показатель; субъект; угроза безопасности информации.

FEATURES OF THE IMPLEMENTATION OF REQUIREMENTS FOR THE EVALUATION OF INDICATORS CRITERIA OF ECONOMIC SIGNIFICANCE OF OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

Shchelokova Ekaterina
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: kece7980@gmail.com

Abstract. The features of the implementation of the requirements of regulatory legal acts and methodological documents defining the procedure for assessing the criteria of economic significance of objects of critical information infrastructure of the Russian Federation are considered.

Keywords: security; significant object; category of significance; criterion of significance; critical information infrastructure; indicator; subject; threat to information security.

В документах стратегического планирования Российской Федерации [1,2] отмечается стремительный рост целенаправленных атак на критическую информационную инфраструктуру России и указывается, что использование иностранных информационных технологий и телекоммуникационного оборудования повышает уязвимость российский информационных ресурсов, включая объекты критической информационной инфраструктуры, к воздействию из-за рубежа. Актуальной является задача развития системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения их источников и оперативной ликвидации последствий реализации угроз [2].

Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности Российской Федерации» предусматривает обязанность субъектов критической информационной инфраструктуры в соответствии с критериями значимости и показателями их значений, а также порядком осуществления категорирования присвоить одну из категорий значимости принадлежащим им на праве собственности, аренды или ином законном основании объектам критической информационной инфраструктуры. Если объект критической информационной инфраструктуры не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий. Субъект критической информационной инфраструктуры обязан соблюдать установленные нормативными правовыми актами требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, которые зависят от категории значимости соответствующего объекта [3].

Оцениваются социальная, политическая, экономическая, экологическая значимость объекта критической информационной инфраструктуры, а также значимость для обеспечения обороны страны, безопасности государства и правопорядка [3].

Рассматриваются правила категорирования объектов критической информационной инфраструктуры и перечень показателей экономических критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений [3,4].

Анализируются особенности оценки показателей критериев экономической значимости при проведении работ по категорированию объектов критической информационной инфраструктуры [5].

СПИСОК ЛИТЕРАТУРЫ

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646).
2. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 2 июля 2021 г. № 400).
3. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
4. Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 «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» (в ред. Постановления Правительства Российской Федерации от 13.04.2019 г. № 452).
5. Проект методического документа ФСТЭК России «Рекомендации по оценке показателей критериев экономической значимости объектов критической информационной инфраструктуры Российской Федерации» - Режим доступа: https://fstec.ru/tekhnicheskaya-zaschita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/338-proekty/ - Загл. с экрана.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТРАНСПОРТНЫХ СИСТЕМ

УДК 004.738.5

ПРИМЕНЕНИЕ IOT НА ВОДНОМ ТРАНСПОРТЕ

Алексеенков Александр Евгеньевич, Ключникова Дарья Дмитриевна, Ли Изольда Валерьевна
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: kseenkovale@gmail.com, lik0011sofia@mail.ru, liiv@gumrf.ru

Аннотация. В статье рассмотрены основные области применения IoT на водном транспорте в настоящее время. Интернет вещей захватывая все больше аспектов нашей жизни дает серьезные предпосылки к применению средств контроля и мониторинга. Системы IoT позволяют гибко и эффективно решать подобные задачи. Это могут быть порты, суда, навигационное оборудование и многие другие сферы. В настоящее время Интернет вещей активно вводится в использование, являясь важной частью работы отрасли водного транспорта.

Ключевые слова: IoT; интернет вещей; водный транспорт; навигация; умный порт; автономное судно.

APPLICATION OF IOT IN WATER TRANSPORT

Alekseenkov Aleksander, Klyuchnikova Daria, Li Izolda
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: kseenkovale@gmail.com, lik0011sofia@mail.ru, liiv@gumrf.ru

Abstract. The article discusses the current uses of IoT at sea. The Internet of Things taking over our lives increasingly provides serious prerequisites for application of controls and monitoring. Today IoT systems allow to solve such tasks flexibly and efficiently. These can be ports, ships, navigational equipment and many other spheres. At present the Internet of things is being actively introduced into use, being an important part of the work of the waterway transport industry.

Keywords: IoT; internet of things; water transport; navigation; smart port; autonomous ship.

Введение. Человечество создает все больше устройств и технологий для более комфортного управления и взаимодействия. Особое внимание уделено автоматизации процессов. Одним из способов автоматизации стал Интернет вещей (Internet of Things). По своей сути Интернетом вещей являются физические объекты, подключенные к сети и обменивающиеся данными.

IoT применяется в самых различных областях: торговля, производство, перевозки, здравоохранение, энергетика и многое другое. Отрасль водного транспорта не исключение. Область применения IoT здесь очень обширна: от различных систем наблюдения до устройств для сохранения экологии.

Машинная связь (MTC - Machine type communications - это форма передачи данных, включающая одну или несколько сущностей, которые не управляются людьми напрямую) является ключом к морскому интернету вещей из-за необходимости установления между судами и берегом, а также между судами для поддержки выполнения различных видов морских услуг. Интернет вещей также может быть полезен при поисково-спасательных операциях, в навигационных устройствах и в устройствах, отслеживающих перевозки. Рассмотрим подробнее области его применения на водном транспорте.

Навигация

Навигация в данный момент не может обойтись без IoT. Одним из важнейших аспектов навигации является мониторинг буев и маяков [1]. Система контроля на основе Интернета вещей позволяет быстро и эффективно реагировать в случае возникновения проблем, что обеспечивает как безопасность навигации, так и целостность сигналов.

Буи и их световые сигналы необходимы для безопасного прохождения маршрута водным транспортом. Так наблюдательные устройства, развернутые в настоящее время на береговых линиях Ирландии, включают буи, передающие данные о погоде и волнении, приливах и отливах. Однако, из-за плохой погоды швартовочный трос может оборваться. Не исключается дрейф буя по течению, если оно достаточно сильное. В подобных случаях, дрейфующий буй представляет серьезную опасность, поскольку может произойти столкновение с судном.

Устройство IoT, мониторящее буй, в определенный промежуток времени активируется и выполняет необходимые измерения, после чего отправляет все собранные данные на сервер (если буй плывет по течению, время интервала уменьшается, чтобы отслеживать скорость, курс и позицию с большей частотой).

Устройство IoT может отправить сигнал о падении напряжения аккумулятора, увеличении смещения координат, сигнал об открытом кожухе лампы, а также отсутствии сигнала от буя более четырех часов.

В навигации отдельно стоит отметить системы морской картографии [2]. Данные системы разработаны для обеспечения бесперебойной, согласованной и стандартизированной базы данных включающей: морской климат, данные о навигации с использованием фотограмметрии, подходы, основанные на зондировании или лазерном сканировании и т.д.

Тем не менее современные методы основаны либо на удаленном мониторинге с применением спутников, не имеющих требуемой точности из-за загрязнений в атмосфере, либо на методах, основанных на разведке. К таким методам относят поисковые суда, включая гидрографические и океанографические суда, которые не могут покрыть обширные пространства океанов и морей из-за физических ограничений и ограниченного количества проведенных исследований.

Умные порты

В основе модели умного порта лежит технология Интернета вещей [3]. Применение данной технологии в процессе создания логистической платформы позволяет уменьшить затраты на логистику. А внедрение Интернета вещей на уровне функционального планирования и при строительстве порта позволяет повысить эффективность каждого реализуемого в порту процесса.

При прохождении сегментов порта судам часто приходится выстраиваться в линию, соблюдая правила навигации. Это не только увеличивает время прохождения маршрута, но также вызывает частые морские дорожно-транспортные происшествия и приводит к гибели людей и порчи имущества, а также к загрязнению окружающей среды. Моделирование транспортных потоков в портах имеет большое значение для проектирования и преобразования порта. Смоделированное поведение судна можно реализовать не только в разработке, но и на практике.

В системе портов каналы являются важной частью обеспечения навигации. Для упрощения анализа отрезок маршрута разделяют на несколько сегментов. Каждый сегмент маршрута в канале заполнен ячейками одинакового размера. Для изменения скорости судна в зависимости от его положения, различают разные участки маршрута, где устанавливаются определенные модели ячеек. Элементарная ячейка канала постепенно становится больше в направлении от причала, так как скорость корабля уменьшается по мере того, как уменьшается расстояние до причала и увеличивается по мере удаления от него.

При строительстве интеллектуального порта можно реализовать интеллектуальное управление производственными операциями порта, управление складом и логистикой.

IoT используется в интермодальных перевозках: система, основывается на постоянной двунаправленной связи с контейнерами, движущимися внутри транспортной цепочки [4]. Модуль, включенный в систему, обеспечивает открытую среду с расширенными возможностями для контроля расположения и состояния каждого контейнера. Это решение позволяет реализовать множество различных способов управления глобальной цепочкой поставок во время транспортировки.

Другие системные модули используют данные отслеживания. Один из которых используется для оптимизации движения внутри морского терминала, а другие регулируют график движения судов. Использование этих модулей с данными отслеживания, должно привести к уменьшению времени пребывания на терминале и времени обработки контейнеров, а также сокращению затрат и времени простоя при транспортировке.

Умные суда

Владельцы автономных судов стремятся оцифровать и зафиксировать большинство жизненно важных параметров [5]. Информация, которую важно знать: текущее положение и статус самых важных датчиков, таких как состояние дверного люка, состояние батареи, температуры, давления и т.д. Ключевыми задачами системы являются: сбор данных от датчиков и управление ими, связь в морской среде. Службы обеспечивают такие функции, как уведомления при достижении критических уровней, после чего пользователь может выполнить вмешательство на основании состояния судна.

Интернет вещей также позволяет реализовать систему швартовки с автоматическим размещением у причала в порту [6]. При получении запроса от судна, прибывающего в порт, система автоматически отправляет данные о месте, где он может пришвартоваться, прежде чем достигнет швартовой пристани.

Каждое место стоянки в порту может содержать автоматически управляемые устройства и датчики. Помимо этого, есть умные порты с различными коммуникационными технологиями для обмена данными с другими портами, умными судами и умными городами. Сервисы, созданные в интеллектуальных портах, состоят из автоматического мониторинга и контроля местоположения судов в порту, графика движения судов, грузов, проезда пассажиров и т.д.

Некоторые из крупных портов по всему миру уже предоставляют интерактивные услуги своим клиентам используя новейшие технологии. Примером может служить порт Гамбург в Германии. Одной из интерактивных услуг для клиентов является возможность найти суда и места их расположения, проверить их состояние в режиме реального времени на сайте порта.

Порт Амстердам запустил несколько приложений. Приложение «I am Port» предлагает информацию о местонахождении судов и маршрутах движения в порту в режиме реального времени. Кроме того, мы можем

найти информацию о прибытии и отправлении, размере, осадке и причаливании каждого судна в порту. Они также маркируют суда разными цветами, но цвет означает не тип судна, а скорее его статус.

Стартап We4Sea (https://www.we4sea.com/) разрабатывает приложение для судов, что позволяет сократить расходы на топливо до 20 процентов. Система We4Sea собирает некоторые оперативные данные по судну, как его местоположение, скорость, курс и данные двигателя, и отправляет их на берег для объединения с другими данными, такими как погода, высоты волн, сила ветра. После объединения этих данных, системные алгоритмы и энергетические модели преобразуют их в полезную информацию для оптимизации эксплуатации и комплектации.

Системы мониторинга физического и психоэмоционального состояния экипажа могли бы быть внедрены с применением технологии IoT.

Заключение. Гибкость и модульность вместе с низкими затратами являются основными сильными сторонами Интернета вещей.

Основная цель IoT - повысить комфорт и производительность в области применения. Интернет вещей может способствовать существенному повышению эффективности и качества услуг, безопасности эксплуатации оборудования и безопасности портов за счет повышения доступности и точности соответствующей информации. Морской IoT должен иметь адаптивную структуру, гибкость для внедрения новых приложений, обеспечивать безопасное подключение к существующим информационным системам и обрабатывать огромное количество данных. Стоит отметить, что количество областей применения IoT только увеличивается. Интернет вещей находит применение не только в порту, но и на судах, в навигационном оборудовании и многих других сферах.

IoT эффективен в сборе данных о погодных условиях, состоянии оборудования, местонахождении и т.д. Использование полученной информации помогает в принятии решений, позволяя оценить ситуацию в более полном объеме, а также сводить к минимуму чрезвычайные и травмоопасные ситуации, что особенно актуально в системах, применяемых в промышленных и коммерческих задачах.

Можно предвидеть, что системы морского IoT станет незаменимым помощником в области водного транспорта.

СПИСОК ЛИТЕРАТУРЫ

1. S. D. Pizzo, A. De Martino, G. De Viti, R. L. Testa and G. De Angelis, "IoT for Buoy Monitoring System," 2018 IEEE International Workshop on Metrology for the Sea; Learning to Measure Sea Health Parameters (MetroSea), 2018, pp. 232-236, doi: 10.1109/MetroSea.2018.8657828.
2. M. Al-Khalidi, R. Al-Zaidi, J. Woods, M. Reed and E. Pereira, "Securing Marine Data Networks in an IoT Environment," 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud), 2019, pp. 125-132, doi: 10.1109/FiCloud.2019.00025.
3. L. Jiang, G. Huang, C. Huang and W. Wang, "Data Mining and Optimization of a Port Vessel Behavior Behavioral Model Under the Internet of Things," in IEEE Access, vol. 7, pp. 139970-139983, 2019, doi: 10.1109/ACCESS.2019.2943654.
4. Jesús Muñuzuri, Luis Onieva, Pablo Cortés, José Guadix, “Using IoT data and applications to improve port-based intermodal supply chains” School of Engineering, University of Seville, CM Descubrimientos, s/n, 41092 Seville, Spain Available online 23 January 2019.
5. M. Cankar and S. Stanovnik, "Maritime IoT Solutions in Fog and Cloud," 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), 2018, pp. 284-289, doi: 10.1109/UCC-Companion.2018.00069.
6. Kamolov, A.; Park, S. An IoT-Based Ship Berthing Method Using a Set of Ultrasonic Sensors. Sensors 2019, 19, 5181. https://doi.org/10.3390/s19235181

УДК 651.011.56

ПРЕВЕНТИВНОЕ УПРАВЛЕНИЕ ПРОИЗВОДСТВОМ ПО ДЕЛАМ ОБ АДМИНИСТРАТИВНЫХ ПРАВОНАРУШЕНИЯХ НА ТРАНСПОРТЕ ПРИ КОНФЛИКТЕ СТОРОН

Бурлов Вячеслав Георгиевич, Миронов Алексей Юрьевич, Миронова Анна Юрьевна
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: burlovvg@mail.ru, wakepolarbear@gmail.com, milpandaaaa@gmail.com

Аннотация. С целью обеспечения информационной безопасности в части достоверности и полноты производства по делам об административных правонарушениях на транспорте рассмотрен синтез облика превентивного управления им в условиях противодействия участников. Административную практику в разумный срок предложено гарантировать за счет системы управления в составе целевой подсистемы с контрольно-надзорным механизмом, защитной подсистемы на базе геоинформатики и обеспечивающей подсистемы на основе геолокации. Каждую из подсистем управления целесообразно моделировать непрерывной цепью Маркова, конкретизированной уравнениями Колмогорова-Чепмена.

Ключевые слова: административное производство на транспорте; синтез превентивного управления; конфликт сторон; непрерывная сеть Маркова; уравнения Колмогорова-Чепмена.

PREVENTIVE MANAGEMENT OF PRODUCTION ON AFFAIRS ABOUT ADMINISTRATIVE OFFENSES ON TRANSPORT WHEN PARTIES CONFLICT

Burlov Vyacheslav, Mironov Aleksey, Mironova Anna
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: burlovvg@mail.ru, wakepolarbear@gmail.com, milpandaaaa@gmail.com

Abstract. In order to ensure information security in terms of the reliability and completeness of production on affairs about administrative offenses on transport, the synthesis of the appearance of its preventive management in conditions of opposition from participants is considered. It is proposed to guarantee administrative practice within a reasonable time by means of a management system as part of a target subsystem with a control and supervisory mechanism, a protective subsystem based on geoinformatics and a providing subsystem based on geolocation. It is expedient to model each of the management subsystems with a continuous Markov chain, concretized by the Kolmogorov-Chapman equations.

Keywords: administrative production on transport; synthesis of preventive management; conflict of parties; continuous Markov chain; Kolmogorov-Chapman equations.

Введение. Хроническое несоблюдение правил эксплуатации транспортных средств, пожары, умышленное или случайное повреждение опасных грузов и магистральных трубопроводов, ненадлежащее строительство и использование транспортной инфраструктуры, техногенные и экологические катастрофы порождаются нарушениями разумного срока. административного производства на транспорте [1]. Преодоление разрушения целостности в виде неполноты и недостоверности административной практики особенно актуально в отношении административных правонарушений, по которым признаки и следы укрыты особенностями местности. а правонарушители противодействуют субъектам административной юрисдикции [2].

В ходе моделирования административной практики следует учитывать, что в административном производстве принимают участие две стороны административно-процессуального правоотношения: субъект административной юрисдикции и противодействующие участники производства, объединенные умышленно или по неосторожности единым стремлением доведения до цели правонарушения. В общем случае, их взаимодействие рассматривается в виде конфликта с несовпадающими интересами.

Адекватность комплекса мероприятий субъекта административной юрисдикции по обеспечению информационной безопасности производства основана на осознании и познании окружающей обстановки и противодействия участников. Принятие управленческих решений для поддержания разумности срока функций административного процесса требует моделировать применение управления производством на протяжении всего жизненного цикла дел об административных правонарушениях. Успешность технологии познания и управления определяется адекватностью моделирования. Мерой адекватности математической модели выступает полнота учета ею закономерностей обеспечения разумного срока на базе закона сохранения целостности производства по делам об административных правонарушениях [3].

Формализация закона сохранения целостности, путем аккумулирования потенциальной эффективности системы управления по требуемым пространственно-временным состояниям в районе сосредоточения ее основных усилий, сформировала инструмент разрешения конфликта.

Цель, вытекающая из интересов, достигается за счет разработки, развертывания и применения системы управления (поддержки). Показатель эффективности ее функционирования является мерой соответствия целевого предназначения. Методология задает множества требуемых пространственно-временных состояний системы управления (поддержки) и определяет их свойства.

Для реализации базовых функций каждая сторона конфликта создает в рамках системы управления (поддержки) соответствующие подсистемы: целевую, защитную, обеспечивающую [4]. Целевая подсистема предназначена для решения целевых задач на множестве пространственно-временных состояний: у субъекта административной юрисдикции – стадий административной практики, у противодействующих участников производства – этапов совершения административного правонарушения. На стороне субъекта административной юрисдикции она образует стержень административного производства с собственным контрольно-надзорным механизмом и управляется в разумный срок за счет дополнения защитной и обеспечивающей подсистемами.

Параллельно собственному целевому процессу защитная подсистема стороны стремиться препятствовать целевой деятельности противника: субъект административной юрисдикции – превентивно выявить и доказать признаки события и состава латентных правонарушений, противодействующие участники производства – затянуть и сорвать разумный срок процессуальных процедур целевого вида административного производства. Защитная функция превалирует в активности стороны конфликта на стадиях возбуждения и расследования дел об административных правонарушениях. При рассмотрении дел и исполнении наказаний защитный эффект постепенно подавляется противником.

Разнонаправленность целевой и защитной функций каждого противника указывает на диалектическое противоречие реализующих подсистем. Для гармоничного их сосуществования и подавления эффекта противодействия естественно предположить у стороны наличие обеспечивающей подсистемы, снимающей противоречие: для субъекта административной юрисдикции – геолокацией участников производства гарантирующей их присутствие в административном процессе, для противодействующих участников производства – активно скрывающей и уничтожающей следы административного правонарушения и его последствий. Угнетая защитную деятельность противника в отношении собственного целевого процесса, обеспечивающая функция стороны конфликта усиливается от расследования дел к стадиям их рассмотрения и исполнения наказаний [5].

При решении комплексной задачи синтеза модели и порядка функционирования системы синтез облика и способов превентивного управления административным производством проходит следующие шаги:

– исследование потенциально требуемых пространственно-временных состояний целевой, защитной и обеспечивающей подсистем на основе оценивания обстановки и организационно-технических возможностей, достигнутых ресурсами сторон;

– формирование потенциала поля эффективности целевой, защитной и обеспечивающей подсистем на основе оценивания обстановки и организационно-технических возможностей, достигнутых сторонами из обеспеченности ресурсами;

– обоснование видов, способов и форм действий, разработка базовых элементов замысла операции, решения на ее проведение в рамках концепции единства системы, цементируемой обеспеченностью ресурсами;

– создание модели оценивания эффективности системы управления, обобщающей целевую, защитную и обеспечивающую реакции;

– разработка предложений по структурному и функциональному наполнению целевой, защитной и обеспечивающей подсистем, исходя из обеспечения устойчивости системы управления в удовлетворении целевого предназначения.

Таким образом, трехфункциональный облик системы превентивного управления в конфликтном противодействии участников административного производства порождает ее целевую, защитную и обеспечивающую реакции, которые моделируются непрерывными цепями Маркова в уравнениях Колмогорова-Чепмена и обобщаются в оценку системного критерия эффективности [6, 7].

Заключение. В обстановке конфликтной активности противодействующих участников производства по делам об административных правонарушениях на транспорте, административная практика в разумный срок субъекта административной юрисдикции гарантированно управляется путем ее сопровождения целевой подсистемой с контрольно-надзорным механизмом, защитной подсистемой на базе геоинформатики и обеспечивающей подсистемой на основе геолокации. В текущей обстановке, характеризуемой интенсивностями Целевого процесса и Появления Проблем, при нормативно установленных уровнях максимально допустимой частоты срыва Целевого процесса и минимально достаточной эффективности, критерий эффективности целевой, защитной или обеспечивающей подсистемы управления позволяет контролировать достаточность и оптимизировать интенсивности Информационно-аналитической работы и Управленческого решения путем рационализации структуры и продолжительностей переходов по их событиям с учетом срывов, мотивированных дефицитом ресурсов.

СПИСОК ЛИТЕРАТУРЫ

1. Дерюга А.Н., Мотрович И.Д. Причины латентности административных правонарушений // Административное право и процесс. – 2013. – №7. – С. 57-62.
2. Миронов А.Ю. Миронова А.Ю., Сипович Д.Е. Информационная безопасность выявления и доказывания административных правонарушений с применением геоинформационной системы // Региональная информатика и информационная безопасность: Сборник трудов: Выпуск 7. – СПб.: СПОИСУ, 2019. – С.402-407.
3. Жуков А.О., Бурлов В.Г., Пестун У.А. К вопросу стратегического планирования развития наукоемких предприятий // Стратегическое планирование и развитие предприятий: материалы XVIII Всероссийского симпозиума. – М.: ЦЭМИ РАН, 2017. – С. 935-939.
4. Матвеев А.В., Иванов М.В., Шевченко А.Б. Аналитическая модель системы управления пожарной безопасностью АЭС // Научно-технические ведомости СПбГПУ: информатика, телекоммуникации, управление. – 2010. – № 6. – С.91-95.
5. Миронов, А.Ю. Превентивное управление административным производством в условиях конфликта сторон // Неделя науки ИСИ: сборник материалов Всероссийской конференции, 26–30.04.2021: В 3 ч. – Ч. 3. – СПб.: ПОЛИТЕХ-ПРЕСС, 2021. – С. 234-237.
6. Лепешкин О.М., Лепешкин М.О., Бурлов В.Г. Синтез процесса управления техническими системами на основе теории радикалов // Нейрокомпьютеры и их применение: XIV Всероссийская научная конференция: тезисы докладов. – М.: МГППУ, 2016. – С. 18-В.
7. Бурлов В.Г., Попов Н.Н., Гарсия Эскалона Х.А. Управление процессом применения космической геоинформационной системы в интересах обеспечения экологической безопасности региона // Ученые записки Российского государственного гидрометеорологического университета. – СПб.: РГГМУ, 2018. – № 50. – С. 118-129.

УДК 004.056.53

ПОСТРОЕНИЕ ЭФФЕКТИВНОЙ ПОДСИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТРАНСПОРТНЫХ СИСТЕМАХ

Голоскоков Константин Петрович, Коротков Виталий Валерьевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: goloskokovkp@gumrf.ru, korotkovvv@gumrf.ru

Аннотация. Рассматриваются основные принципы построения эффективных сбалансированных транспортных информационных систем за счет создания подсистемы информационной безопасности.

Ключевые слова: информационная безопасность; транспортная система; инструментальная среда; технические и программные средства.

BUILDING AN EFFECTIVE INFORMATION SECURITY SUBSYSTEM IN TRANSPORT SYSTEMS

Goloskokov Konstantin, Korotkov Vitaly
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: goloskokovkp@gumrf.ru, korotkovvv@gumrf.ru

Abstract. The basic principles of building effective balanced transport information systems by creating an information security subsystem are considered.

Keywords: information security; transport system; tool environment; technical and software tools.

Введение. Построение эффективной, сбалансированной, экономически оправданной транспортной информационной системы напрямую связано с правильно построенной подсистемой информационной безопасности [1-3].

При этом необходимо решить следующие задачи:

1. произвести качественную оценку текущего уровня безопасности, задать допустимые уровни рисков, разработать план обеспечения требуемого уровня;

2. обосновать требуемые финансовые вложения в создание информационной безопасности на основе технологии анализа рисков;

3. выявить и ликвидировать уязвимые для атак позиции;

4. определить функциональные отношения и зоны ответственности взаимодействия подразделения и служб по обеспечению информационной безопасности;

5. создать необходимый пакет организационно-распорядительной документации;

6. спланировать создание и внедрить;

7. обеспечить поддержку информационной безопасности в условиях развития организации (бизнеса), регулярными доработками и развитием комплекса защиты.

Для решения поставленных задач необходимо провести:

1. аудит – оценку и переоценку уровня текущего состояния информационной безопасности на соответствие современным нормам;

2. анализ информационных рисков;

3. выработку рекомендаций по обеспечению информационной безопасности предприятия;

4. разработку концепции, политики и плана защиты, проектирование информационной безопасности;

5. экспертизу информационной безопасности на предмет соответствия заданному уровню безопасности и выработанным рекомендациям;

6. разработку пакета организационно-распорядительной документации;

7. внедрение, обслуживание, развитие и интегрированные решения по управлению информационной безопасности.

К средствам, обеспечивающим решение поставленных задач на современном уровне, следует отнести следующие подсистемы, приведённые ниже.

1. Средства анализа защищенности (сканеры безопасности). Существует острая необходимость в средствах анализа защищенности для своевременного обнаружения уязвимостей и принятия мер по их ликвидации.

Сложившаяся ситуация в сфере информационной безопасности предполагает обязательное использование средств анализа защищенности в компаниях, имеющих выход в сети связи общего пользования, осуществляющих обработку персональных данных, а также в иных случаях (соответствие стандартам PCI DSS, ISO 17799, СТО БР ИББС).

Для транспортного бизнеса через сети связи общего пользования осуществляется реализация взаимодействия с клиентской сетью, с контрагентами и контролирующими государственными структурами (налоговая инспекция, пенсионный фонд и др.) [4-6].

При аудите безопасности, аттестации используются сетевые сканеры уязвимостей, позволяющие проводить инвентаризацию сети и идентификацию уязвимостей. На рынке сканеров представлен широкий спектр устройств. Это и условно бесплатные устройства с открытым кодом до специализированных комплексов аудитора информационной безопасности. Сетевые сканеры служат для анализа защищенности сети путем сканирования и зондирования сетевых ресурсов и выявления их уязвимостей [7-9].

Применение сканеров позволяет решить следующие задачи:

- инвентаризация ресурсов, включающих устройства сети, ОС, службы и ПО;
- идентификация и анализ уязвимостей;
- патчинг (автоматизированная отдельно поставляемая программа необходимая для устранения проблем в ПО или изменения его функционала) новых уязвимостей до выхода официальных исправлений от производителя;
- формирование отчетов, в том числе с описанием проблем и вариантами устранения.

При проведении обследования защищенности ресурсов могут быть использованы различные инструменты выявления проблем безопасности. Большую часть их, как правило, составляют различные сетевые сканеры.

С каждым годом растет количество нового вирусного ПО, увеличивается процент вероятности заражения вредоносным кодом. Факт заражения может произойти на конечных рабочих станциях пользователей, серверах, шлюзах или мобильных устройствах, в том числе использующихся удаленно.

Заключение. Исходя из этого, необходимо осуществлять комплексную защиту всех точек возможного проникновения вредоносного кода в корпоративную сеть.

Данный тип защиты подразумевает применение систем антивирусной защиты, обеспечивающих безопасность всех без исключения устройств внутри и за пределами сети компании

Необходимо использовать единый центр управления всеми узлами системы антивирусной защиты для удобства администрирования и наглядности процессов, происходящих в области вирусной активности.

Сложившаяся ситуация в сфере информационной безопасности предполагает обязательное использование систем антивирусной защиты (соответствие стандартам PCI DSS, ISO 17799, СТО БР ИББС, выполнение требований по защите персональных данных).

Применение систем антивирусной защиты позволяет решить следующие задачи:

– блокирование проникновения вирусов на информационную систему при использовании на них инфицированных файлов с переносимых устройств памяти;

– предотвращение заражения вирусами с помощью ПО из Интернета;

– предотвращение проникновения вирусов при подключении к информационным системам удаленных или мобильных пользователей;

– предупреждение заражения вирусами с удаленного сервера, обменивающегося данными с корпоративными серверами файл - приложений и БД;

– блокирование распространения почтовых и Интернет-«червей»;

– предупреждение с помощью эвристической защиты заражения новыми и ранее неизвестными угрозами;

– управление доступом к конкретным процессам, файлам и папкам со стороны пользователей и приложений;

– контроль подключения и использования периферийных устройств;

– восстановление работы приложений после вирусных эпидемий и предотвращение вирусных эпидемий.

СПИСОК ЛИТЕРАТУРЫ

1. Голоскоков К.П. Прогнозирование и оценка технического состояния сложных систем// Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. 2008. № 1 (53). С. 164-
2. Малюк В.И., Голоскоков К.П. Методика оценки рационального распределения ограниченных инвестиций в развитие производственной системы региона// Вестник ИНЖЭКОНа. Серия: Экономика. 2009. № 1 (28). С. 51-60
3. Власов М.П., Голоскоков К.П., Панова Е.Н.Оценка экономической эффективности нововведений// Экономическое возрождение России. 2011. № 4 (30). С. 25-38.).
4. Брусакова И.А., Власов М.П., Голоскоков К.П. Информационные технологии в научных исследованиях высшей школы// Санкт-Петербург, 2012. 146с.
5. Голоскоков К.П. Автоматизированная система испытаний в структуре системы управления качеством// Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2008. № 6 (69). С. 116-120.
6. Голоскоков К.П. Технология испытаний и прогнозирования технического состояния электронных средств судовых систем управления//диссертация на соискание ученой степени доктора технических наук / Санкт-Петербургский государственный университет водных коммуникаций. Санкт-Петербург, 2009
7. Голоскоков К.П., Нестеренко Н.К., Чиркова М.Ю. Повышение эффективности деятельности производственного предприятия//Аудит и финансовый анализ. 2014. № 1. С. 331-335.
8. Брусакова И.А., Голоскоков К.П. Математическая модель функциональной надежности автоматизированных систем управления//Вестник ИНЖЭКОНа. Серия: Технические науки. 2010. № 8. С. 48-51.
9. Голоскоков К.П., Железняк М.В. Прогнозирование с применением теории распознавания образов// Вестник ИНЖЭКОНа. Серия: Технические науки. 2011. № 8. С. 114-118.

УДК 004

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ ПО ЦИФРОВИЗАЦИИ МУЗЕЙНОГО КОМПЛЕКСА С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ IBEACON

Ильина Анастасия Андреевна, Шипунов Илья Сергеевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: nastya185342@yandex.ru, mr-shis@yandex.ru

Аннотация. В статье описывается технология iBeacon и разработка мобильного приложения для цифровизации музейного комплекса с использованием технологии iBeacon. Описывается алгоритм работы приложения.

Ключевые слова: iBeacon; Bluetooth-маячок; swift; ios; мобильная разработка; core location.

DEVELOPMENT OF A MOBILE APPLICATION FOR DIGITALIZATION OF THE MUSEUM COMPLEX USING IBEACON TECHNOLOGY

Anastasia Ilina, Shipunov Ilya
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: nastya185342@yandex.ru, mr-shis@yandex.ru

Abstract. The article describes the iBeacon technology and the development of a mobile application for the digitalization of the museum complex using the iBeacon technology. The algorithm of the application is described.

Keywords: iBeacon; Bluetooth beacon; swift; ios; mobile development; core location.

Введение. В последние годы интерес к использованию Bluetooth-маячков возрос. Они используются повсеместно, начиная от навигации внутри какого-либо помещения или музейного комплекса, заканчивая функцией уведомления об акциях в магазинах, когда человек проходит мимо него.

В 2013 году компания Apple представила технологию iBeacon, предназначенную для передачи Bluetooth-сигнала на устройства, находящиеся в радиусе действия Bluetooth-маячков. Суть работы системы состоит в установке миниатюрных маяков, которые связываются со смартфонами пользователей посредством стандарта Bluetooth Low Energy – технологии беспроводной связи, обеспечивающей смартфонам низкое энергопотребление. В сравнении с Wi-Fi, смартфоны при работе с iBeacon-маяками потребляют примерно в 30 раз меньше энергии. Когда человек оказывается вблизи iBeacon-маяка, тот приводит в действие мобильное приложение на его смартфоне, которое в свою очередь начинает выполнять заранее подготовленный алгоритм работы: например, присылает пользователю какое-то уведомление.

Целью работы является обзор разработки мобильного приложения для цифровизации музейного комплекса с использованием технологии iBeacon.

При разработке приложения использовался язык программирования Swift и фреймворк CoreLocation, частью которого является iBeacon – протокол-подмножество Bluetooth Low Energy, который позволяет узнать следующую информацию:

UUID, который является уникальным идентификатором группы маячков;

Major, который определяет некоторую подсеть маячков;

Minor, который определяет конкретный маячок в группе;

RSSI (Received Signal Strength Indicator) – индикатор мощности принятого сигнала, после чего сопоставляет его с уровнем сигнала в 1 метре от передатчика.

Силу сигнала от маячка. Стандарт iBeacon создавался не с целью определения точного расстояния

от смартфона до маячка и оперирует лишь зонами: непосредственная близость (очень близко к маячку), близко (расстояние 1-3 метра до маячка), далеко (зона, где сигнал слишком колеблется и точнее определить расстояние нельзя) и неизвестно [1].

Был создана структура данных Beacon, которая содержит параметры, по которым ее можно идентифицировать. Далее был создан массив Bluetooth-маячков типа Beacon.

Для определения области поиска маячков существует объект region. Мониторинг региона Bluetooth-маячков осуществляется при помощи различных делегатов, которые сообщают об их состоянии даже если приложение находится в фоновом режиме или мобильное устройства заблокировано. Например, мы можем узнать о входе/выходе из региона Bluetooth-маячка при помощи метода startMonitoringForRegion. Когда пользователь заходит в зону действия маячка или покидает ее, возникают события didEnterRegion/didExitRegion.

Для поиска маячков и отслеживания событий их обнаружения существует объект locationManager.

В отличие от мониторинга регионов, который позволяет пользователям обнаруживать вход/выход устройств из диапазона iBeacon, ранжирование предоставляет список iBeacon-маячков, обнаруженных в данном регионе, вместе с предполагаемым расстоянием от устройства пользователя до каждого iBeacon. Фиксируются три зоны позиционирования:

Immediate – менее метра;

Near – в пределах 1-10 метров;

Far – более 10 метров.

Алгоритм работы приложения для цифровизации музейного комплекса следующий:

Проверяем, включен ли Bluetooth. Если включен – идём дальше, иначе предлагаем пользователю его включить. Пока Bluetooth выключен, на отображается экран с предложением включить его.

Начало мониторинга регионов.

Нахождение ближайшего маяка. В связи с тем, что объекты в музее могут располагаться достаточно близко друг к другу, необходимо использовать несколько проверок:

Проверка на близость к Bluetooth-маячку. Значение distance должно быть равно immediate. Т.к. на данном этапе несколько маячков могут располагаться рядом с мобильным устройством, необходимо определить, какой из них находится ближе всего.

Нахождение ближайшего Bluetooth-маячка из доступных в регионе. Для этого используется значение accuracy типа Double. Если обе проверки пройдены, предлагается посмотреть информацию об экспонате и прослушать аудио-экскурсию.

Проверка на выход из региона и приближение к другому маячку.

Заключение. iBeacon предоставляет отличные возможности для цифровизации музейного комплекса: мы можем отслеживать приближение посетителя к конкретному экспонату и выдавать информацию о нем. А если приложение находится в фоновом режиме или мобильное устройство выключено, то придет уведомление на телефон с предложением прослушать аудио-экскурсию или же ознакомиться с информацией об экспонате.

СПИСОК ЛИТЕРАТУРЫ

1. Алексей Панов. Как работают маяки: Физика технологии iBeacon. [Электронный ресурс]. URL: https://habr.com/ru/company/navigine/blog/269735/ (дата обращения: 18.06.2020).
2. Sokolov S. Countering Cyberattacks During Information Operations / S. Sokolov, A. Nyrkov, T. Knysh, A. Shvets // In: Mottaeva A. (eds) Proceedings of the XIII International Scientific Conference on Architecture and Construction 2020. Lecture Notes in Civil Engineering, vol 130. Springer, Singapore. – 2021. – Pp. 84 - 100. https://doi.org/10.1007/978-981-33-6208-6_8

УДК 004.056

СИСТЕМЫ ОЦЕНКИ И ПРОГНОЗИРОВАНИЯ КИБЕРУГРОЗ НА МОРСКИХ СУДАХ ПОД ФЛАГОМ РФ С ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Когтев Алексей Валерьевич
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mail: xx.ww.zz@ya.ru

Аннотация. В статье рассмотрены возможные взаимодействия автоматизированной информационной системы оценки и прогнозирования киберугроз на морских судах под флагом РФ с внешними информационными системами.

Ключевые слова: автоматизированная информационная система; киберугрозы; киберинциденты; морские суда.

INTERACTION AND INTEGRATION OF THE AUTOMATED INFORMATION SYSTEM FOR ASSESSING AND PREDICTING CYBER THREATS ON SEA VESSELS UNDER THE FLAG OF THE RUSSIAN FEDERATION WITH EXTERNAL INFORMATION SYSTEMS

Kogtev Alexey
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mail: xx.ww.zz@ya.ru

Abstract. The article discusses possible interactions of an automated information system for assessing and predicting cyber threats on sea vessels under the flag of the Russian Federation with external information systems.

Keywords: automated information system; cyber threat; cyber incidents; sea vessels.

Современный уровень развития информационных технологий и автоматизации судовых процессов обуславливает активный рост объёмов загрузки данных морскими судами [1]. Например, с января 2020 г. по март 2021 г. среднесуточный объём загрузки данных на одно судно вырос в 3 раза и составил 9,8 Гб в сутки [2]. Вследствие этого, очевиден рост количества киберинцидентов на морских судах и повышение уровня реализации киберугроз в отношении судов, что делает морскую кибербезопасность актуальным вопросом для судоходной отрасли [3].

Возможной мерой, направленной на обеспечение морской кибербезопасности, может стать создание автоматизированной информационной системы оценки и прогнозирования киберугроз на морских судах под флагом РФ (автоматизированная ИС ОиПК).

Одна из основных задач автоматизированной ИС ОиПК, реализация которой необходима для достижения поставленных перед ней целей, заключается во взаимодействии и интеграции с внешними ИС.

Основными системами, взаимодействие с которыми необходимо для выполнения возложенных на автоматизированную ИС ОиПК функций и задач, могут являться Система управления движением судов (СУДС) и Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

Взаимодействие и интегрирование с СУДС необходимо для реализации ряда важных аспектов:

- оперативного обмена информацией с морскими судами о произошедших киберинцидентах;
- получения (сбора) имеющейся у судов информации и данных о киберинцидентах, их последствиях и нанесённому ущербу;
- оперативного информирования судов об актуальных киберугрозах и киберрисках;
- информирования судов о необходимых (рекомендуемых) мерах (способах) защиты.

Взаимодействие и интегрирование с ГосСОПКА необходимо для реализации следующих аспектов:

- оперативного обмена информацией о произошедших киберинцидентах на морских судах;
- предоставления информации и данных, необходимых для анализа и оценки киберинцидентов;
- получения актуальной информации о существующих и прогнозируемых киберугрозах;
- получения информации об актуальных средствах и способах защиты.

Взаимодействие автоматизированной ИС ОиПК с ГосСОПКА и СУДС должно осуществляться круглосуточно в режиме «online».

Таким образом, создание автоматизированной ИС ОиПК подразумевает взаимодействие и интегрирование с внешними ИС для реализации части возложенных на неё функций и задач.

СПИСОК ЛИТЕРАТУРЫ

1. Судоходство в аспекте кибербезопасности // Морские вести. 2019. № 18 [Электронный ресурс]. URL: http://www.morvesti.ru/analitika/1689/82714/ / (дата обращения: 20.06.2020).1.
2. Моряки чаще выходят на связь [Электронный ресурс]. – URL: http://www.sur.ru/ru/news/lent/2021-05-31/morjaki_chashhe_vykhodjat_na_svjaz_20123/ (дата обращения 20.06.2021).
3. Семенов С.А. Морская кибербезопасность: 01.01.2021 // Морские вести. 2020. № 10 [Электронный ресурс]. URL: http://www.morvesti.ru/analitika/1692/86359/?sphrase_id=3602295/ (дата обращения: 20.06.2021).

УДК 004.056

СФЕРА ПРИМЕНЕНИЯ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОЦЕНКИ И ПРОГНОЗИРОВАНИЯ КИБЕРУГРОЗ НА МОРСКИХ СУДАХ ПОД ФЛАГОМ РФ

Когтев Алексей Валерьевич, Ныркoв Анатолий Павлович
Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
e-mails: xx.ww.zz@ya.ru, apnyrkow@mail.ru

Аннотация. В статье рассмотрена возможная сфера применения автоматизированной информационной системы оценки и прогнозирования киберугроз на морских судах под флагом РФ.

Ключевые слова: автоматизированная информационная система; киберугрозы; кибербезопасность; морские суда; речные суда.

SCOPE OF THE AUTOMATED INFORMATION SYSTEM FOR ASSESSING AND PREDICTING CYBER THREATS ON SEA VESSELS UNDER THE FLAG OF THE RUSSIAN FEDERATION

Kogtev Alexey, Nyrkov Anatoliy
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
e-mails: xx.ww.zz@ya.ru, apnyrkow@mail.ru

Abstract. The article discusses possible areas of application of an automated information system for assessing and predicting cyber threat on sea vessels under the flag of the Russian Federation.

Keywords: automated information system; cyber threat; cybersecurity; sea vessels; river vessels.

Современный уровень развития информационных технологий и масштаб, стоящих перед судоходной отраслью задач, обуславливает активный рост объёмов загрузки данных морскими судами, развития технологий автономного (безэкипажного) судоходства и автоматизации судовых процессов [1-3]. Например, с января 2020 года по март 2021 года среднесуточный объём загрузки данных на одно судно вырос в 3 раза и составил 9,8 гигабайт в сутки [4]. Вследствие этого, очевиден рост количества киберинцидентов на морских судах и повышение уровня реализации киберугроз в отношении судов [5, 6]. Таким образом, морская кибербезопасность для судоходной отрасли становится все более актуальной [7, 8].

Одной из мер, направленных на обеспечение морской кибербезопасности, может стать создание автоматизированной информационной системы оценки и прогнозирования киберугроз на морских судах под флагом РФ (автоматизированная ИС ОиПК).

Автоматизированная ИС ОиПК может быть применима на различных типах (классов) судов:

- танкерах;
- сухогрузах;
- газовозах;
- контейнеровозах;
- паромах и судах «ро-ро»;
- пассажирских и круизных судах.

Сфера применения автоматизированной ИС ОиПК может быть расширена и применяться не только для морских судов, но и для речных судов каботажного плавания и класса типа «река-море». Это обусловлено тем, что современные киберугрозы для водного транспорта во многих случаях могут быть одинаково реализуемы и на морских, и на речных судах [9, 10].

Учитывая темпы развития автономного (безэкипажного) судоходста в мире и исследований в этой области, важнейшей сферой применения, автоматизированной ИС ОиПК в перспективе, могут стать подобные суда. Именно автономное (безэкипажное) судоходсто со временем может не только заменить собой традиционные суда с командами (экипажем), но и оказать существенное влияние на перечень актуальных киберугроз для морских судов и способы их реализации.

Отдельно стоит выделить особую сферу возможного применения автоматизированной ИС ОиПК, которая при необходимости сможет быть направлена на:

- буксиры, лоцманские суда, портовый флот;
- различные морские суда специального назначения;
- корабли Военно-Морского Флота и Пограничной службы ФСБ России.

Автоматизированная ИС ОиПК также должна предусматривать возможность интегрирования и реинтегрирования отдельных подсистем в свою структуру в случае необходимости, что может влиять на сферу её применения. Отметим, что расширение сферы применения, автоматизированной ИС ОиПК может происходить за счёт интегрирования в неё различных новых подсистем (например, подсистемы речного флота) или за счёт расширения существующих подсистем.

Помимо этого, сфера применения автоматизированной ИС ОиПК должна отражать в себе не только направленность непосредственно на различные суда, но и возможность информационного взаимодействия с

другими ИС (АСУ) в рамках выполнения возложенных на автоматизированную ИС ОиПК функций и задач, например, с системой ГосСОПКА, СУДС и др.

Таким образом, автоматизированная ИС ОиПК может иметь широкую сферу применения, охватывающую различные типы (классы) судов, в том числе с учётом современных мировых тенденций, таких как автономное (безэкипажное) судоходство, а также охватывающую и область информационного взаимодействия со сторонними ИС. Данные условия смогут способствовать эффективной реализации широкого круга возложенных на автоматизированную ИС ОиПК функций и задач, что позволит повысить общий уровень кибербезопасности на судах под флагом РФ.

СПИСОК ЛИТЕРАТУРЫ

1. 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, No. 5. – 2020. – Pp. 6619 - 6625. https://doi.org/10.3233/JIFS-179741
2. 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. https://doi.org/10.1109/EIConRus49466.2020.9039181
3. Судоходство в аспекте кибербезопасности // Морские вести. 2019. № 18 [Электронный ресурс]. URL: http://www.morvesti.ru/analitika/1689/82714 (дата обращения: 20.06.2020).
4. Моряки чаще выходят на связь [Электронный ресурс]. – URL: http://www.sur.ru/ru/news/lent/2021-05-31/morjaki_chashhe_vykhodjat_na_svjaz_20123/ (дата обращения 20.06.2021).
5. Sokolov S. Countering Cyberattacks During Information Operations / S. Sokolov, A. Nyrkov, T. Knysh, A. Shvets // In: Mottaeva A. (eds) Proceedings of the XIII International Scientific Conference on Architecture and Construction 2020. Lecture Notes in Civil Engineering, vol 130. Springer, Singapore. – 2021. – Pp. 84 - 100. https://doi.org/10.1007/978-981-33-6208-6_8
6. Shipunov, I.S. Investigation of Computer Incidents as an Important Component in the Security of Maritime Transportation / I. S. Shipunov, A. P. Nyrkov, M. U. Ryabenkov, A. A. Nyrkov, Y. F. Katorin // Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). – 2021. – Pp. 657-660. https://doi.org/10.1109/ElConRus51938.2021.9396501
7. Семенов С.А. Морская кибербезопасность: 01.01.2021 // Морские вести. 2020. № 10 [Электронный ресурс]. URL: http://www.morvesti.ru/analitika/1692/86359/?sphrase_id=3602295/ (дата обращения: 20.06.2021).
8. 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. https://doi.org/10.1007/978-3-030-19756-8_46
9. Shipunov, I.S. The Concept of a Partially Unmanned Sea Convoy / I. S. Shipunov, A. P. Nyrkov, M. U. Ryabenkov, A. A. Nyrkov, Y. F. Katorin // Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). – 2021. – Pp. 661-664. https://doi.org/10.1109/ElConRus51938.2021.9396302
10. 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 – 2020. – Pp. 958–963. https://doi.org/10.3103/S0146411620080234

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ МОРСКОЙ ТЕХНИКИ И МОРСКОЙ ИНФРАСТРУКТУРЫ

УДК 629.12

КВАЛИМЕТРИЧЕСКИЙ SWOT-АНАЛИЗ ПРОГРАММНЫХ КОМПЛЕКСОВ РОБОТИЗАЦИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ИНЦИДЕНТАМИ

Алексеев Анатолий Владимирович, Куприянов Дмитрий Олегович, Заведеев Юрий Михайлович, Гадаев Егор Михайлович, Стефанович Игорь Денисович
Институт автоматизации процессов борьбы за живучесть корабля, судна
Ленинский пр., 101, Санкт-Петербург, 198262, Россия
e-mail: iapbgks@bk.ru

Аннотация. В развитие вопросов роботизации управления информационной безопасностью автоматизированных систем в защищенном исполнении (АСЗИ) как основного способа снижения негативного влияния человеческого фактора операторов АСЗИ, сформирована квалиметрическая база данных и знаний (КБДЗ) программно-аппаратных комплексов (ПАК), декларирующих возможность автоматического управления информационными инцидентами. Выполненный по технологии QSWOT анализ показал, что данная задача является исключительно сложной и далеко нерешенной при ее особой востребованности в настоящее время. Приведены сравнительные свойства и количественные оценки конкурентного превосходства 14 вариантов ПАК роботизированного управления информационными инцидентами информационной безопасности (РУБ), среди которых конкурентно способным определен вариант интеграции SOC & СПРУ, рекомендуемый для судов, портового оборудования, систем навигационного обеспечения, АСЗИ управления портами и пароходствами.

Ключевые слова: роботизация управления инцидентами; квалиметрический анализ; синтез; оптимизация; технология сравнения свойств; конкурентное превосходство.

QUALIMETRIC SWOT ANALYSIS OF SOFTWARE SYSTEMS FOR ROBOTIZATION OF INFORMATION INCIDENT MANAGEMENT

Alekseyev Anatoly, Kupriyanov Dmitry, Zavadeev Yuri, Gadaev Egor, Stefanovich Igor
Institute of automation of processes of struggle for survivability of the ship, vessel
101 Leninsky Av, St. Petersburg 198262, Russia
e-mail: iapbgks@bk.ru

Abstract. In the development of issues of robotization of information security management of automated systems in protected execution (ASSI) as the main way to reduce the negative impact of the human factor of ASPI operators, a qualimetric database and knowledge (KBDZ) of software and hardware complexes (PAK) declaring the possibility of automatic management of information incidents has been formed. The analysis performed using SWOT technology showed that this task is extremely complex and far from unsolved, given its special demand at the present time. Comparative properties and quantitative estimates of the competitive advantage of 14 variants of the automated control system for information security Information incidents (RUB) are presented, among which the SOC & SPRU integration option recommended for ships, port equipment, navigation support systems, ASSI management of ports and shipping companies is determined to be competitive.

Keywords: robotization of incident management; qualimetric analysis; synthesis; optimization; property comparison technology; competitive advantage.

В развитие вопросов роботизации управления информационной безопасностью АСЗИ [1-4] как основного способа снижения негативного влияния человеческого фактора операторов АСЗИ, в результате исследований [3] была впервые сформирована и опубликована КБДЗ ПАК РУБ, декларирующих возможность автоматического управления инцидентами информационной безопасности (ИБ).

Актуализация КБДЗ на настоящий момент позволила перейти к ее анализу по технологии QSWOT, который подтвердил, что задача РУБ, в решение которой участвуют более десятка вендеров, является исключительно сложной и далеко нерешенной в настоящее время при ее особой востребованности и актуальности для обоснования облика, структуры и характеристик ПАК роботизированного управления ИБ.

В этой связи представляется ***актуальным*** обобщить полученные данные и сформулировать результаты сравнительного количественного анализа с определением наиболее предпочтительных ПАК обеспечения информационной безопасности (ОИБ) при решении задач анализа (задача IDS) и предотвращения (задача IPS)

информационных вторжений в типовых условиях функционирования АСЗИ. В том числе ПАК РУБ для использования на судах, АСЗИ портов и пароходств, систем навигационного обеспечения, АСЗИ береговых центров экстренного реагирования и других объектов морской техники и морской инфраструктуры (ОМТИ).

Данная задача в последнее время приобретает особую актуальность в связи с особой практической значимостью. Решения задачи на сегодня практически нет. И, как это часто бывает, многие исследователи эту задачу пытаются решить, заходя «с разных сторон», о чем говорит весьма немалое количество публикаций. От самых «прямолинейных» подходов, требующих решения «здесь и сейчас» типа [4], до «системных» с полномасштабным обзором большого числа источников, неменьшим числом критериев сравнения (порядка 180!, но одноуровневых, что вызывает большое сомнение) и их аналитическим обобщением типа [5].

Понимая особую значимость решения данной задачи сегодня, мы стремились получить ответ на вопрос о перспективных путях максимально полной автоматизации задачи ОИБ, ее роботизации (в «нашем» контексте [1-3]) с позиции многокритериального количественного (цифрового) оценивания и обоснованного выбора оптимального (лучшего из возможных альтернативных) путей. В этой связи в состав «нашей» КБДЗ вошли с учетом опыта [1-3, 6-10] 14 рассмотренных альтернативных вариантов ПАК РУБ АСЗИ. Предложения типа «ручного» мониторинга приложений, снимков экрана, клавиатуры и т.п. были сразу вынесены за рамки анализа как не дающие ответ на главный вопрос РУБ АСЗИ. Из 14 «сильных» альтернатив в результате сравнительного анализа удалось выделить 7 лидирующих по критерию агрегированного показателя качества (АПК) вариантов. Анализ полученных результатов позволил сделать следующие выводы:

В сравнении с первоначальным вариантом КБДЗ [3] по состоянию на февраль 2021 г., в котором конкурентно способными вариантами были ПК по вариантам 45 (при оценке качества по АПК Q=9,4) и 41 (Q=8,6), введение в рассмотрение и практическое тестирование варианта 52 (DLP), а также рассмотрение варианта 51 (DLP & СПРУ) его интеграции с вариантом 17 (СПРУ), позволило, с одной стороны, уточнить свойства и количественные оценки по критериям S, W, O, T и Q, а, с другой стороны, выйти, по нашему мнению, на более корректные сравнительные оценки ПАК РУБ по качеству ОИБ с Q=8,46 (вариант 46).

Рассмотренные декларируемые варианты ПАК РУБ, по нашему мнению, задачу в полном объеме и с требуемым качеством в реальном масштабе времени (РМВ) без интеграции с СПРУ не решают.

Именно интеграция с ПАК типа СПРУ позволяет в РМВ за счет квалиметрической оценки системных свойств и характеристик процессов РУБ, их безизбыточной визуализации с цветовым кодированием, а также системного мониторинга и контроля позволяет практически автоматически реагировать на инциденты.

Алгоритмы реагирования в КБДЗ формируются по дискреционному принципу с учетом всего комплекса требований руководящих и нормативно-методических документов, а также «дерева» сценариев.

При этом, среди типовых инцидентов рассматриваются несанкционированный доступ в сеть Интернет, DDoS-атака, многократный ввод неправильного логина/пароля, установка программного обеспечения и др.

В соответствии с данными моделями инцидентов в качестве типовых вариантов реагирования на инциденты рассматриваются процедуры перехвата трафика (копирование), блокирование трафика устройств и сетевых каналов, карантин трафика, формирование теневых копий, блокировка по содержимому и др.

Конкурентные варианты 46, 45, 51 близки по уровню качества РУБ, что указывает на целесообразность организационного объединения усилий вендеров DLP, SGRC, SOC, СПРУ и соответствующую возможность форсированной разработки перспективной технологии создания ПАК РУБ.

Приведенные с использованием технологии QSWOT - экспресс-анализа (по 4 критериям) сравнительные свойства и количественные оценки конкурентного превосходства 14 альтернативных вариантов ПАК роботизированного управления информационными инцидентами подлежат дополнительной проверке и возможному уточнению в соответствии с концепцией полимодельного подхода путем сопоставления с результатами многокритериального анализа качества, например, по технологии АСОР, АСПИД, МАИ [1, 2, 8].

Дальнейшая актуализация КБДЗ представляется нам уже более доступной, так как сравнение новых вариантов ПАК будет удобно оценивать и анализировать в сопоставлении с выявленными лидерами рынка, что одновременно позволит повысить точность оценивания, корректировать ранее введенные данные.

Перспективными направлениями дальнейших исследований по обоснованию, разработке технологии и созданию программно-аппаратных средств роботизированного управления инцидентами информационной безопасности, по нашему мнению, следует считать интеграцию усилий разработчиков по согласованию позиций в части выбора системы критериев и формированию требований к ПАК РУБ, учету широкого спектра вариантов реагирования на информационные вторжения, системы критериальных предпочтений.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В., Воробьев В.И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с. 153 – 159.
2. Алексеев А.В., Балицкая К.В. Роботизация управления как способ снижения негативного влияния человеческого фактора на информационную безопасность АСЗИ / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7 / СПОИСУ. – СПб., 2019, с. 237-242.
3. Алексеев А.В., Куприянов Д.О., Заведеев Ю. М., Стефанович И.Д. Анализ интеллектуальных технологий управления ИБ морских интегрированных автоматизированных систем // Актуальные проблемы морской энергетики: материалы десятой международной научно-технической конференции в рамках Пятого Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2021, с. 363 – 369.
4. Как мы DLP-систему выбирали (практический опыт) - https://habr.com/ru/post/440838/ (Дата обращения – 7.01.2021).
5. Сравнение систем SGRC (SECURITY GOVERNANCE, RISK, COMPLIANCE) 2017 - https://eplat4m.ru/articles/id/42/ (7.04.2021).

6. Куприянов Д.О., Стефанович И.Д., Заведеев Ю.М., Алексеев А.В. Развитие технологии IDS и комплексная безопасность мореплавания // Межвузовская научно-практическая конференция студентов, аспирантов и молодых ученых «Развитие инфраструктуры внутреннего водного транспорта: традиции, инновации» (РИВВТ-2020) – ГУМРФ, 2020.12.4.
7. Заведеев Ю.М., Куприянов Д.О., Алексеев А.В. Анализ технологий интеграции программных комплексов CRS и СПРУ в интересах роботизации управления информационной безопасностью // Актуальные проблемы морской энергетики: материалы десятой международной научно-технической конференции в рамках Пятого Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2021,
8. 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). XII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2021 г.: Материалы конференции / СПОИСУ. – СПб., 2021.
9. D.O. Kupriyanov, I.D. Stefanowitsch, Ju.M. Zavedeev, Je.M. Gadaev, A.V. Alekseev. Analyse der intelligenten Technologie der Datensicherhetssteuerung “A-SGRC + SPRU” / Д.О. Куприянов, И.Д. Стефанович, Ю.М. Заведеев, Е.М. Гадаев, А.В. Алексеев/ Анализ интеллектуальной технологии управления ИБ “a-SGRC + СПРУ” // 2-я региональная научно-практическая конференция «Диалог поколений», Санкт-Петербург, 23 апреля 2021 г., СПБГУПТД - ВШТЭ.
10. Алексеев А.В., Москаленко В.А., Куприянов Д.О., Заведеев Ю. М., Стефанович И.Д., Гадаев Е.М. Программный комплекс поддержки принятия решений по оценке технической готовности корабля к выходу в море / Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет; науч. ред. Б.В. Соколов. – Севастополь: СевГУ, 2021

УДК 629.561

БЕЗОПАСНОСТЬ ДИСТАНЦИОННОГО КОНТРОЛЯ ЛОГИСТИКОЙ ДВИЖЕНИЯ ТРАНСПОРТА МОРСКОЙ ИНФРАСТРУКТУРЫ

Алексеев Сергей Алексеевич, Гончар Артем Александрович, Парфенов Николай Петрович, Стахно Роман Евгеньевич

Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mail: ksgati@yandex.ru

Аннотация. Представленное в статье решение обеспечивает повышение избирательности, помехоустойчивости и надежности дуплексной радиосвязи между диспетчерским пунктом и объектами управления, которое базируется на материале Патентов РФ авторов статьи № 2733054, Компьютерная система дистанционного контроля и управления объектами морской инфраструктуры, 2020 и № 2725100, Экологический дирижабль, 2020. Предлагаемая система относится к области дистанционного контроля и управления логистикой движения транспорта морской инфраструктуры и может быть использована для принятия решений на всех уровнях контроля и управления процессами на указанных объектах с использованием компьютерной техники.

Ключевые слова: организационное управление; логистика; помехоустойчивость; надежность; фазоманипулированный сигнал.

SECURITY OF REMOTE CONTROL OF LOGISTICS OF TRANSPORT TRAFFIC OF MARINE INFRASTRUCTURE

Alekseyev Sergey, Gonchar Artem, Parfenov Nikolai, Stakhno Roman

St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mail: ksgati@yandex.ru

Abstract. The solution presented in the article provides an increase in the selectivity, noise immunity and reliability of duplex radio communication between the control room and control objects, which is based on the material of the Russian Federation Patents of the authors of article No. 2733054, Computer system for remote monitoring and control of marine infrastructure objects, 2020 and No. 2725100, Environmental Airship, 2020. The proposed system relates to the field of remote control and management of logistics of transport traffic of marine infrastructure and can be used for decision-making at all levels of control and management of processes at these facilities using computer technology.

Keywords: organizational management; logistics; noise immunity; reliability; phase-manipulated signal.

Введение. В условиях роста интенсивности транспортного движения использование крупнотоннажных транспортных средств, перевозка опасных грузов, интенсивность движение транспорта на основных городских путях и подходах к городу увеличивает вероятность транспортных аварий и их неблагоприятных экологических последствий, среди которых одним из самых опасных видов аварийных ситуаций являются столкновения транспортных средств, как на дорогах, так и в акватории порта. Экологическая опасность таких происшествий усугубляется отсутствием специальных коридоров для движения транспорта в портовой инфраструктуре. Учащающиеся аварийные случаи на транспорте, ведущие к катастрофическим последствиям, гибели людей, экологическим катастрофам, а также возросшая угроза террористических актов выдвигают проблему управления обеспечения безопасности на транспорте в ранг общенациональной безопасности.

Основная часть. Наиболее эффективным средством обеспечения безопасности движения транспорта могут быть объекты системы контроля и управления движением портовыми средствами (СКУДПС), осуществляющие мониторинг и контроль за соблюдением правил движения, а при необходимости, помощь в определении

местоположения и при возникновении аварийных ситуаций. СКУДПС представляет собой сложный комплекс стационарных технических сооружений вблизи дорожных служб. К основным недостаткам современных СКУДПС относятся ограниченность зоны действия мониторинга дорожной сети, стационарность размещения (местоположения), недостаточная "привязка" к морской инфраструктуре, громоздкость и сложность применяемых процедур управления, которые требуют дорогостоящего специализированного оборудования и развитой инфраструктуры энергоснабжения. Ключевая функция в основном контуре управления отводится оператору диспетчерского центра СКУДПС, что определяет большое влияние человеческого фактора на принятие решения.

Использование современных СКУДПС эффективно только в экономически развитых регионах с достаточно мощной транспортной инфраструктурой, связанной с обслуживанием крупнотоннажных перевозок. При этом недостаточно внимания уделяется совершенствованию и усилению роли информационных и интеллектуальных технологий в управлении, которые являются альтернативой технической модернизации. Современное развитие и совершенствование информационных технологий, а также технологий искусственного интеллекта позволяет существенно расширить область задач по контролю за обстановкой в районе ответственности современных СКУДПС. К интегральной проблеме из всего выше названного можно выделить проблему организации связи между всеми перечисленными объектами, проблему организации информационной безопасности передачи цифровых данных, проблему эффективности организации сбора и обработки информации.

Каждое транспортное средство или динамической объект морской инфраструктуры должны быть оборудованы специальным контейнером, снабженным радиочастотной меткой и набором отражателей. Контейнер оборудован дуплексной радиостанцией, приемником навигационных GPS-сигналов, датчиками номера и технического состояния транспортного средства или динамического объекта, а также микропроцессором, к которому они подключены [1]. Приемники ГЛОНАС-GPS сигналов, установленные в диспетчерском центре, динамических и стационарных пунктах контроля, а также на транспортных средствах позволяют определять координаты объектов (широту и долготу), скорость их движения и точное время [3].

Решать подобные проблемы возможно с помощью использования специальных мобильных систем управления движением транспортных средств (МСУДТС). В данной статье рассматриваются вопросы построения эффективных систем мониторинга и управления движением в районе ответственности с использованием МСУДТС, основным элементом информационного обеспечения и связи которого может стать дирижабль. Дирижабль имеет аппаратуру оперативной двухсторонней связи между дирижаблем и наземными стационарными, и мобильными центрами управления (далее центры управления) с использованием двух частот и сложных сигналов с фазовой манипуляцией (Фмн), что повышает надежность и достоверность обмена дискретной информацией [2]. Дирижабли могут быть использованы качестве ретрансляторов спутниковой системы геодезической привязки. При этом дирижабли могут размещаться на разных высотах и сами выполнять функции объекта геодезической привязки. Организация связи методом, предложенным в патенте РФ № 2725100, Экологический дирижабль [2] и описанным в предлагаемой статье обеспечит повышение эффективности функционирования СКУДПС за счет улучшения избирательности, помехоустойчивости и надежности дуплексной радиосвязи между дирижаблем и диспетчерским центром, стационарными и динамическими пунктами контроля путем подавления ложных сигналов (помех), принимаемых по дополнительным каналам. Системы фазовой автоподстройки частоты (ФАПЧ) обеспечивают автоматическое слежение за изменениями несущих частот принимаемых сложных Фмн сигналов, которые могут возникать над влиянием различных дестабилизирующих факторов, в том числе и эффекта Доплера [3].

Технической задачей решения, представленного в данной статье и подтвержденного патентом [2] является построение общей структуры комплекса управления СКУДПС за счет использования специальных контейнеров, оборудованных дуплексной радиостанцией, приемником навигационных ГЛОНАС-GPS сигналов, датчиками номера и технического состояния динамических объектов, а также микропроцессором, к которому они подключены [1]. Важнейшей частью задачи является повышение помехоустойчивости и достоверности определения местоположения МСУДТС на базе дирижабля, диспетчерского центра управления и объектов, управляемых ими в режиме реального времени. Что позволит обеспечить повышение эффективности функционирования СКУДПС морской инфраструктуры в целом. Структурная часть задачи решается, приборным составом СКУДПС морской инфраструктуры в целом и в частности МСУДТС на базе дирижабля [4]. Предлагаемый дирижабль в составе МСУДТС обеспечивает повышение надежности и достоверности обмена дискретной информацией между дирижаблем, диспетчерским центром и управляемыми объектами. Реализуемость этого проекта подтверждается широкой демонстрацией дирижаблей на международных авиационных и морских выставках. Энергетическая скрытность данных сигналов определяется их высокой сжимаемостью по спектру и во времени, что позволяет снизить мгновенную излучаемую мощность. Вследствие этого сложный Фмн сигнал в точке приема оказывается замаскированным шумами и помехами. Такие схемные конструкции свободны от дополнительных каналов приема, а системы ФАПЧ обеспечивают автоматическое слежение за изменениями несущих частот принимаемых сложных ФМн сигналов [3].

Заключение. Предлагаемая структура СКУДПС обеспечивает повышение эффективности функционирования за счет помехоустойчивости и достоверности связи между СКУДПС и объектами управления. Это достигается системами акустоэлектронных меток, которые позволяют с высокой точностью

идентифицировать все объекты управления морской инфраструктуры, включая динамические. Важным достоинством таких меток по сравнению с полупроводниковыми является высокая помехоустойчивость и стойкость к электромагнитным и радиационным воздействиям за счет подавления ложных сигналов (помех), принимаемых по дополнительным (зеркальному и комбинационным) каналам. Внедрение в структуру СКУДПС объектов группы МСУДТС на базе дирижабля позволяет существенно расширить площадь контроля и управления объектами морской инфраструктуры, включая динамические. Использование дирижаблей а качестве МСУДТС значительно расширяет функциональные возможности их применения, включая оперативную переброску спасателей на место аварии.

СПИСОК ЛИТЕРАТУРЫ

1. Патент РФ № 2733054, Компьютерная система дистанционного контроля и управления объектами жизнеобеспечения городской инфраструктуры. Алексеев С.А., Дикарев В.И., Парфенов Н.П., Стахно Р.Е. Заявка № 2019135858 от 08.11.2019 г.
2. Патент РФ № 2725100, Экологический дирижабль. Алексеев С.А., Дикарев В.И., Парфенов Н.П., Стахно Р.Е. Заявка № 2019140886 от 11.12.2019г.
3. Дикарев В.И., Ефимов В.В., Калинин В.А., Мельников В.А. Радиочастотная идентификация в нашей жизни. / Изд. Трактат. СПб., 2018. – 246 с.
4. Алексеев С.А., Гончар А.А., Стахно Р.Е., Яковлева Н.А. Повышение эффективности функционирования системы управления движением судов морского порта. / Информационные технологии управления объектами морской техники и морской инфраструктуры. Сборник трудов Морской техники. Выпуск 1 / ИАП БЖКС, эл. изд. - СПб., 2020. - 105 с.

УДК 629.12.001.2

ПРЕДЛОЖЕНИЯ ПО ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЪЕКТА МОРСКОЙ ТЕХНИКИ НА ОСНОВЕ ТЕХНОЛОГИЙ КЛАССА MES В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Алиев Алексей Михайлович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
e-mail: aliev.alexey.98@mail.ru

Аннотация. Рассматривается комплекс вопросов автоматизации и эффективного управления производством при использовании MES-систем. На основе сравнительного анализа наиболее предпочтительных по системному показателю качества программных комплексов в MES-классе типа «СПРУТ-ОКП», «Global MES», «Zenith SPPS» применительно к созданию АПЛ, сделан вывод о том, что использование таких систем позволяют автоматизировать часть рутинной, но напряжённой работы, а также взять на себя задачи по сбору и предоставлению информации для разных уровней менеджмента предприятия. Внедрение этой системы позволяет сэкономить время и средства при производстве, а также для увеличить производительность, но при условии нейтрализации уязвимостей и угроз информационной безопасности, обусловленных внутренними субъективными факторами типа некачественного организационного обеспечения обработки и защиты данных и ошибок обслуживания оборудования.

Ключевые слова: MES-системы; планирование; квалиметрическое ранжирование; технология АСОР-поддержки принятия решения; анализ.

OFFERS FOR DIGITAL TRANSFORMATION OF MARINE EQUIPMENT FACILITIES BASED ON MES TECHNOLOGIES IN A PROTECTED VERSION

Aliev Alexey
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
e-mail: aliev.alexey.98@mail.ru

Abstract. A complex of problems and effective production management when using MES-systems is considered. Based on a comparative analysis of the most preferable software systems in terms of the system quality indicator in the MES-class "SPRUT-OKП", "Global MES", "Zenith SPPS" in relation to the creation of nuclear submarines, it was concluded that the use of such systems makes it possible to automate part of routine work, but hard work, as well as taking on the task of collecting and providing information for different levels of enterprise management. Provides internal subjective factors such as poor organizational data processing and protection and service errors.

Keywords: MES systems; planning; qualimetric ranking; ASOR decision support technology; analysis.

Информационные технологии класса MES призваны решать задачи синхронизации, координировать, анализировать и оптимизировать выпуск продукции в рамках определённого производства с соответствующими корпоративными данными ограниченного распространения [1-4].

Система управления производством — это связующее звено между ориентированными на хозяйственные операции ERP-системами в защищенном исполнении, системами планирования цепочек поставок и деятельностью в реальном масштабе времени на уровне производственных линий и оборудования [5, 13].

Сдерживающим фактором является широкий выбор систем управления предприятием иностранных и отечественных производителей с соответствующим сохранением защищаемых данных. Для заказчика такое

многообразие систем и производителей, а также отсутствие методики по выбору системы для конкретного предприятия является фактором риска. Из-за этого решение о внедрении системы может откладываться, несмотря на назревшую необходимость повышения эффективности управления производством [5].

Внедрение MES-системы при создании, например, АПЛ будет весьма целесообразным для экономии времени и средств, для увеличения производительности в целом. Но следует помнить, что внедрение MES-системы без изменения бизнес-процессов может принести к ресурсным процессам, включая информационные.

Целью данной работы было квалиметрического ранжирование ИТ класса MES с учетом возможности реализации требований по защите данных, а также анализ возможности их внедрения на всех стадиях ЖЦ АПЛ.

Для достижения этой цели предусмотрено решение следующих задач:

1. Квалиметрический анализ и сравнительный анализ свойств, включая информационную безопасность, и характеристик программных средств реализации ИТ класса MES с количественной оценкой конкурентной способности и перспективности развития.

2. Изучение основных положений и освоение методов практического использования современных ИТ данного класса с учетом требований и современных технологий информационной безопасности.

В ходе исследований был произведен сбор и изучение широкого круга материалов с составлением базы данных и знаний для ИТ заданного класса, включая показатели информационной безопасности, аналитический обзор возможностей MES, квалиметрический SWOT-анализ и многокритериальный полимодельный анализ с использованием АСППР «АСОР» [2].

В ходе сравнительного анализа, ранжирования и составления рейтинг-анализа с графической интерпретацией на основе АСППР «АСОР» был сделан вывод, что оптимальным вариантом по всему комплексу требований следует считать программно-аппаратный комплекс «СПРУТ-ОКП».

Его конкурентными преимуществами в сравнении с 7 альтернативными вариантами типа «Global MES», «Zenith SPPS» применительно к процессам создания АПЛ в условиях цифровой трансформации личности, общества и государства следует считать:

Возможность план-факторного анализа и прогнозирования процессов освоения и эксплуатации в типовых условиях производства.

Возможность широкомасштабного использования в различных машиностроительных отраслях в интересах формирования единого информационно-технологического пространства.

Высокое быстродействие процессов выявления информационных инцидентов и их нейтрализации при интеграции с системами класса SIEM.

Стабильное технологическое развитие и совершенствование продуктов линейки «СПРУТ-ОКП» [6] при конкурентной способности в сравнении с «Global MES», «Zenith SPPS» более 15% применительно к процессам создания и освоения АПЛ.

Перспективность практики системного проектирования новых технологических решений одновременно с модулями автоматической защиты данных и контроля организационно-технической защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Алиев А.М. Стартап-проект «Квалиметрическое ранжирование информационных технологий класса "MES" в жизненном цикле объекта морской техники типа «АПЛ пр. 971» / Санкт-Петербург, СПбГМТУ, ИТвЖЦ МТ, 2021 г.
2. Программный комплекс анализа, синтеза и оптимизации решений «АСОР 14.5» / Федеральная служба по интеллектуальной собственности, номер государственной регистрации 2013612649, 24.01.2013.
3. MES-системы. Вид «сверху», взгляд изнутри. Критерии, которые мы выбираем. Web: http://www.management.com.ua/ims/ims146.html. Дата обращения: 29.04.2021.
4. Этапы жизненного цикла промышленных изделий. Web: https://studopedia.ru/18_54529_etapi-zhiznennogo-tsikla-promishlennih-izdeliy.html. Дата обращения: 28.04.2021.
5. Системы управления производством и производственными операциями и современные вызовы. Web: https://habr.com/ru/company/ds/blog/534210/. Дата обращения: 28.04.2021.
6. СПРУТ-ОКП. Система Оперативно-Календарного Планирования и управления производством. Web: https://csprut.ru/sprutokp/. Дата обращения: 29.04.2021.
7. ФОБОС. Web: http://www.fobos-mes.ru/fobos-system/fobos-MES-system.html. Дата обращения: 28.04.2021.
8. PolyPlan. http://polyplan.ru/index_6_polyplan.htm. Дата обращения: 28.04.2021.
9. T-FACTORY 6. Web: http://www.adastra.ru/products/overview/MES/. Дата обращения: 28.04.2021.
10. Global MES. Web: https://global-system.ru/index.php?id=58&idp=5. Дата обращения: 28.04.2021.
11. Zenith SPPS. Web: http://www.zspps.ru/. Дата обращения: 28.04.2021.
12. SIMATIC IT. Web: https://simatic-market.ru/catalog/Siemens-CA01/10016178/info/. Дата обращения: 28.04.2021.
13. MES-системы – функции и преимущества. Web: https://www.tadviser.ru/index.php. Дата обращения: 30.04.2021

УДК 629.12.001.2

ВОЗМОЖНОСИ ИНФОРМАЦИОННОЙ СИСТЕМЫ СТЕНДОВОЙ ДИАГНОСТИКИ ГАЗОТУРБИННЫХ ДВИГАТЕЛЕЙ ПРИ ИХ ВРАЩЕНИИ ОТ ВНЕШНЕГО ПРИВОДА

Баркова Наталия Александровна[1], Грищенко Дмитрий Вячеславович[2], Селищев Кирилл Павлович[1]

[1] Санкт-Петербургский государственный морской технический университет

Лоцманская ул., 3, 190121, Санкт-Петербург, Россия

[2]Ассоциация ВАСТ

Стачек пр., 140, Санкт-Петербург, 198207, Россия

e-mails: barkova@vast.su, gdv@vast.su, skp98@yandex.ru

Аннотация. Рассматривается вопрос создания информационной системы диагностики газотурбинных двигателей на низких частотах вращения в стендовых условиях при холодной прокрутке. Показаны преимущества низкоскоростной диагностики за счет снижения вибрационных помех, вызываемых потоками воздуха и газа при работающей камере сгорания. Практическая диагностика группы двигателей ВК-2500 на стенде завода изготовителя подтвердила возможность вибрационной диагностики их механической системы, а также дополнительные возможности диагностики, которые дает анализ тока приводных электродвигателей.

Ключевые слова: газотурбинный двигатель; вибрация; безопасность; информационная система; диагностика; холодная прокрутка.

CAPABILITIES OF THE INFORMATION SYSTEM FOR BENCH DIAGNOSTICS OF GAS TURBINE ENGINES WHEN THEY ARE ROTATED FROM AN EXTERNAL DRIVE

Barkova Natalia[1], Grishchenko Dmitriy[2], Selishev Kirill[1]
[1] St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
[2]Association VAST
140 Stachek Av, St. Petersburg, 198207, Russia
e-mails: barkova@vast.su, gdv@vast.su, skp98@yandex.ru

Abstract. The issue of creating an information system for gas turbine engines diagnostics at low rotational speeds in bench conditions with cold scrolling is considered. The advantages of low-speed diagnostics are shown by reducing vibration interference caused by air and gas flows when the combustion chamber is running. The practical diagnostics of the VK-2500 engines group at the manufacturer's stand confirmed the possibility of their mechanical system vibration diagnostics, as well as additional diagnostic capabilities provided by the analysis of the drive electric motors current.

Keywords: gas turbine engine; vibration; safety; information system; diagnostics; cold scrolling.

Безопасность эксплуатации и живучесть судна во многом определяется состоянием его движительной установки, оценку которой призваны давать бортовые системы мониторинга и диагностики. Большинство из них рассчитано на обнаружение опасных дефектов незадолго до отказа, и времени на их устранение без нарушения условий эксплуатации судна не хватает.

Естественный путь развития – периодическая диагностика с повышением глубины диагноза, обнаружением зарождающихся дефектов и отслеживанием их развития, позволяющая оценивать интервал безопасной эксплуатации до следующего диагноза. В этом случае система мониторинга и диагностики делится на две части – бортовую, задача которой – обнаружить опасную ситуацию, а также собрать и передать на берег необходимые данные для глубокой диагностики, и береговую, решающую задачи ранней диагностики и прогноза безопасного функционирования, а также планирования работ по обслуживанию и ремонту после возвращения судна в порт.

Существует, однако, энергетические установки, не вписывающиеся в такую концепцию, так как объема данных, получаемых бортовой системой в номинальных режимах работы, не хватает для глубокой диагностики и на борту, и в береговых диагностических центрах. К ним в первую очередь относятся установки с высокооборотными газотурбинными двигателями. Основным процессом, по которому производится их глубокая диагностика, является вибрация. Но в номинальном режиме работы шумы потока в газотурбинном двигателе велики и создают такие вибрационные помехи при диагностировании механических узлов двигателя, которые не позволяют проводить глубокую диагностику энергетической установки, особенно подшипников компрессора и силовой турбины.

Предлагается расширить возможности диагностики высокооборотных движительных установок на основе газотурбинных двигателей, проводя дополнительное диагностирование двигателя в режиме его прокрутки от внешнего привода на низких скоростях вращениях, не запуская камеру сгорания, как это делается в авиастроении при обслуживании авиационных двигателей между полетами. В режиме «холодной» прокрутки на скоростях вращения в 10 раз ниже номинальных уровни шумов двигателя падают более, чем в 30 раз, позволяя диагностировать механическую систему двигателя – валы компрессора и силовой турбины с подшипниками, а также навесные коробки передач систем смазки, электрогенератора и пусковой турбины с использованием традиционных методов вибрационной диагностики роторных машин.

В качестве привода предложено использовать электродвигатель со статическим преобразователем частоты питающего напряжения, последовательно прокручивая компрессор с заторможенной силовой турбиной и силовую турбину с заторможенным компрессором. Возможности такой диагностики отработаны на группе авиационных двигателей ВК – 2500, используемых в составе вертолетов разных модификаций.

Низкоскоростная диагностики газотурбинного двигателя проводилась по его вибрации в стандартных точках его крепления к промежуточной раме, а также по току электродвигателя. Частота вращения валов турбокомпрессора, а также силовой турбины при диагностировании составляла 30 Гц, время синхронного измерения по 8 вибрационным и двум каналам измерения тока составляла от 5 до 15 секунд. Короткое время измерений позволяет перейти от диагностики на стендах холодной прокрутки газотурбинного двигателя к диагностике в режиме его прокрутки в полевых условиях от пусковой газовой турбины.

В результате диагностирования группы из семи новых двигателей ВК-2500 в одном из них были обнаружены признаки слабого дефекта радиально-упорного подшипника турбокомпрессора в виде наклепа наружного кольца подшипника. В двух двигателях были обнаружены признаки неточного монтажа (слабый дефект) зубчатых передач в распределительных устройствах, обеспечивающих вращение вспомогательных механизмов. По результатам проведенных исследований составлен проект основных положений методики диагностирования газотурбинного двигателя ВК-2500 по его вибрации на стенде холодной прокрутки двигателя и по току приводных электродвигателей.

СПИСОК ЛИТЕРАТУРЫ

1. Barkova, N. A. Vibration diagnostics of equipment units with gas turbine engines /Natalia Barkova, Aleksey Barkov, Dmitriy Grishchenko // Vibroengineering Procedia. – 2019. – Vol. 25. – P. 89 – 94. – ISSN 2345-0533.
2. Неразрушающий контроль: Справочник: В 7 т. Под общ. ред. В. В. Клюева. Т.7. В 2 кн. Кн. 2. Вибродиагностика / Ф. Я. Балицкий, А. В. Барков, Н. А. Баркова и др. – М.: Машиностроение, 2005. – 829 с.
3. Рандалл, Р. Б. Частотный анализ / Р. Б. Рандалл. – Глоструп, Дания : К. Ларсен и сын, 1989. – 389 с. – IBSN 87-87355-25-6.
4. Barkov, A. Condition Assessment and Life Prediction of Rolling Element Bearing / A. Barkov N. Barkova, J. Mitchell // Sound and Vibration. – 1995. – Issue 6, P. 10-17.

УДК 629.12

ИНФОРМАЦИОННАЯ ЖИВУЧЕСТЬ КОРАБЛЯ: УГРОЗЫ, МОДЕЛЬ, СИСТЕМНЫЕ ТРЕБОВАНИЯ, ПУТИ РЕАЛИЗАЦИИ

Бобрович Владимир Юрьевич[1], Алексеев Анатолий Владимирович[2], Антипов Василий Васильевич[1], Смольников Александр Васильевич[1]

[1] АО « Концерн «НПО «Аврора»
Карбышева ул., 15, Санкт-Петербург, 194021, Россия
[2] Институт автоматизации процессов борьбы за живучесть корабля, судна
Ленинский пр., 101, Санкт-Петербург, 198262, Россия
e-mails: dpr@avromail.ru, iapbgks@bk.ru

Аннотация. В развитие понятия информационной живучести судна систематизированы 5 угроз информационной живучести корабля, приведена аналитическая модель и сформулированы системные требования по обеспечению борьбы за информационную живучесть корабля, а также организационно-технические пути их реализации. Сформирована парадигма, концепция и приведены технологии борьбы за информационную живучесть корабля в интересах обеспечения информационной устойчивости управления кораблем в составе соединения. Подтверждена целесообразность перехода к технологии роботизированного управления радиоэлектронным и информационным противодействием корабля.

Ключевые слова: информационная живучесть корабля; парадигма; концепция; модель; системные требования; характеристики; технология оценки и мониторинга; исследовательское проектирование.

INFORMATION SURVIVABILITY OF THE SHIP: THREATS, MODEL, SYSTEM REQUIREMENTS, WAYS OF IMPLEMENTATION

Bobrovich Vladimir[1], Alekseev Anatoly[2], Antipov Vasily[1], Smolnikov Alexander[1]

[1] JSC "Concern "NGOs "Aurora»
15 Karbysheva St, St. Petersburg, 194021, Russia
[2] Institute of automation of processes of struggle for survivability of the ship, vessel
101 Leninsky Av, St. Petersburg 198262, Russia
e-mails: dpr@avromail.ru, iapbgks@bk.ru

Abstract. In the development of the concept of information survivability of the ship, 5 threats to the information survivability of the ship are systematized, an analytical model is given and system requirements for ensuring the fight for the information survivability of the ship, as well as organizational and technical ways of their implementation are formulated. The paradigm, concept and technologies of the struggle for the information survivability of the ship are formed in the interests of ensuring the information stability of the control of the ship as part of the connection. The expediency of switching to the technology of robotic control of the ship's electronic and information counteraction is confirmed.

Keywords: information survivability of the ship; paradigm; concept; model; system requirements; characteristics; evaluation and monitoring technology; research design.

Среди факторов развития автоматизированных систем в защищенном исполнении (АСЗИ) объектов морской техники и морской инфраструктуры (ОМТИ) наибольшее влияние на технологическое, организационное и методологическое их развитие оказывают инновационные и инвестиционные системные факторы [1-3]. Их многообразие и разнородность указывает на необходимость соответствующих системных исследований, модельного описания, научно обоснованного ретроспективного анализа и синтеза перспективных вариантов развития с формированием соответствующих ожидаемых и планируемых качественных и количественных показателей развития перспективных образцов АСЗИ ОМТИ.

Актуальность. Одним из важнейших понятий для объектов морской техники является понятие их живучести, определяемое сегодня как способность противостоять последствиям аварийных повреждений, возникновению и распространению пожаров, возникновению взрывов и радиационных заражений, сохранять, восстанавливать и поддерживать при этом в достаточной мере свои мореходные качества и обеспечивать безопасность находящихся на его борту людей, сохранность грузов и судового имущества [4, 5].

Живучесть (survivability) в соответствии с определением профессора Рябинин И.А. рассматривается как способность системы сохранять свойства, необходимые для выполнения заданного назначения при форс-мажорных поражающих воздействиях, не предусмотренных условиями нормальной эксплуатации, т.е. при взрывах, пожарах, затоплениях и прочих факторах, к которым сегодня в полной мере можно относить факторы информационной живучести корабля (ИЖК) [6], устойчивость от воздействия которых непосредственно определяет свойства устойчивости системы управления, защищенность экипажа, живучесть технических средств и оружия, взрыво-, пожаро-, радиационную безопасность и непотопляемость корабля [1, 7, 8].

Понятие ИЖК включает в себя способность обеспечивать постоянную готовность к действиям по прямому назначению, сохранять и восстанавливать свойства корабля при информационных воздействиях (ИВ, инцидентах), готовность противодействовать последствиям ИВ, сохранять и восстанавливать при этом в достаточной мере управляемость корабля, обеспечивать безопасность находящегося на борту экипажа, сохранность общекорабельных систем и имущества.

Борьба за ИЖК должна быть отработанной на тренировках и учениях обязанностью всех членов экипажа, регламентироваться Корабельным уставом, Руководством по обеспечению живучести корабля (РОЖ) и документами по управлению соединением кораблей, требованиями Международного кодекса по управлению безопасностью (МКУБ). Борьба за живучесть корабля (БЖК) - комплекс взаимосвязанных и своевременных, энергичных, инициативных и квалифицированных действий экипажа корабля по комплексному обеспечению живучести корабля в обеспечение эффективного управления кораблем, гарантированное обеспечение безопасности службы экипажа, поддержания в постоянной готовности к действию и эффективному использованию всего комплекса технических средств и оружия.

В этой связи особое внимание сегодня следует уделять комплексной подсистеме (системе) защиты информации (КСЗИ), как одному из ключевых элементов АСЗИ, в состав которой, как правило, входят [1, 2]:

Комплекс организационно-технических мероприятий (КОТМ) по обеспечению ИЖК на основе реализации комплекса мероприятий, регламентированных соответствующей организационно-распорядительной (ОРД) и нормативно-методической документацией (НМД) корабля в составе соединения.

КОТМ по управлению проектным качеством и эффективностью (мерой практической реализации проектного качества) подсистемы ИЖК, включая мероприятия по контролю, оценке технической и боевой готовности корабля по предназначению для действий в составе соединения.

Подсистема мониторинга, прогнозирования, контроля и управления ИЖК в составе АСЗИ.

Подсистема разграничения доступа к информационным ресурсам (ИР) корабля (ПРД).

Подсистема оценки, мониторинга, анализа и контроля защищенности ИР (ПАЗ).

Подсистема обнаружения и защиты от вторжений в ИР (ПЗВ).

Подсистема криптографической защиты ИР (ПКЗИ).

Подсистема защиты от вредоносных (вирусов, спама, фишинга и т.п.) кодов (ПЗВК).

Подсистема контроля целостности ИР корабля в составе соединения (ПКЦ).

При этом типовыми моделями уязвимостей (существующих дефектов построения, функционирования и использования АСЗИ в части ИЖК) и соответствующих угроз ИЖК (потенциальных событий по реализации уязвимостей, нарушению регламентов обработки информации) следует считать:

У-1: Негативное влияние субъективных свойств членов экипажа (ЧФ, «человеческий фактор»). Угроза ЧФ обусловлена недостаточной подготовкой (знаниями, навыками, способностями, опытом) и соответствующими ошибками эксплуатации, ограниченной мотивируемостью (безинициативностью, безответственностью) и нелояльностью (злоупотреблением должностным положением) членов экипажа и т.п.

У-2: Кибер-сетевые воздействия (КСВ), осуществляемые установленными и/или неустановленными субъектами информационного взаимодействия по информационно-коммуникационным каналам. Угроза КСВ реализуется с использованием средств разведки (включая технический шпионаж), средств противодействия, формирования напряженной и ложной обстановки, провоцирования экипажа на нерациональные действия, шантажа, заражения вредоносными кодами с деструктивными функциями, спама и т.п.

У-3: Технологические угрозы (ТУгр), обусловленные спецификой программно-аппаратных средств и процессов (отказ в работе, включая «зависания» программного обеспечения, потеря целостности и доступности данных, использование не по прямому назначению и т.п.).

У-4: Угрозы рефлексивного воздействия (УРВ), обусловленные формированием установленными и/или неустановленными субъектами информационного взаимодействия «целевой» обстановки в информационной среде в интересах рефлексивного управления членами экипажа, кораблем и соединением кораблей в целом.

У-5: Другие возможные и ранее не идентифицированные угрозы (ДрУ), обусловленные интенсивным развитием информационных технологий, включая искусственный интеллект, роботизацию управления.

Модель ИЖК. Для модельного представления процессов и качества создаваемых систем обеспечения ИЖК целесообразно использовать Полимодельный квалиметрический метод системной оптимизации (ПКМ СО) и

соответствующую аналитическую модель, обеспечивающие возможность анализа и синтеза системы ИЖК по агрегированному (интегральному, системному, обобщенному) критерию проектного качества и эффективности при эксплуатации (как меры реализации проектного качества) [10].

Парадигма обеспечения ИЖК, по нашему мнению, должна включать системообразующую идею непрерывной оценки, мониторинга, квалиметрического контроля уровня и управления ИЖК на основе анализа функциональных свойств, проектного качества и эффективности боевого применения корабля по предназначению с учетом всего множества системных критериев и показателей проектного качества.

Концепция обеспечения ИЖК, по нашему мнению, должна включать с учетом специфики и быстротечности процессов информационного взаимодействия и противоборства комплекс взаимосвязанных принципов: роботизированного управления процессами обеспечения ИЖК; делегирования операторам функции целеполагания с исключением их из контура управления целераспределением; системной оптимизации процессов информационного анализа, синтеза, противодействия с использованием ресурсов сетецентрического управления, включая береговые центры реагирования на информационные воздействия (инциденты) и ИЖК.

Системные требования. Для эффективного предотвращения названных возможностей и нейтрализации угроз ИБ, соответствующих рисков ИЖК сегодня, прежде всего, требуются проведение специальных концептуальных и исследовательских (модельных) обоснований вариантов информационного противоборства с вариантным проектированием соответствующих архитектур, функционала и алгоритмов обеспечения ИЖК с информационно-техническим превосходством по каждой из угроз ИВ, У-1…У-5 [11].

Пути реализации. В этой связи уже сегодня по результатам проведенных исследований [9, 11] необходимо форсированное развитие и широкомасштабное внедрение в составе КСЗИ подсистем автоматического квалиметрического мониторинга ИЖК и их соединений, прогнозирования и контроля системной защищенности АСЗИ на основе средств автоматической поддержки решений и управления информационной безопасностью (ИБ) ОМТИ с приоритетным использованием перспективных технологий типа СПРУ в варианте систем организационно-технического мониторинга и управления ИЖК [1, 8, 11]. С учетом специфики ОМТИ и анализа тенденций развития средств обеспечения ИБ общего назначения как никогда остро возникает вопрос применительно к кораблям и судам создания и развития роботизированных систем управления ИЖК, ИБ судна. Это позволит в определенной мере снять дополнительную нагрузку с экипажей судов. С учетом тенденции роста сложности общесудовых и специализированных систем это, как показывает практика, имеет сегодня весьма большое значение.

Заключение. Системный анализ аспектов ИЖК в составе соединений, систематизация угроз ИБ, разработанных вариантов их модельного представления позволяет сформулировать системные требования по БИЖ и определить наиболее перспективные пути реализации этих требований в интересах обеспечения радиоэлектронного и информационного превосходства в информационной сфере, живучести ОМТИ в целом.

Анализ понятийного аппарата, проблем и технологий реализации ИЖК в свете современных требований и регламентов обеспечения безопасности мореплавания указывает на особую актуальность решения сравнительно новой организационно-технической и научной задачи обеспечения гарантированной устойчивости одного из критических сегментов системы управления безопасностью корабля, судна.

СПИСОК ЛИТЕРАТУРЫ

1. Автоматизация процессов борьбы за живучесть корабля, судна // Коллективная монография /Под ред. К.Ю. Шилова. – Санкт-Петербург: ИАП БЖКС, эл. изд. третье, испр. и доп., 2020. – 692 с.
2. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В. Комплексное моделирование системного управления качеством и конкурентной способностью морской техники / Шестая международная научно-практическая конференция «Имитационное и комплексное моделирование морской техники и морских транспортных систем» (ИКМ МТМТС-2021). Труды конференции. – М. Издательство «Перо», 2021, с. 26 – 32.
3. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В. Квалиметрическая концепция цифровизации управления инновационным и инвестиционным развитием предприятия / Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020 г.: Материалы конференции. СПОИСУ. – СПб, 2020, с. 158-160.
4. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В. Информационная технология и система мониторинга конкурентной способности продукции как главного фактора технологического развития предприятия / Материалы конференции «Информационные технологии в управлении» (ИТУ-2018). – СПб.: АО «Концерн «ЦНИИ «Электроприбор», 2018, с. 358 - 362.
5. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В. От декларации и сертификации соответствия к сертификации качества / Актуальные проблемы морской энергетики: материалы девятой международной научно-технической конференции в рамках Четвертого Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2020, с. 363 – 369.
6. Алексеев А.В. Понятие, проблемы и технологии обеспечения информационной живучести судна / Информационная безопасность регионов России (ИБРР-2019). XI Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 24-26 октября 2019 г.: Материалы конференции / СПОИСУ. – СПб., 2019, с. 325-326.
7. Отчет о ОКР «Поддержка-У» (Х-478/11200/4318-2012) «Разработка технологии создания систем информационной поддержки судоводителей по обеспечению безопасной эксплуатации систем (погрузки, выгрузки танков, системы вентиляции и т.п.) в нормальных условиях и при аварийных ситуациях» - СПбГМТУ, 2014. № ДЛМК 421452.034 ПЗ, инв. № 012221.
8. Алексеев А.В., Смольников А.В., Ушакова Н.П., Сус Г.Н. Программный комплекс Макетного действующего образца Системы информационной поддержки судоводителей при обеспечении безопасности эксплуатации в части грузовых операций, локализации аварийных ситуаций, аварий и борьбы за живучесть морских объектов повышенного риска (ПК МДО СИП ЛА-ГО о3) – Свидетельство о государственной регистрации программ для ЭВМ (Реестр программ ФСИС) № 2014614620, 29.04.2014.
9. Алексеев А.В., Воробьев В.И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с. 153 - 159.
10. Алексеев А.В. Модель инвариантной оценки качества и эффективности объектов морской техники / Морские интеллектуальные технологии/Marine intellectual technologies, № 2 том 2, 2020, с. 53-60.
11. Алексеев А.В., Карпов А.Е., Каганский М.А. Модель и технология мониторинга военно-технического превосходства в морской операции / Интеллектуальные разработки в интересах строительства и развития ВМФ: Тр. НИИ ОСИС ВМФ ВУНЦ ВМФ «Военно-морская академия». Науч.-техн. сб. статей и докладов (с включением матер. НТК 6.12.2018 г.) – Петродворец, 2019. – Ч. 1. – С. 15–25.

УДК 629.12

ПРЕДЛОЖЕНИЯ ПО ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОМТ КЛАССА ЛЕСОВОЗ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Богданов Антон Валерьевич, Макеев Александр Сергеевич
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
e-mail: antonluxcor@gmail.com

Аннотация. Рассматриваются вопросы, связанные с цифровой трансформацией объектов морской техники (ОМТ) типа Лесовоз. Произведён квалиметрический анализ альтернативных вариантов ERP систем в защищенном исполнении. Приведены экспертные оценки, касающиеся внедрения ERP систем. Приведен перечень предложений по цифровизации ОМТ типа Лесовоз.

Ключевые слова: цифровая трансформация; цифровизация; ERP в защищенном исполнении; объект морской техники; квалиметрический анализ; жизненный цикл.

OFFERS FOR DIGITAL TRANSFORMATION OF MTO CLASS LESOVOZ IN A PROTECTED VERSION

Bogdanov Anton, Makeev Aleksandr
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
e-mail: antonluxcor@gmail.com

Abstract. The issues related to the digital transformation of Timber carrier are considered. A qualimetric analysis of alternative options for ERP systems has been performed. Provides expert assessments regarding the implementation of ERP systems. A list of proposals for the digitalization of Timber carrier is presented.

Keywords: Digital transformation; digitalization; ERP; marine engineering facility; qualimetric analysis; life cycle.

В настоящее время термины цифровая трансформация, цифровизация используется в узком и широком смысле. Под цифровизацией в узком смысле понимается преобразование информации в цифровую форму, которое в большинстве случаев ведет к снижению издержек, появлению новых возможностей и т. д. Большое число конкретных преобразований информации в цифровую форму приводит к таким существенным положительным последствиям, которые обусловливают применение термина цифровизации в широком смысле [1]. В широком смысле под цифровизацией понимают тренд эффективного развития, охватывающий различные сферы деятельности человека (науку, бизнес, производство и т.д.)

Цифровая трансформация требует смещения акцента на периферию предприятий и повышение гибкости центров обработки данных, которые должны поддерживать периферию при одновременном качественном обеспечении защиты данных. Этот процесс также означает постепенный отказ от малоэффективных технологий, обслуживание которых может дорого обходиться предприятиям, а также изменение «цифровой культуры», которая теперь должна поддерживать ускорение процессов, обеспечиваемое цифровой трансформацией [2].

При цифровой трансформации предприятия можно выделить два крупных этапа [3]:

1. Развитие технической инфраструктуры. На этом этапе осуществляются изменения в технической инфраструктуре предприятия: происходит автоматизация процессов производства; создаются центры для хранения данных; полученная информация структурируется; подготавливаются центры для анализа и информационной защиты полученных данных.

2. Развитие компетенций персонала. На этом этапе происходит перестроение процессов управления; происходит внедрение систем искусственного интеллекта в производство; происходит обучения персонала; совершенствуются процессы сбора и обеспечения информационной безопасности данных.

В настоящее время на предприятиях большинство процессов уже автоматизированы, на них осуществляется сбор и хранение данных, некоторые предприятия даже строят дата-центры. Однако, сотрудники зачастую не извлекают пользу из этой информации. Поэтому для цифровой трансформации недостаточно просто использовать передовые технологии, необходимо также качественно обучать персонал работе с ними.

К основным положительным последствиям цифровизации можно отнести [1]:

1. Повышение качества жизни и появление экономического и социального эффекта за счет повышения конкурентной способности продукции и услуг;

2. Ускорение бизнес-процессов, снижение издержек, повышение гибкости предприятия за счет комплексной автоматизации процессов;

3. Осуществление автоматической переработки и анализа больших объемов данных, прежде всего, переход на полномасштабное использование систем электронного документооборота.

Рассмотрены основные аспекты цифровизации на примере объектов морской техники типа Лесовоз при внедрении информационных технологий и систем класса ERP в защищенном исполнении.

ERP (Enterprise Resource Planning - планирование ресурсов предприятия) — это класс систем для управления производством, трудовыми ресурсами, финансами и активами, ориентированных на оптимизацию ресурсов предприятия.

Комплексные системы управления предприятием, такие как ERP, это, в первую очередь, инструмент для планирования ресурсов предприятия. Системы ERP предназначены для хранения и обработки большого объема данных с учетом сохранности корпоративной тайны, что позволит более рационально распределять производственные ресурсы и принимать точные управленческие решения.

В жизненном цикле объекта морской техники типа Лесовоз ERP-системы используются, прежде всего, на этапе подготовки производства и реализации основных производственных процессов.

Основную информационную поддержку процессов ЖЦ ОМТ должно составлять единое информационное пространство, в котором будет циркулировать в защищенном исполнении вся информация, полученная на каждом этапе ЖЦ ОМТ. Для решения этой задачи применяют интегрированные системы поддержки ЖЦ изделия (Product Life Cycle Management, PLM). Такие системы объединяют в себе САПР, ERP, PDM, SCM, CRM и другие автоматизированные системы, причем, одновременно нескольких предприятий.

В ходе исследований был проведён квалиметрический анализ современных систем данного класса. Был подготовлен перечень систем, в который вошли как отечественные, так и зарубежные системы. В результате анализа лучшей системой по критерию максимума агрегированного (интегрального) показателя качества была признана «1С:ERP» в защищенном исполнении в сравнении с альтернативными вариантами «SAP R3» и «Axapta».

На сегодняшний момент по публикуемым данным программные продукты «1С:ERP» используются более чем в 11 000 компаний. Порядка 65 000 пользователей успешно автоматизировали свой бизнес.

При непосредственном использовании 1С:ERP можно достичь [4]:

- сокращения расходов на материальные ресурсы (по экспертным оценкам до 9%);
- снижения производственных издержек (до 7%);
- сокращения трудозатрат в различных подразделениях (до 30%);
- ускорения получения управленческой отчетности (до 4 раз);
- сокращения операционных и административных расходов (до 15%);
- сокращения сроков исполнения заказов (до 25%).

Конечно, цифровизацию необходимо осуществлять как в рамках систем управления производственными процессами ERP и жизненным циклом продукции (PLM), так и дальнейшего обслуживания на протяжении всего жизненного цикла ОМТ.

Поэтому для цифровой трансформации ОМТ типа «Лесовоз» необходимо:

1) убедить руководство предприятия в эффективности использования ERP-систем в защищенном исполнении с обоснованным выбором оптимального варианта системы класса ERP с дальнейшей поддержкой;
2) обучить работников предприятия эффективной работе с выбранной программой;
3) непрерывно способствовать дальнейшему развитию предприятия в области цифровизации;
4) создать условия по системному импортозамещению в области цифровизации;
5) создать условия по тестированию различных вариантов ERP-систем, после чего внедрять их;
6) поддерживать «цифровизированные» предприятия. После внедрения программного продукта необходимы рекомендации по улучшению бизнес-процессов и процессов производства;
7) создать условия по реализации отечественных защищенных облачных технологий;
8) применять ERP-систем как частными, так и государственными компаниями;
9) наращивать возможности ERP-систем, например, за счет использования возможностей подсистем искусственного интеллекта. По мнению отдельных экспертов [5], они уже сегодня могут принимать полноправное участие в решении любых бизнес-задач, в том числе традиционных для ERP-систем;
10) интегрировать ERP-системы в защищенном исполнении с мобильными телефонами, в частности, с чат-ботами, для повышения удобства работы с ними, прежде всего, ключевым пользователем.

СПИСОК ЛИТЕРАТУРЫ

1. Халин, В. Г. Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски* / В. Г. Халин, Г. В. Чернова // Управленческое консультирование. — 2018. — № 10. — С. 46-63.
2. Что такое цифровая трансформация. — Текст : электронный // Hewlett Packard Enterprise Development : [сайт]. — URL: https://www.hpe.com/ru/ru/what-is/digital-transformation.html (дата обращения: 03.05.2021).
3. Максим, Комель Цифровая трансформация производства / Комель Максим. — Текст : электронный // DuPont Sustainable Solutions : [сайт]. — URL: https://www.consultdss.ru/digital-transformation-production-operations (дата обращения: 03.05.2021).
4. Описание программы 1С:ERP. — Текст : электронный // Новое образование : [сайт]. — URL: https://www.vnedriupp.ru/region/ (дата обращения: 20.03.2021).
5. Сергей Свинарев, ERP и цифровая трансформация / Свинарев Сергей. — Текст : электронный // ITWeek : [сайт]. — URL: https://www.itweek.ru/idea/article/detail.php?ID=208664 (дата обращения: 22.03.2021).

УДК 629.12.001.2

ПРОБЛЕМА СОЗДАНИЯ ЕДИНОЙ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Каранташев Дмитрий Викторович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
e-mail: dkarantashev@mail.ru

Аннотация. Рассматривается комплекс вопросов автоматизации и эффективного управления деятельностью объекта морской техники типа Администрация большого порта «Санкт-Петербург» за счет внедрения технологии единой системы электронного документооборота. При неоспоримых преимуществах ускорения обмена информационными ресурсами, обеспечения информационной прозрачности документопотока, повышения исполнительской дисциплины показано, что актуальной задачей развития государства, общества, личности в стране является научно-техническое обоснование и создание национальной единой системы электронного документооборота в защищенном исполнении.

Ключевые слова: единая система электронного документооборота; цифровизация; квалиметрическое ранжирование; оптимизация; морской порт; эффективность.

THE PROBLEM OF CREATING A UNIFIED ELECTRONIC DOCUMENT MANAGEMENT SYSTEM IN A SECURE VERSION

Karantashev Dmitriy
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
e-mail: dkarantashev@mail.ru

Abstract. The complex of issues of automation and effective management of the activities of the marine equipment facility of the Large Port Administration "Saint Petersburg" type due to the introduction of the technology of the unified electronic document management system is considered. With the undeniable advantages of accelerating the exchange of information resources, ensuring information transparency of the document flow, and improving performance discipline, it is shown that the current task of the development of the state, society, and the individual in the country is the scientific and technical justification and creation of a national unified electronic document management system in a secure execution.

Keywords: unified electronic document management system; digitalization; qualimetric ranking; optimization; seaport; efficiency.

Проблема внедрения единой системы электронного документооборота в защищенном исполнении уже долгие годы остается актуальной в нашей стране. В ходе реализации национального проекта «Цифровая экономика» к 2024 г. государство намерено осуществить комплексную цифровую трансформацию экономики и социальной сферы России, одним из важнейших элементов которой, по нашему мнению, должно быть создание единой национальной системы электронного документооборота (ЕСЭД).

Система документооборота (СЭД) предприятия или организации – базовый элемент их «цифровой» инфраструктуры. Вместе с тем, работа с «внешними» и «внутренними» документами - наиболее сложно организуемый, трудоемкий и «проблемный» участок их деятельности. Именно электронные решения СЭД подобно кровеносной системе живого организма дают возможность существенно упростить, ускорить и оптимизировать ее.

Использование систем электронного документооборота открывают новые перспективы по повышению прибыльности, эффективности, оптимизации потоков информации и бумаг, межведомственному взаимодействию.

Вместе с тем, процесс внедрения СЭД сегодня обладает целым рядом проблем:

1. Сложности в процессе организации. Она возникают тогда, когда нет четкого понимания того, зачем необходимы СЭД и в том случае, если персонал не заинтересован в использовании новых принципов работы, т.к. при этом существенно возрастает информационная «прозрачность» процессов документооборота, их хранения, обеспечения режима разграничения доступа, повышение контролируемости исполнительской дисциплины, строгого соблюдения технологических регламентов.

2. Традиционная проблема ограниченных финансовых возможностей организаций на приобретение, освоение современных систем электронного документооборота, общее число которых на рынке давно превысило 70 при их практически одинаковых решаемых задачах. И это в условиях, когда в стране по существу нужны всего порядка трех «универсальных» и единых для государства СЭД, например: для открытого документооборота широких масс населения и их взаимодействия с организациями любого уровня, включая государственные; для обработки персональных данных и других видов конфиденциального документооборота (врачебная, юридическая, коммерческая тайна и т.п.); для обработки документов, содержащих государственную тайну и обладающих средствами гарантированной защиты.

Как нам известно, проблема создания единых контуров документооборота в стране даже не поднимается, а решается на «местном» уровне каждой организацией самостоятельно, что, естественно, приводит к неоправданным ресурсным затратам и, даже, снижению уровня защиты данных, ее контроля и неуправляемости.

3. Сложность переходного к «безбумажным технологиям» процесса, обусловленная необходимостью непрерывной актуализации баз данных и поддержания гибкости процессов при одновременной необходимости выполнения ряда требований по хранению документов в традиционной бумажной форме. Более того, если рассматривать данную проблему с точки зрения крупного предприятия, где используется документация, содержащая коммерческую тайну, переход на безбумажные технологии невозможен в связи с высокими

требованиями к безопасности. Данная проблема также требует своего научно-методического обоснования и решения на государственном уровне путем корректировки соответствующих регламентов.

4. Немаловажная проблема сложности выбора СЭД с учетом специфики и принятых на предприятии регламентов обработки документов, в том числе в части информационной безопасности, которая, по нашему мнению, может потерять свою актуальность после принятия решений на государственном уровне о создании в стране системы единой СЭД.

В этих условиях эффект от внедрения, например, СЭД «Directum» в Администрации большого порта «Санкт-Петербург» практически не поддается учету. Прямой эффект от внедрения системы связан с экономией рабочего времени сотрудников и средств на материалы (исчисляемые выгоды). Но есть и так называемые неисчисляемые выгоды, обусловленные теми преимуществами функционирования организации, которые дает автоматизированная система (скорость и качество предоставления услуг, сокращение времени прохождения документов, повышение качества выпускаемых документов и контроля исполнительской дисциплины и т.д.).

С учетом изложенного возникает актуальная задача государственного значения - научно-технического инновационного обоснования создания в России единой системы электронного документооборота в информационно-защищенном исполнении в обеспечение цифровизации государства, общества, личности. Преимущества ЕСЭД по существу не вызывают сомнений, т.к. позволят существенно повысить качество организационной инфраструктуры государства. Однако, решение этой задачи потребует и качественно новых решений в области защиты данных.

Это, полагаем, одновременно позволит продвинуть и сами технологии информационной безопасности за счет концентрации национальных усилий на решении важной государственной задачи создания единого информационно-защищенного пространства взаимодействия граждан, организаций и государства в целом.

СПИСОК ЛИТЕРАТУРЫ

1. Цифровизация управления и системы электронного документооборота [Электронный ресурс] URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-upravleniya-i-sistemy-elektronnogo-dokumentooborota. (дата обращения: 14.04.2021).
2. Официальный сайт «Verdox» [Электронный ресурс] URL: https://verdox.ru/ (дата обращения: 14.04.2021).
3. Официальный сайт «DocSpace» [Электронный ресурс] URL: https://docspace.ru/ (дата обращения: 14.04.2021).
4. Официальный сайт «Tessa» [Электронный ресурс] URL: https://mytessa.ru/system/docs/ (дата обращения: 14.04.2021).
5. Официальный сайт «Контур.Диадок» [Электронный ресурс] URL: https://kontur.ru/diadoc?p=w03698 (дата обращения: 14.04.2021).
6. Статья «Обзор систем электронного документооборота» [Электронный ресурс] URL: https://www.cfin.ru/software/kis/edms.shtml/ (дата обращения: 14.04.2021).

УДК 681.518

ПРЕДЛОЖЕНИЯ ПО ЦИФРОВОЙ ТРАНСФОРМАЦИИ СУДОВ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ТИПА «ПОИСК» С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА CAE В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Клавднева Ольга Дмитриевна
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
e-mail: olechka_klavdneva@mail.ru

Аннотация. Показано, что при выборе программных средств класса CAE, позволяющих решать задачи инженерного анализа, важное значение имеет наличие сертификатов безопасности на соответствие требованиям по ТУ, СВТ, НСД, НДВ, ПДн. Для этого количественного оценивания весьма успешно может быть использован программный комплекс «АСОР», позволяющий оценить интегральный показатель качества с учетом требований по информационной безопасности. Этим требованиям в классе CAEдля обеспечения жизненного цикла судов специального назначения типа «Поиск» наилучшим образом соответствует программный комплекс «АРМ WinMachine». Показано, что его использование позволит на новом качественном уровне решать задачи формирования алгоритмов технологических процессов, снижения трудозатрат при проектировании, обеспечения требований по информационной безопасности.

Ключевые слова: ранжирование; цифровизация; обеспечение информационной безопасности; сертификация.

PROPOSALS FOR THE DIGITAL TRANSFORMATION OF SPECIAL-PURPOSE VESSELS OF THE "SEARCH" TYPE WITH THE USE OF SAE-CLASS INFORMATION TECHNOLOGIES IN A PROTECTED VERSION

Klavdneva Olga
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
e-mail: olechka_klavdneva@mail.ru

Abstract. It is shown that when choosing software tools of the CAE class that allow solving engineering analysis problems, it is important to have security certificates for compliance with the requirements for technical specifications, SVT, NSD, NDV, PDn. For this quantitative assessment, the software package "ASOR" can be used very successfully,

which allows evaluating the integral quality indicator taking into account the requirements for information security. The "APM WinMachine" software package best meets these requirements in the CAE class for ensuring the life cycle of special purpose vessels of the "Search" type. It is shown that its use will allow solving the problems of forming algorithms of technological processes at a new qualitative level, reducing labor costs during design, ensuring the requirements for information security.

Keywords: ranking; digitalization; information security; certificate.

Современные CAE-системы (англ. Computer-aidedengineering) представляют собой мощные средства инженерного анализа (расчётов, анализа и симуляции физических процессов) с развитым сервисным инструментарием, успешно применяющиеся для решения всех практических задач. В настоящее время на рынке представлено большое количество самых разнообразных расчетных пакетов с использованием широкого ряда математических методов, включая [1-3]:

– метод конечных элементов (МКЭ, конечно-элементный анализ) - численный метод решения дифференциальных уравнений с частными производными, а также интегральных уравнений, возникающих при решении задач прикладной физики;

– метод конечных разностей - численный метод решения дифференциальных уравнений, основанный на замене производных разностными схемами;

– метод конечных объемов (метод контрольных объемов) - численный метод интегрирования систем дифференциальных уравнений в частных производных.

Эти методы традиционно применяются для решения задач прочности, механики деформируемого твёрдого тела, теплообмена, гидродинамики и электродинамики, электромагнитных полей, тепла, механики жидкостей и газов, акустики, моделирования техпроцессов и других инженерных задач. В этой связи актуальным и практически востребованным на сегодняшний день является рассмотрение наиболее эффективного применения и развития CAE-программных комплексов (ПК) [4], причем, с учетом нейтрализации ряда информационных уязвимостей, включая ошибки пользователей, ошибки пользователей при сетевом взаимодействии, несанкционированное копирование инновационных системных и технологических решений и другие «незначительные факторы» обеспечения информационной безопасности (ОИБ).

Важнейшим средством ОИБ является наличие у ПК класса CAEсоответствующих сертификатов на соответствие ТУ, по контролю НСД, НДВ, обеспечению требований по СВТ, ПДн и др., что выполняется далеко не всегда и приводит к соответствующим рискам ОИБ.

В настоящее время существует настолько большой выбор среди ПК класса CAE, что сам выбор для ряда компаний превращается в значительную проблему, особенно, с учетом факта отсутствия у ряда конкурирующих ПК должной сертификации, тем более с учетом оценки опыта поставщиков информационной технологии.

Для решения данной проблемы в порядке цифровой трансформации судов специального назначения типа «Поиск»был использован ПК «АСОР 14.5» (разработка СПбГМТУ), который позволяет количественнооценитьинтегральный показатель качества с учетом названных выше аспектов ИБ [2].

Выполненные оценки показали, что наиболее предпочтительным споказателем конкурентной способности КС=1,5и с учетом данных сертификации следует считать ПК «АРМ WinMachine» [4].

Среди задач цифровой трансформации судов специального назначения типа «Поиск» на всех этапах их жизненного цикла названы:

– навыки квалиметрического сравнительного анализа характеристик ПК, реализующих ИТ класса CAE в защищенном исполнении;

– создание типовых интерактивных электронных технических руководств (ИЭТР) с целью ускоренного изучения и освоения практического использования ПК и его эффективной эксплуатации, включая нехарактерные для CAEаспекты ОИБ;

– проведение специальных учений по вопросам ОИБ при решении основных производственных задач с целью практического контроля действий персонала с выдачей соответствующих лицензий на право использования ПК класса CAEв защищенном исполнении.

Реализация данных предложений позволит минимизировать негативное влияние на процессы человеческого фактора, включая снижение угроз ОИБ, а также экономить временные и человеческие ресурсы, сократить неточности в планирование, использовать методы многовариантного проектирования и оптимизации для поиска эффективных вариантов и принятия проектных и управленческих решений.

СПИСОК ЛИТЕРАТУРЫ

1. Клавднева О.Д. Стартап-проект «Квалиметрическое ранжирование информационных технологий класса "CAE" в жизненном цикле объекта морской техники типа «Суда специального назначения типа «Поиск» / Санкт-Петербург, СПбГМТУ, ИТвЖЦ МТ, 2021 г.
2. Программный комплекс анализа, синтеза и оптимизации решений «АСОР 14.5» / Федеральная служба по интеллектуальной собственности, номер государственной регистрации 2013612649, 24.01.2013.
3. CAE-система http://sewiki.ru/CAE-система (Дата обращения: 26.04.2021).
4. Системы инженерного расчета и анализа деталей и сборочных единиц https://books.ifmo.ru/file/pdf/855.pdf (Дата обращения: 26.04.2021).

УДК 629.12

ОЦЕНКА ИНФОРМАЦИОННОЙ ЖИВУЧЕСТИ ТАКТИЧЕСКОЙ ГРУППЫ МРК: ПОСТАНОВКА ЗАДАЧИ ИССЛЕДОВАНИЙ

Корнева Юлия Васильевна
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
e-mail: tata.911843@gmail.com

Аннотация. Одним из ключевых критериев успешности ведения боя традиционно является способность корабля противостоять различным повреждениям, включая задачу обеспечения информационной живучести корабля. В этой связи рассмотрен актуальный вопрос постановки задачи аналитической оценки информационной живучести корабля в составе тактической группы, возможности автоматизации управления для дальнейшего мониторинга и прогнозирования тактической обстановки. Рассмотрены основные аспекты постановки задачи по разработке модели качественной и количественной оценки информационной живучести корабля применительно к тактической группе малых ракетных кораблей.

Ключевые слова: информационная живучесть; автоматизация управления; модель; постановка задачи; тактическая группа МРК.

ASSESSMENT OF INFORMATION SECURITY SURVIVABILITY OF THE TACTICAL GROUP OF SMALL MISSILE SHIPS: SETTING THE RESEARCH TASK

Korneva Yulia
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
e-mail: tata.911843@gmail.com

Abstract. One of the key criteria for the success of combat is traditionally the ability of the ship to resist various damage, including the task of ensuring the information survivability of the ship. In this regard, the topical issue of setting the task of assessing the information survivability of a ship as part of a tactical group, the possibility of automating control for further monitoring and forecasting the tactical situation is considered. The main aspects of the task of developing a model for the qualitative and quantitative assessment of the information survivability of a ship in relation to a tactical group of small missile ships are considered.

Keywords: information survivability; control automation; model; formulation of the problem; tactical group of the MRK.

Актуальность темы. В условиях стремительно развивающегося современного боя очень важен контроль и мониторинг обстановки, которые включают в себя информационную безопасность и живучесть, проявляющуюся в защищенности боевой информационно-управляющей системы (БИУС) от информационного вторжения, удаления данных, использования информации не по назначению, заражения вредоносными кодами и т.п. Поэтому встает вопрос о дальнейшем развитии такого направления как информационная безопасность (живучесть в информационной сфере) корабля, группы кораблей.

Предмет исследования. Термин "живучесть" введен адмиралом С.О. Макаровым: "Живучесть – это способность корабля вести бой, имея повреждения в различных боевых частях" (1894 г.) [Ошибка! Источник ссылки не найден.]. Элементами живучести корабля сегодня рассматриваются: непотопляемость, взрыво-пожаро-радиационная безопасность, безопасность службы экипажа, живучесть оружия и технических средств, управляемость (качество управления) системой борьбы за живучесть.

Термин информационная живучесть введен в практику в последнее время [2, 3] в связи с активным развитием и внедрением информационных технологий, обострившейся проблемой необходимости эффективной защиты информационных ресурсов (данных, информационно-коммуникационных средств, операторов) и отражает один из сегментов живучести корабля (ЖК) в информационной сфере.

Информационная живучесть корабля и их соединений (ИЖ) - совокупность организационно-технических мероприятий по обеспечению управления кораблем в условиях информационных вторжения противником в каналы управления. ИЖ включает в себя оценку, прогнозирование, мониторинг, анализ и принятие оптимальных решений в управлении кораблем в сложившейся обстановке [3].

Очевидно, что для обеспечения информационной живучести необходимо обеспечить постоянный мониторинг обстановки посредством автоматизированной информационной системы (АИС) корабля, а также устойчивость элементов АИС при их объединении в сложную систему. В свою очередь АИС корабля должна минимизировать вероятность ошибки личного состава и обеспечить наглядное представление обстановки.

Постановка задачи. В связи с этим можно выдвинуть ряд требований к системе моделирования процессов обеспечения в части ИЖ ТГ МРК:

Модель ИЖ ТГ МРК должна быть элементом и входить в модель оценки боевой устойчивости ТГ МРК в целом, включающей, по нашему мнению, в том числе модели оценки информационной устойчивости БИУС с учетом ее надежности, безопасности эксплуатации, способности реагирования на изменения обстановки

(адаптивности), модели адекватности действий экипажа, модели управления оружием и техническими средствами МРК в составе ТГ.

Модель ИЖ ТГ МРК должна обеспечивать визуализацию на средствах отображения БИУС процессов, наиболее важных и критичных для обеспечения ИЖ, т.е. обеспечивать наглядность представления данных.

Модель ИЖ ТГ МРК должна учитывать основные факторы обеспечения управления ТГ МРК (управляемость) – оперативность управления (включая пропускную способность каналов связи, быстродействие БИУС), достоверность используемых данных, устойчивость, скрытность непрерывность управления, ресурсную обеспеченность управления ТГ МРК (укомплектованность кадрами, оружием, техническими средствами, расходными материалами, финансами и т.п.).

Типовые требования к моделям объектов исследований, включая их адекватность, конечность, информативность, безизбыточность, функциональность, ресурсную доступность.

Полномасштабность процесса разработки модели ИЖ ТГ МРК, включая обязательные и традиционные этапы моделирования: определение целей; определение задач; определение системы критериев; ранжирование параметров; выбор модели; выбор метода исследования; проведение модельного эксперимента; анализ результатов; верификация модели; оценка ее валидности; апробация и эксплуатация; модернизация.

Предметом изучения и использования разработанной модели является процесс обеспечения информационной живучести (за счет информационной устойчивости БИУС) корабля в составе ТГ МРК и в целом – ИЖ ТГ МРК как способность системы «Корабль - ТГ кораблей» противостоять информационному вторжению в каналы управления ТГ МРК, восстанавливать свои свойства и ликвидировать последствия нарушения этой системы. Цель исследование - обеспечение информационной живучести (безопасности) корабля в составе тактической группы кораблей. В рамках поднятого вопроса поставлены следующие задачи:

1. Разработка вербальной и математической модели качественной и количественной оценки ИЖ корабля, включая факторы быстродействия системы (в части возможности функционирования БИУС в условиях воздействия DDos-атак), возможности управления системой в условиях вторжений различного рода, защищенности БИУС от ошибок персонала при управлении, надежности ПО, способность системы своевременно уведомлять о различного рода вторжениях или отклонениях от нормального функционирования.

2. Систематизация и развитие понятийного аппарата ИЖ, включая определения: понятие ИЖ ТГ МРК, информационной защищенности (ИЗ) МРК и ТГ МРК, информационного противодействия (ИПД), информационного противоборства (ИП), вторжения, атаки, операции, факторы ИЖ, уязвимость, угроза, модель нарушителей ИЖ, способы восстановления ИЖ.

3. Рассмотрение практических вопросов управления ИЖ МРК в составе ТГ МРК, включая:

Требования, вытекающие из определения и требований к устойчивости БИУС в условиях ИП

Уточнение предмета ИЖ, цель, задачи.

Анализ обеспечения этих требований сегодня.

Риски информационной безопасности (ИБ), ИЗ, ИП, ИЖ с учетом всего спектра возможных уязвимостей и угроз.

Необходимость модельного описания ИЖ.

Предлагаемые принципы и концепция решения проблемы ИЖ

Варианты и предлагаемые возможности количественной оценки ИЖ в соответствии с разработанной моделью ИЖ корабля в составе ТГ.

Пример количественной оценки применительно к МРК

4. Пути развития принципов и возможности количественной оценки и управления ИЖ корабля в составе ТГ (предложение положить их в основу мониторинга и контроля ИЖ при управлении ЖК).

Заключение. Понятие информационной живучести в настоящее время имеет особую актуальность в связи со стремительным ростом и развитием информационных технологий. Задача защиты информации, недопущения вторжения в каналы управления является одним из решающих факторов успешности операции. И в этой связи встает вопрос о разработке системы, отвечающей за информационную защиту, которая будет соответствовать современным требованиям.

Информационная живучесть корабля является частью живучести корабля, следовательно, очевидна необходимость обеспечения корабля надежной системой, способной дать наглядное представление об ИЖ, это поможет избежать ошибок в принятии тактических решений, а также даст возможность работать на опережение и иметь полный контроль над обстановкой.

СПИСОК ЛИТЕРАТУРЫ

1. MIL.PRESS FLOT / [Электронный ресурс] URL: https://flot.com/ (Дата обращения: 1.06.2021).
2. Алексеев А.В., Воробьев В.И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с. 153 - 159.
3. Алексеев А.В. Информационная живучесть судна: понятие, проблемы, технологии / Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 7 / СПОИСУ. – СПб., 2019, с. 345 – 348.

УДК 629.12

СЕМЬ АКТУАЛЬНЫХ ПРОБЛЕМ ОБЕСПЕЧЕНИЯ ИБ, ПУТИ И ДОРОЖНАЯ КАРТА ИХ РЕШЕНИЯ

Михальчук Андрей Васильевич[1], Давыдчик Виталий Владимирович[2], Алексеев Анатолий Владимирович[3]

[1] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
[2] ПАО «Информационные телекоммуникационные технологии «Интелтех»
Кантемировская ул., 8, Санкт-Петербург, 197342, Россия
[3] Институт автоматизации процессов борьбы за живучесть корабля, судна
Ленинский пр., 101, Санкт-Петербург, 198262, Россия
e-mails: mikhalchuk@oogis.ru, zavit@bk.ru, iapbgks@bk.ru

Аннотация. Выполнен системный анализ развития вопросов обеспечения информационной безопасности (ИБ) автоматизированных систем в защищенном исполнении (АСЗИ) различного назначения, включая объекты критической информационной инфраструктуры (ОКИИ). На основе положений теории синтетической квалиметрии выявлены 7 актуальных и наиболее значимых (критичных) проблем обеспечения ИБ АСЗИ. Показаны технологические пути и приведена дорожная карта их решения на основе концепции и технологий роботизированного управления, системной визуализации и мониторинга имитостойкости каналов управления и информационным противоборством в целом.

Ключевые слова: системный анализ; синтетическая квалиметрия; информационная живучесть; роботизированное управление; имитостойкость каналов управления; исследовательское проектирование.

SIEBEN AKTUELLE PROBLEME DER BEREITSTELLUNG VON IBS, WEGE UND EINE ROADMAP FÜR IHRE LÖSUNGEN

Mikhalchuk Andrey[1], Davydchik Vitaly[2], Alekseev Anatoly[3]

[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[2] JSC «INTELTECH»
8 Kantemirovskay St, St. Petersburg, 197342, Russia
[3] Institute of automation of processes of struggle for survivability of the ship, vessel
101 Leninsky Av, St. Petersburg 198262, Russia
e-mails: mikhalchuk@oogis.ru, zavit@bk.ru, iapbgks@bk.ru

Abstract. Die Systemanalyse der Entwicklung der Fragen der Versorgung der informativen Sicherheit (IB) der automatisierten Systeme in der sicheren Ausführung (ASZI) verschiedener Bestimmung, einschließlich der Objekte der kritischen Informationsinfrastruktur (OKII) erfüllt. Auf der Grundlage der Bestimmungen der Theorie der synthetischen Qualimetrie wurden 7 aktuelle und bedeutendste (kritische) Probleme bei der Bereitstellung von IB AZZIE identifiziert. Zeigt den technologischen Pfad und den Fahrplan finden Sie Ihre Entscheidungen auf der Grundlage der Konzepte und Technologien der automatischen Steuerung, der Visualisierungs-und Monitoring-имитостойкости Steuerkanäle Antagonismus und it im Allgemeinen.

Keywords: systemanalyse; synthetische qualimetrie; informative uberlebensfähigkeit; robotersteuerung; imitation der steuerkanäle; forschungsdesign.

Среди вопросов развития АСЗИ различного назначения, включая объекты морской техники и морской инфраструктуры (ОМТИ) и, особенно, ОКИИ, сегодня первостепенное значение приобрели вопросы обеспечения их информационной безопасности (ИБ). Именно они в условиях широкомасштабного внедрения информационных технологий и тренда цифровизации национальной экономики в целом имеют наибольшее влияние на технологическое, организационное и методологическое развитие и эффективное освоение АСЗИ [1].

Системный анализ данных вопросов на основе положений теории синтетической квалиметрии [2], включая оценку и анализ факторов корневой чувствительности интегрированных показателей качества АСЗИ [3] с использованием аппарата QSWOT-анализа и синтеза [4] позволил выявить 7 актуальных и наиболее значимых (критичных) проблем обеспечения ИБ АСЗИ объектов информатизации в составе:

1. Методологическая проблема качества управления ИБ в результате разрыва между масштабом требований к АСЗИ, технологической сложностью их реализации и возможностью эффективного управления ИБ на объектах информатизации типа ОМТИ и, особенно, ОКИИ в реальном масштабе времени.

2. Организационно-техническая проблема структурной, процессной и алгоритмической адаптации АСЗИ к постоянно изменяющейся инфраструктуре объектов информатизации.

3. Программно-аппаратная и методическая проблема критической потребности системного мониторинга ИБ и в целом информационным противоборством в реальном масштабе времени.

4. Ситуационная проблема потери контроля качества обеспечения ИБ в условиях масштабного перехода к технологиям удаленного доступа к критически значимым информационным ресурсам предприятий, организаций и компаний, определенной технологической их неготовности по обеспечению ИБ в этих условиях.

5. Неразрешимые «традиционные» проблемные вопросы обеспечения импортозамещаемости, конкурентной способности отечественных технологий, ограниченной результативности сертификации продукции и услуг в области ИБ, аттестации объектов и лицензирования деятельности.

6. Традиционные проблемы планирования бюджета на ИБ и его ресурсной отдачи (экономичности).

7. Проблема повышения квалификации специалистов ИБ, их переподготовки и сдерживания ротации.

В рамках дорожной карты (ДК) решения названных проблем среди основных мероприятий предложены:

– создание национального центра компетенций (НЦК) для координации научно-методологических решений и рекомендаций с ранжированием ожидаемой их результативности на основе технологии квалиметрии моделей и полимодельных комплексов [5, 6];

– дополнение системы сертификации соответствия сертификацией качества средств защиты информации (СЗИ) [7] с учетом, например, технологий ранговой партнерской сертификации [8];

– форсированное развитие средств роботизированного управления ИБ в классе IPS типа SIEM, PDM, SOAR, CRS, SGRC [9, 10] с выделением, полагаем, Министерством цифрового развития соответствующих инвестиций на внедрение лучших образцов по результатам сравнительных сертификационных испытаний;

– создание региональных полигонов открытого тестирования демонстрационного программного обеспечения АСЗИ [11] для практической отработки конкурентноспособных технологических решений [12];

– объявление гранта на создание унифицированного комплекса СЗИ, инвариантного к специфике решаемых типовых задач обработки информации в защищенном исполнении для формирования базы данных и знаний администраторов ИБ в интересах отработки лучших практик ситуационного управления ИБ [13, 14];

– разработка национального стандарта управления сложностью объектов информатизации с использованием моделей оценивания и контроля информационной и программно-аппаратной избыточности на основе, например, оценивания и контроля системных показателей качества объектов информатизации [15];

– создание национальной системы оценки публикационной активности специалистов в области ИБ с ранжированием качества публикаций по регламентированной системе критериев и показателей их качества [16]

Названные технологические пути и приведенная дорожная карта их решения позволят, по нашему мнению, на основе их публичного обсуждения и развития сконцентрировать усилия разработчиков и специалистов по практическому решению 7 наиболее значимых из актуальных проблем обеспечения ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В. Квалиметрическая концепция цифровизации управления инновационным и инвестиционным развитием предприятия / Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября 2020 г.: Материалы конференции. СПОИСУ. – СПб, 2020, с. 158-160.
2. Субетто А.И., Алексеев А.В. Теория практики квалиметрического обеспечения развития морских автоматизированных систем / Актуальные проблемы морской энергетики: материалы седьмой Всероссийской межотраслевой научно-технической конференции в рамках Второго Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2018, с. 78 – 86.
3. Алексеев А.В., Михальчук А.В. Перспективные направления развития технологии полимодельного квалиметрического анализа, синтеза и оптимизации организационных и технических решений / Перспективные направления развития отечественных информационных технологий: материалы VII межрегиональной научно-практической конф. Севастополь, 21-25 сентября 2021 г. / Севастопольский государственный университет; науч. ред. Б.В. Соколов. – Севастополь: СевГУ, 2021.
4. Алексеев А.В. Модифицированный SWOT-анализ и синтез алгоритмов информационной поддержки принятия проектных и управленческих решений / Региональная конференция (РИ-2012). Юбилейная XIII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2012)». Санкт-Петербург, 24-26.10.2012: Материалы конференции. \ СПОИСУ. – СПб, 2012, с. 27-28.
5. Микони С.В., Соколов Б.В., Юсупов Р.М. Квалиметрия моделей и полимодельных комплексов: монография. – М.: РАН, 2018. – 314 с.
6. Алексеев А.В. Примеры реализации полимодельного квалиметрического метода системной оптимизации объектов морской техники и морской инфраструктуры / Морские интеллектуальные технологии/Marine intellectual technologies, № 2 (52) том 3, 2021, с. 69-81.
7. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В. От декларации и сертификации соответствия к сертификации качества / Актуальные проблемы морской энергетики: материалы девятой международной научно-технической конференции в рамках Четвертого Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: СПбГМТУ, 2020, с. 363–369.
8. Алексеев А.В. Антипов В.В., Бобрович В.Ю., Смольников А.В. Ранговая партнерская сертификация качества: концепция, теория, практика // Региональная информатика и информационная безопасность. Сборник трудов. Вып. 1 / СПОИСУ. – СПб., 2015, с. 485-491.
9. Заведеев Ю.М., Куприянов Д.О., Алексеев А.В. Анализ технологий интеграции программных комплексов CRS и СПРУ в интересах роботизации управления информационной безопасностью // Актуальные проблемы морской энергетики: материалы десятой международной научно-технической конференции в рамках Пятого Всероссийского научно-технического форума «Корабельная энергетика: из прошлого в будущее». – СПб.: Изд-во СПбГМТУ, 2021, с. 363 – 369.
10. Алексеев А.В., Куприянов Д.О., Заведеев Ю.М., Гадаев Е.М., Стефанович И.Д. Квалиметрический SWOT-анализ программных комплексов роботизации управления информационными инцидентами / Информационная безопасность регионов России (ИБРР-2021). XII Санкт-Петербургская межрегиональная конференция: Материалы конференции / СПОИСУ. – СПб., 2021.
11. Алексеев А.В., Барабаш П.А., Жигадло В.Э., Зикратов И.А., Нырков А.П. Концепция Полигона сетевой межобъектовой отработки технологий управления и обеспечения превосходства в инфосфере / Информационная безопасность регионов России (ИБРР-2017). Юбилейная X Санкт-Петербургская межрегиональная конференция: Материалы конференции / СПОИСУ. – СПб., 2017, с. 304 – 306.
12. Александров В.Л., Алексеев А.В. Теория практики квалиметрического обеспечения конкурентной способности и перспективности развития объектов морской техники и морской инфраструктуры / Восьмая Всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика» (ИММОД-2017). 18-20 октября 2017 г. Труды конференции – СПб.: НОИМ, 2017, с. 74-80.
13. Бобрович В.Ю., Алексеев А.В., Антипов В.В., Смольников А.В., Бороненков И.М., Мусатенко Р.И. Автоматизация процессов борьбы за живучесть критических объектов: проблемы, лучшие практики, перспективы развития / Актуальные проблемы защиты и безопасности: Труды XXI Всероссийская научно-практической конференции РАРАН (3-6.04.2018). Изд. ФГБУ «РАРАН». Москва – 2018, с. 344 - 347.
14. Алексеев А.В. Модель инвариантной оценки качества и эффективности объектов морской техники / Морские интеллектуальные технологии/Marine intellectual technologies, № 2 том 2, 2020, с. 53-60.

15. Алексеев А.В. Системная избыточность как мера оптимальности технического решения / Материалы конференции «Информационные технологии в управлении» (ИТУ-2018). – СПб.: АО «Концерн «ЦНИИ «Электроприбор», 2018, с. 263- 268.
16. Алексеев А.В., Сус Г.Н., Ушакова Н.П. Системный анализ и ранжирование качества вариантов интеллектуальной поддержки принятия решений и управления борьбой за живучесть корабля, судна / Материалы 9-й конференции «Информационные технологии в управлении» (ИТУ-2016). - Спб., ГНЦ РФ АО «Концерн «ЦНИИ «Электроприбор», 2016, с. 786-790.

УДК 629.12.001.2

ПРЕДЛОЖЕНИЯ ПО ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЪЕКТА МОРСКОЙ ТЕХНИКИ НА ОСНОВЕ ТЕХНОЛОГИЙ КЛАССА CRM В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Никольский Иван Сергеевич
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
e-mail: vanya.nicolsky2015@yandex.ru

Аннотация. Рассматривается комплекс вопросов автоматизации и управления взаимоотношениями с клиентами при использовании систем CRM в защищенном исполнении. На основе сравнительного анализа наиболее предпочтительных по системному показателю качества программных комплексов в CRM-классе типа, Битрикс 24, Wire CRM, Мегаплан применительно к созданию и эксплуатации Тральщиков пр.12700, что их использование позволяет за счет автоматизации сложных технологических процедур и повышения уровня менеджмента качества предприятия сократить время, объем требуемых технологических процедур и средств, повысить производительность труда при условии нейтрализации уязвимостей и угроз информационной безопасности, обусловленных внутренними субъективными факторами типа некачественного организационного обеспечения обработки и защиты данных и ошибок обслуживания оборудования.

Ключевые слова: crm-системы; crm; успех; планирование; квалиметрическое ранжирование; acop; анализ; человеческий фактор; организационно-техническая защита информации.

OFFERS FOR DIGITAL TRANSFORMATION OF MARINE EQUIPMENT OBJECT BASED ON CRM TECHNOLOGIES IN A PROTECTED PERFORMANCE

Nicolsky Ivan
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
e-mail: vanya.nicolsky2015@yandex.ru

Abstract. A complex of issues of automation and customer relationship management when using CRM systems in a secure design is considered. Based on a comparative analysis of the most preferable in terms of the system quality indicator of software systems in the CRM-class such as Bitrix 24, Wire CRM, Megaplan in relation to the creation and operation of minesweepers pr.12700, which makes it possible by automating complex technological procedures and improving the level of quality management enterprises to reduce the time, the amount of required technological procedures and tools, to increase labor productivity, subject to neutralization of vulnerabilities and threats to information security caused by internal subjective factors such as poor organizational support for data processing and protection and equipment maintenance errors.

Keywords: crm systems; crm; success; planning; qualimetric ranking; acor; analysis; human factor; organizational and technical protection of information.

Развитие глобальных транспортных систем становится приоритетным видом деятельности в бизнесе и политике ведущих стран мира. Так, например, в РФ к числу таких систем отнесен водный транспорт, развитие которого обуславливает судостроение в качестве базовой отрасли при внедрении в нее наукоемких инновационных технологий и современной организации производства. Создана судостроительная корпорация, объединяющая ведущие судостроительные предприятия и проектные организации как центрального, так и регионального характера.

Развитие судостроения и его конкурентоспособность связаны с целым рядом факторов, снижающих себестоимость продукции. К их числу необходимо отнести такие, как сокращение затрат на проектирование и постройку судов, углубленную специализацию предприятий, уменьшение доли затрат рабочей силы за счет повышения производительности труда при одновременном обеспечении требуемого качества изделий.

Снижение затрат, вязанных с проектированием и постройкой судов, невозможно без комплексного использования информационных технологий.

Одной из таких технологий является система управления взаимоотношениями с заказчиками (CRM), она предназначена для улучшения обслуживания клиентов путём сохранения информации о клиентах и истории взаимоотношений с клиентами, установления и улучшения бизнес-процедур на основе сохранённой информации и последующей оценки их эффективности. Основные функции системы CRM вытекают из необходимости информационного сопровождения продажи, маркетинга и сервисного обслуживания.

Судостроительное предприятие имеет партнерские отношения с заказчиками (судовладельцами), и информация, получаемая от них, влияет на весь процесс производства. Судовладельцы участвуют в ряде

процессов на нескольких стадиях производства и иногда играют в них решающую роль. На стадии проектирования они участвуют в процессах составления технического задания, принятия основных параметров судна, выбора оборудования, а на стадии изготовления – в выборе способа и технологии изготовления и испытания. Кроме того, судовладельцы задают многие требования к постройке, техническому обслуживанию, ремонту и модернизации судна.

Из изложенного следует, что система CRM должна обеспечивать четкое и наглядное представление о выпускаемой продукции с использованием трехмерных изображений. Потребители и заказчики должны иметь возможность получать информацию о продукции и обмениваться ею с заинтересованными организациями. Кроме того, система CRM должна иметь базу данных о заказчиках и клиентах и своевременно реагировать на изменение условий и требований с их стороны.

Целью данной работы является выполнение квалиметрического ранжирования ИТ класса CRM, а также анализ возможности внедрения в ЖЦ Тральщиков пр.12700

Для достижения цели работы предусматривается решение следующих задач:

1. Освоение навыков квалиметрического анализа и выполнение сравнительного анализа свойств и характеристик программных средств реализации ИТ класса CRM с оценкой конкурентной способности и перспективности развития;

2. Освоение и отработка навыка поиска и использования научно-технической литературы;

3. Изучение основных положений и освоение методов практического использования современных ИТ.

В работе произведен сбор и изучение материалов индивидуального задания с составлением описательной части заданного класса ИТ, краткий обзор CRM был составлен на основе метода SWOT-анализа и АСППР «АСОР».

СПИСОК ЛИТЕРАТУРЫ

1. Чан Динь Тьен. Информационные технологии в судостроении/ Д. Т. Чан. А: Астраханский государственный технический университет, 2009 – 5с.
2. Конспект лекций по дисциплине: «Информационные технологии в жизненном цикле морской техники», проф. Алексеев А. В.
3. [Электронный ресурс] URL: https //studopedia.ru/18_54529_etapi-zhiznennogo-tsikla-promishlennih-izdeliy.html. (дата обращения: 17.03.2021).
4. [Электронный ресурс] URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-v-sudostroenii-suschestvuyuschie-sistemy-sfery-i-vozmozhnosti-ih-ispolzovaniya/viewer (дата обращения: 17.03.2021).
5. [Электронный ресурс] URL: https://www.hubspot.com/pricing/crm(Дата обращения: 12.04.2021).
6. [Электронный ресурс] URL: https://www.workbooks.com(Дата обращения: 12.04.2021).
7. [Электронный ресурс] URL:https://megaplan.ru/company/(Дата обращения: 17.04.2021).
8. [Электронный ресурс] URL: https://www.reallysimplesystems.com(Дата обращения: 18.04.2021).
9. [Электронный ресурс] URL: https://www.bitrix24.ru(Дата обращения: 25.04.2021).
10. [Электронный ресурс] URL: https://wirecrm.com(Дата обращения: 25.04.2021).
11. [Электронный ресурс] URL: https://www.freshworks.com/ru/freshsales-crm/ (Дата обращения: 25.04.2021).
12. [Электронный ресурс] URL: https://best-crm.ru/crm-system-chto-eto-kak-rabotaet/(Дата обращения: 25.04.2021).
13. [Электронный ресурс] URL: https://www.aberdeen.com/research/(Дата обращения: 25.04.2021).
14. [Электронный ресурс] URL: http://masters.donntu.org/2010/fimm/teriaiev/ind/index.htm(Дата обращения: 26.04.2021).
15. [Электронный ресурс] URL: https://www.cleverence.ru/articles/auto-busines/chto-takoe-bitriks-24-v-dvukh-slovakh-opisanie-vsekh-funktsiy-programmy-bitrix24-dlya-chego-nuzhna/(Дата обращения: 26.04.2021).
16. [Электронный ресурс] URL: http://edrj.ru/article/08-08-2018(Дата обращения: 26.04.2021).

УДК 629.12.001.2

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ, МОНИТОРИНГА И ЗАЩИЩЕННОГО УПРАВЛЕНИЯ ОБЕСПЕЧЕНИЕМ БЕЗОПАСНОЙ ЭКСПЛУАТАЦИИ КОРАБЛЕЙ ОХРАНЫ ВОДНОГО РАЙОНА

Прудниченко Петр Сергеевич, Алексеев Анатолий Владимирович
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
e-mail: prudnichenkopeter453@gmail.com

Аннотация. Рассматривается комплекс вопросов автоматизации и эффективного управления безопасностью эксплуатации технических средств, оружия корабля и соединения в целом при использовании автоматизированных систем поддержки принятия решений класса СПРУ в защищенном исполнении. Предлагаемые структурно-функциональная модель и свойства системы поддержки принятия решений и управления «СПРУ-БрК» применительно к бригаде кораблей охраны водного района позволяет информационно безопасно и системно целостно оценивать, прогнозировать, мониторить, анализировать, автоматически синтезировать и оптимизировать варианты управленческих решений и их реализации для выбора оператором. Это повышает качество информационно безопасного управления технической готовностью как корабля, так и соединения в целом, безошибочность и оперативность принятия решений при обеспечении безопасности эксплуатации, в аварийной ситуации, борьбе за живучесть корабля, включая информационную.

Ключевые слова: система поддержки принятия решений и управления; защита данных; командный пункт; квалиметрический анализ; жизненный цикл; корабли охраны водного района.

DECISION-MAKING SUPPORT, MONITORING AND SECURE MANAGEMENT SYSTEM FOR ENSURING THE SAFE OPERATION OF WATER AREA PROTECTION SHIPS

Prudnichenko Peter, Alekseev Anatoly
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
e-mail: prudnichenkopeter453@gmail.com

Abstract. The complex of issues of automation and effective safety management of the operation of technical means, weapons of the ship and the connection as a whole when using automated decision support systems of the SPRU class in a protected version is considered. The proposed structural and functional model and properties of the decision support and management system "SPRU-DbK" in relation to the crew of ships protecting the water area allows for information-safe and systemically holistic assessment, forecasting, monitoring, analyzing, automatically synthesizing and optimizing options for management decisions and their implementation for selection by the operator. This improves the quality of information-safe management of the technical readiness of both the ship and the connection as a whole, the accuracy and efficiency of decision-making when ensuring the safety of operation, in an emergency situation, the struggle for the survivability of the ship, including information.

Keywords: decision-making and management support system; data protection; command post; qualimetric analysis; life cycle; water area protection ships.

Современный корабль как сложная эргатическая (человеко-машинная) система в части условий эксплуатации требует непрерывного внимания и контроля состояния безопасности использования технических средств и оружия и, особенно, с учетом условий морской среды, тактической обстановки, сложности морской службы экипажа, возможности возникновения нештатных и форсмажорных обстоятельств, включая вопросы несанкционированного доступа, недекларированных возможностей и нарушения целостности данных [1-3].

Это налагает особые требования к системам автоматизированного управления техническими средствами и оружием кораблей, а также, и это имеет особое значение, их соединений в части систематизации данных, их анализа и выработки вариантов проектов управленческих решений, их оптимизации для соединения в целом.

При этом возникают такие специфические задачи, например, для бригады кораблей охраны водного района (БрКОВР), её флагманских специалистов как прогнозирование вариантов развития обстановки, информационно-аналитическая и интеллектуальная поддержка экипажей кораблей. Как при решении штатных, так и нештатных задач по обеспечению безопасной эксплуатации технических средств и оружия корабля (ОБЭ ТСО), по локализации аварийных ситуаций и аварий (ЛА), по борьбе за живучесть корабля (БЖК).

Для решения этих задач необходимо совершенствование и разработка новых принципов, способов, алгоритмов, каналов дистанционного мониторинга и автоматического контроля системных и технических характеристик корабля, каналов взаимодействия с корабельными специалистами с целью контроля регламентов эксплуатации ТСО, обеспечения и поддержания их проектного качества, минимизации возможности возникновения нештатных/чрезвычайных ситуаций по непотопляемости (Н), взрывопожаро-радиационной безопасности (ВПРБ), живучести ТСО (Жтсо), безопасности службы экипажа (БС) и управляемости ТСО (У).

Предложена архитектура, функциональные свойства и вербальная модель Системы поддержки принятия решений и управления «СПРУ-БрК», позволяющая флагманским специалистам БрКОВР системно целостно оценивать, прогнозировать, мониторить обстановку по ОБЭ-ЛА-БЖК, анализировать, автоматически синтезировать и оптимизировать варианты решений и их реализации. Это повышает качество управления технической готовностью кораблей соединения в целом, а также безошибочность и оперативность (своевременность) принятия решений в возможных аварийных ситуациях, борьбе за живучесть кораблей.

В основу концепции и модели функционирования СПРУ-БрК положены свойства инвариантности и масштабируемости ранее разработанной в СПбГМТУ совместно с АО «Концерн «НПО «Аврора» технологии «СПРУ ЛА-ГО.о3» [3-5], а также принцип создания единого информационного пространства и возможность создания и использования малоизбыточных каналов структурно скрытной информации между кораблями БрКОВР. Это предлагается обеспечить за счет передачи не текущих данных каналов контроля состояния корабельных помещений и боевых постов корабля, обнаружения аварийных ситуаций по Н, ВПРБ, Жтсо, БС, У, а их групповых и агрегированных показателей качества, обеспечивая тем самым их системное шифрование и информационную защиту [6]. Среди других инновационных предложений – модификация интерфейса, математического и программного обеспечения обработки данных по оценке состояния каждого корабля и технология формирования и выдачи рекомендаций командирам корабля и боевых частей по ОБЭ, ЛА, БЖК.

Предлагаемая модель и переход от СПРУ отдельного КОВР к системе автоматизированного управления «СПРУ-БрК» позволяет одновременно, по нашему мнению, как контролировать и управлять состоянием ТСО отдельных кораблей, так и накапливать, систематизировать и унифицировать опыт по ОБЭ-ЛА-БЖК в составе соединения, обосновывать перспективные пути развития, что также имеет существенное значение [1-6].

Базовым вариантом реализации данных предложений может быть принята при минимальных инвестиционных вложениях модернизация алгоритмов функционирования корабельных автоматизированных систем типа 83Т170-Э, «Сигма-Э», АСБУ «Лесоруб-Э», ИМС и других в защищенном исполнении [7].

Для технологической отработки предлагаемой модели и технологии СПРУ по ОБЭ ТСО, ЛА и БЖК, по нашему мнению, целесообразно выполнение исследовательских и проектных работ в современной форме

стартапа (сокращенный вариант НИОКР) применительно к условиям, например, бригады кораблей охраны водного района «СПРУ-БрК», что позволит создать необходимые и достаточные условия реализации.

При этом, на первом этапе этих исследований и работ целесообразно выполнить (ближайшие задачи):

- Систематизацию данных и анализ требований по ОБЭ ТСО КО КОВР в составе БрКОВР.
- Квалиметрический анализ и ранжирование современных средств и технологий класса АСППР.
- Разработку модели и архитектуры СПРУ по ОБЭ ТСО КОВР (СПРУ-К) в составе СПРУ-БрК.
- Адаптацию и отработку технологии СПРУ к задаче СПРУ-К и СПРУ-БрК.
- Обоснование предложений по внедрению и развитию предлагаемой технологии СПРУ-БрК.
- Для реализации этих задач целесообразно использовать в качестве научно-технического задела и учесть опыт многочисленных инновационных предложений и разработок, включая [8-13].

В качестве аналогов и прототипа (ближайшего аналога) целесообразно использовать технологическое и технические решения из [4-5, 15], а в качестве базового критерия исследовательского проектирования и оптимизации структуры и характеристик СПРУ-БрК - критерий «Конкурентная способность (военно-техническое превосходство) АСППР «СПРУ-БрК» при информационно защищенном решении комплекса задач ОБЭ ТСО, ЛА, БЖК». При этом, индексы критериальной значимости решаемых задач, показателей качества с учетом данных по сертификации средств по требованиям ИБ и эффективности КОВР и БрКОВР (модели предпочтений) должны задаваться в трех вариантах для условий: 1.ЛенВМБ. 2.СевВМБ. 3.Адаптивный.

Представленный вариант постановки задачи на выполнение стартапа может уточняться в ходе работ.

СПИСОК ЛИТЕРАТУРЫ

1. Алексеев А.В., Фролов А.А. Концептуальное обеспечение развития технологий и управления информационной безопасностью крупных автоматизированных информационных систем /Сб. докл. IV Всероссийской конференции «Обеспечение информационной безопасности. Региональные аспекты. 2005», 13-17.09.2005, Сочи. – М.: Академия информационных систем, 2005, с. 88 - 91.
2. Алексеев А.В. Оптимизация проектных и управленческих решений при комплексном обеспечении безопасности большого города // Безопасность большого города / Сб. ст. под ред. Э.И. Слепяна. – С.-Петербург: Издательство Сергея Ходова, 2007, с. 400-418.
3. Отчет о ОКР «Поддержка-У» (Х-478/11200/4318-2012) «Разработка технологии создания систем информационной поддержки судоводителей по обеспечению безопасной эксплуатации систем (погрузки, выгрузки танков, системы вентиляции и т.п.) в нормальных условиях и при аварийных ситуациях» - СПбГМТУ, 2014. № ДЛМК 421452.034 ПЗ, инв. № 012221.
4. Алексеев А.В., Смольников А.В., Сус Г.Н., Ушакова Н.П. Когнитивные технологии системы поддержки принятия решений и управления борьбой за живучесть корабля, судна //Системы управления и обработки информации: научн.-техн. сб. /АО «Концерн «НПО «Аврора». СПб, 2019. Вып. 3(46), с. 18-27.
5. Алексеев А.В., Смольников А.В., Ушакова Н.П., Сус Г.Н. Программный комплекс Макетного действующего образца Системы информационной поддержки судоводителей при обеспечении безопасности эксплуатации в части грузовых операций, локализации аварийных ситуаций, аварий и борьбы за живучесть морских объектов повышенного риска (ПК МДО СИП ЛА-ГО о3) – Свидетельство о государственной регистрации программ для ЭВМ (Реестр программ ФСИС) № 2014614620, 29.04.2014.
6. Алексеев А.В., Воробьев В.И. Информационное противоборство: 20 лет концептуального и технологического развития // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 1 / СПОИСУ. – СПб., 2015, с. 153 - 159.
7. Морская радиоэлектроника. Справочник /И.В.Соловьев, Г.Н.Корольков, А.А.Бараненко, М.Н.Баранов, А.В.Алексеев, Л.С.Васильев, В.Г.Дзюба, И.Г.Корж, М.Б.Солодовниченко, Б.М.Усвяцов /Под ред. В.А. Кравченко. - СПб.: Политехника, 2003. - 246 с.
8. Клименок А.А. Разработка системы информационной поддержки принятия решений вахтенным механиком танкера при обеспечении безопасности эксплуатации специальных судовых систем в процессе проведения грузовых операций. - СПбГМТУ, ВКР, 2014. – 88 с.
9. Соколовский П.С. Система информационной поддержки принятия решений и управления командира электромеханической боевой части подводной лодки. - СПбГМТУ, ВКР, 2015. – 87 с.
10. Еникеев А.И. Система информационной поддержки принятия решений и управления командира электромеханической боевой части МРК проекта 22800. – СПбГМТУ, ВКР, 2019. – 59 с.
11. Пантелейкин С.В. Методы и технологии мониторинга и управления локализацией аварийных ситуаций танкеров ледового класса. – СПбГМТУ, ВКР, 2018. – 90 с.
12. Солуянов В.А. Распределенный ситуационный центр борьбы за живучесть корабля, судна. – СПбГМТУ, ВКР, 2019. – 68 с.
13. Селиверстов С.Л. Автоматизированная система поддержки принятия решений и управления Берегового центра экстренного реагирования. – СПбГМТУ, ВКР, 2019. – 76 с.
14. Майский Ю. Программный модуль автоматизированного контроля и мониторинга качества управления «СПРУ-К». . – СПбГМТУ, ВКР, 2020. – 59 с.
15. Алексеев А.В. Модель инвариантной оценки качества и эффективности объектов морской техники / Морские интеллектуальные технологии/Marine intellectual technologies, № 2 том 2, 2020, с. 53-60.

УДК 629.59

ОЦЕНКА БЕЗОПАСНОСТИ ПОВРЕЖДЕННОЙ ПОДВОДНОЙ ЛОДКИ ПО ПЛАВУЧЕСТИ И СТАТИЧЕСКОЙ ОСТОЙЧИВОСТИ

Трошин Антон Николаевич, Москаленко Василий Александрович,
Поминов Сергей Геннадьевич, Поляков Сергей Алексеевич
Военный учебно-научный центр Военно-Морского флота «Военно-Морская академия им. Н.Г. Кузнецова»
Ушаковская наб., 17, Санкт-Петербург, 197045, Россия
e-mail: 424756b@mail.ru

Аннотация. Выполнен анализ влияния показателей продольной остойчивости на безопасность подводной лодки при контроле плавучести в автоматизированной системе борьбы за живучесть в защищенном исполнении и показаны пути ее обеспечения в различных условиях плавания.

Ключевые слова: подводная лодка; комплексная безопасность; защита данных; остойчивость; затопление; аварийная ситуация.

ASSESSMENT OF THE SAFETY OF A DAMAGED SUBMARINE IN TERMS OF BUOYANCY AND STATIC STABILITY

Troshin Anton, Moskalenko Vasiliy, Pominov Sergey, Polyakov Sergey
Military training and research center of the Navy «Naval Academy named after N. G. Kuznetsov»
17 Ushakovskaya Emb, St. Petersburg, 197045, Russia
e-mail: 424756b@mail.ru

Abstract. The analysis of the influence of longitudinal stability indicators on the safety of a submarine under buoyancy control in an automated survivability control system in a protected design is performed and the ways of ensuring it in various navigation conditions are shown.

Keywords: submarine; integrated security; data protection; stability; flooding; emergency.

Развитие теории о надводной непотопляемости подводных лодок (ПЛ) является одним из наиболее убедительных подтверждений тезиса А. Н. Крылова о том, что "...Вопросы теории корабля ставились практикою, обыкновенно какою-нибудь крупною катастрофою с кораблем, на котором не были соблюдены принципы теории..."

Действительно, после гибели в марте 1970 г. ПЛ "К-8" особое внимание было обращено на продольную остойчивость поврежденной ПЛ и оценке с этих позиций опасности ее состояния. Главным был вопрос об установлении критического состояния ПЛ и путях отдаления от него. Затопление при этом в исследованиях принималось стационарным процессом. На следующую, более высокую ступень внимание к надводной непотопляемости ПЛ подняла гибель в апреле 1989 г. ПЛ К-278 "Комсомолец". При этом впервые всерьез был поставлен вопрос об анализе развития аварии, оценке "времени жизни" поврежденной ПЛ и путях его увеличения. Главным был вопрос об оценке момента, когда экипажу следовало покинуть аварийную ПЛ в процессе продолжающегося поступления воды [1].

Как показал опыт, выводы и рекомендации, полученные в ходе исследований, не всегда совпадают, что вполне естественно в связи с различием рассматриваемых условий о стационарности развивающегося затопления. В качестве "рабочего инструмента" при подобных исследованиях для простоты и наглядности используется диаграмма надводной непотопляемости (ДНН) ПЛ [2].

Развивая идею Ю. К. Прыткова, используем нанесенные на ДНН вспомогательные кривые:

– внешние ограничительные по продольной остойчивости $Vx_c(V, \psi = \psi_m)$, отвечающие углам максимума ψ_m продольных диаграмм статической остойчивости (ДСО) $l_\psi(\psi, V = const)$ и их максимальным ординатам l_m, характеризующим запас остойчивости;

– аналогичные внутренние ограничительные кривые, эквидистантные внешним и смещенные внутрь ДНН на величину $l_д V_н$, где

$l_д$ - минимально допустимое плечо продольной остойчивости ПЛ, принятое согласно положению Ю. К. Прыткова равным 0,5 м, а $V_н$ – объемное водоизмещение неповрежденной ПЛ при нормальной нагрузке. Учитывая возможные погрешности при неполноте информации о затоплении и неточности данных о посадке ПЛ, представляется целесообразным увеличить $l_Д$ до 1,0 м.

Для ПЛ с бескингстонными цистернами главного балласта (БЦГБ) кривые $Vx_c(V, \psi = \psi_m)$ принципиально точно определяются внешними огибающими кривых равных дифферентов $\psi = const$ ДНН. Если все ЦГБ кингстонные, за эти кривые принимают (с ошибкой в безопасную сторону) крайние внешние кривые равных дифферентов (обычно при $\psi = 10° - 20°$).

По аналогии используем ограничительные кривые по запасу плавучести. Для ПЛ с БЦГБ внешняя из этих кривых проводилась в районе обрыва вверху кривых равных дифферентов (при потере ПЛ вертикальной устойчивости), а при наличии только кингстонных ЦГБ - через верхнюю точку ДНН. Внутренние ограничительные кривые были опущены ниже на величину минимально допустимого запаса плавучести $\omega_д$. Предлагалось принимать $\omega_д = 0{,}2\omega_н$, где $\omega_н$ - запас плавучести неповрежденной ПЛ при нормальной нагрузке. Построение последних двух ограничительных кривых теряет смысл, если область малых запасов плавучести "перекрывается" ограничительными кривыми по продольной остойчивости [3].

В качестве внутренних ограничительных кривых по продольной остойчивости в дальнейшем другими авторами было предложено использовать кривые, отвечающие углам дифферента $\psi_{ПН}, \psi_{ПК}$, при которых входят в воду верхние кромки непроницаемых оконечностей ПЛ.

Принятые в качестве критерия безопасности углы $\psi_П$, имея под собой определенное физическое основание (замедление роста остойчивости формы в связи с последующим уменьшением центральных моментов инерции площади ватерлинии), мотивировалось, главным образом, относительной легкостью определения этого угла по входу в воду шпигатов надстройки в районах оконечностей непроницаемого корпуса (при носовых и кормовых марках осадок). Поскольку этому критерию может отвечать большой запас продольной остойчивости, Г. В. Лушин рекомендовал использовать его лишь в качестве "сигнала" к началу продольного спрямления.

Проведенные исследования и полученные результаты показали возможность и пути обеспечения в различных условиях плавания безопасности подводной лодки при контроле плавучести в автоматизированной системе борьбы за живучесть в защищенном исполнении с учетом временных факторов.

СПИСОК ЛИТЕРАТУРЫ

1. Абрамов Л.А. и др.: Методы расчета живучести КЭС на базе логико-дефференциальной модели развития аварии при коротком замыкание. С-Пб: ВМА, 1993.
2. Васюнькин В.В. Живучесть надводных кораблей. Учебное пособие. С-Пб: ВМА, 1992.
3. Арцыкова Л.А., Парфенов Ю.М., Соколов В.С. Оценка живучести технических систем на ранних этапах проектирования. Алгоритм № 249. В кн.: Сборник алгоритмов и программ, выпуск №11. Л.: ВМА, 1987, с.53-70.

УДК 372.853

ПРИМЕНЕНИЕ АЛГОРИТМИЧЕСКИХ И ИНСТРУМЕНТАЛЬНЫХ СРЕДСТВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ МОДЕРНИЗАЦИИ ОЧНО-ДИСТАНЦИОННОГО ФОРМАТА ОБУЧЕНИЯ НА ОСНОВЕ ДАННЫХ LMS

Шавинская Сания Караматовна
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
e-mail: sankar52@mail.ru

Аннотация. Основная цель работы - выполнить аналитический обзор инструментов Big Data для реализации полного цикла анализа данных, включающий преобразование и фильтрацию, собственно анализ, визуализацию и экспорт, моделирование и прогнозирование, а также выбрать инструмент для анализа возможности реализации очно-дистанционного формата обучения на корпоративной платформе ИСУ СПбГМТУ, используя учебную аналитику данных, основанную на анализе цифрового следа.

Ключевые слова: большие данные; цифровой след; анализ больших данных; алгоритмы машинного обучения; искусственный интеллект; моделирование; платформа обучения; очно-дистанционный формат; Knime.

APPLICATION OF ALGORITHMIC AND MACHINE LEARNING TOOLS FOR MODERNIZING THE FACE-TO-FACE-DISTANCE LEARNING FORMAT BASED ON LMS DATA (ANALYTICAL REVIEW)

Shavinskaya Sanya
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
e-mail: sankar52@mail.ru

Abstract. The main goal of the work is to perform an analytical review of tools for implementing a full cycle of data analysis, including transformation and filtering, analysis itself, visualization and export, modeling and forecasting, as well as to choose a tool for analyzing the possibility of implementing a full-time-distance learning format on the corporate platform of the ISU SPbGMTU, using educational data analytics based on digital footprint analysis.

Keywords: big data; digital footprint; big data analysis; machine learning algorithms; artificial intelligence; modeling; learning platform; full-time and distance learning; Knime analitic platform.

В современном мире, особенно в период пандемии, студент почти не привязан ни к преподавателю, ни к своей среде обитания. Современные цифровые технологии предоставляют возможность выбора среды развития, а в дальнейшем, выбор деятельности. Успех зависит от умения быстро адаптироваться к новым, постоянно изменяющимся условиям и эффективно осваивать новую деятельность, и приобретать новые профессиональные качества. Это предъявляет новые, принципиально другие требования к системе образования. Система должна обеспечить как качественно высокий уровень каждого конкретного преподавателя, обучающего конкретной дисциплине, а также обеспечить студента:

– различными образовательными инструментами для осознанного выбора,

– технологиями навигации в пространстве образовательных возможностей (с учетом их релевантности целям, личным качествам, способностям обучающегося),

– надежными средствами оценки эффективности того или иного образовательного процесса.

«Цифровые изменения» отчасти происходят сами по себе за счет появления десятков глобальных образовательных платформ. А отчасти нуждаются в согласованных действиях крупных, в том числе государственных, образовательных субъектов, способных вместе решить базовую задачу, открывающую дверь этому «цифровому переходу»: создать эффективные методы цифровой фиксации и интерпретации фактов в образовании, а также систему хранения, доступа и обмена этими данными между всеми участниками рынка.

Речь идет о таких инструментах, как рекомендательные системы по персональным траекториям развития, системы мониторинга эффективности образовательных процессов, системы цифровых профилей обучающихся. Мы должны научиться помогать студентам строить свои траектории развития, мы должны научиться отражать в данных все значимые элементы этих траекторий, фиксировать цифровой след развития человека.

Благодаря большим данным могут быть созданы системы, которые помогают человеку принять правильное решение о ближайшем шаге развития. Большие данные сопоставляют эффективность тех или иных

образовательных методов для конкретного роста. Big Data — это множество подходов, инструментов и методов, используемых для обработки структурированных и неструктурированных данных огромных объемов и значительного разнообразия для получения результатов, воспринимаемых людьми. Актуальность использования технологии Big Data достаточно велика, так как в данный момент она является одним из ключевых драйверов развития информационных технологий. Big Data помогают обработать опыт тысяч преподавателей и студентов, на основе анализа получить эффективную методику. Помимо повышения качества и эффективности создаваемых методик, большие данные помогают персонализировать контент под потребности каждого обучающегося.

В образовательной практике нашего ВУЗа мы проанализировали цифровой след, собранный в результате обучения студентов в период пандемии в ИСУ, все преподаватели работали в режиме онлайн, проводили лекции и практические занятия в формате вебинара, запись лекций затем размещалась на странице курса. Для анализа был выбрана платформа Knime Analytics:

– Knime Analytics Platform позволяет реализовывать полный цикл анализа данных, включающий чтение данных из различных источников, преобразование и фильтрацию, собственно анализ, визуализацию и экспорт;

– в образовательной среде анализ данных позволяет работать с индивидуальными программами обучающихся, персонализировать обучение. Обучение становится адаптивным и личностноориентированным;

– образовательная аналитика на основе больших данных меняет представление о формате образовательных программ и дает возможность студенту успешно двигаться по своей индивидуальной траектории обучения, изменяет подход к мониторингу и оценке, как самого образовательного процесса, так и образовательных результатов;

– BigData аналитика больших данных помогает лучше понять способности и возможности студентов.

СПИСОК ЛИТЕРАТУРЫ

1. http://www.edutainme.ru/post/learning-analytics/
2. https://cyberleninka.ru/article/n/onlayn-obrazovanie-klyuchevye-trendy-i-prepyatstviya3. https://www.sciencedaily.com/releases/2020/02/200205132409.htm
3. https://xmldatafeed.com/top-30-instrumentov-big-data-big-data-dlja-analiza-dannyh-kak-analizirovat-dannye/
4. https://www.uplab.ru/blog/big-data-technologies/
5. Технологии Big Data вскоре изменят высшее образование. [Электронный ресурс] – Режим доступа: https://mel.fm/novosti/7249138-bigdata (дата обращения: 25.05.19).
6. Утёмов В. В., Горев П. М. Развитие образовательных систем на основе технологии Big Data // Научно-методический электронный журнал. «Концепт». – 2018. – № 6 (июнь). – С. 449–461. – URL: http://e-koncept.ru/2018/181039.htm.

УДК 629.12.001.2

ПРЕДЛОЖЕНИЯ ПО ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЪЕКТА МОРСКОЙ ТЕХНИКИ НА ОСНОВЕ ТЕХНОЛОГИЙ КЛАССА CNC В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Шавловский Гордей Витальевич
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
e-mail: shavlovskiy2012@mail.ru

Аннотация. Рассматривается комплекс вопросов автоматизации и эффективного управления производством при использовании средств числового программного управления технологическими процессами (ComputerNumericalControl) в защищенном исполнении. На основе сравнительного анализа наиболее предпочтительных по системному показателю качества программных комплексов в CNC-классе типа «FANUC 30i», SINUMERIK 840D, Heidenhain itnc TNC 640 применительно к созданию и эксплуатации судового трансформатора показано, что их использование позволяет за счет автоматизации сложных технологических процедур и повышения уровня менеджмента качества предприятия сократить время, объем требуемых технологических процедур и средств, повысить производительность труда более чем в 3 раза, но при условии нейтрализации уязвимостей и угроз информационной безопасности, обусловленных внутренними субъективными факторами типа некачественного организационного обеспечения обработки и защиты данных и ошибок обслуживания оборудования.

Ключевые слова: CNC-системы; планирование; квалиметрическое ранжирование; технология АСОР-поддержки принятия решений; человеческий фактор; организационно-техническая защита информации.

PROPOSALS FOR THE DIGITAL TRANSFORMATION OF A MARINE ENGINEERING FACILITY BASED ON CNC CLASS TECHNOLOGIES IN A PROTECTED DESIGN

Shavlovskiy Gordey
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
e-mail: shavlovskiy2012@mail.ru

Abstract. The complex of issues of automation and effective production management when using the means of numerical software control of technological processes (ComputerNumericalControl) in a secure version is considered. Based on a comparative analysis of the most preferred software systems in the CNC class such as "FANUC 30i",

SINUMERIK 840D, Heidenhain itnc TNC 640 in relation to the creation and operation of a marine transformer, it is shown that their use allows, by automating complex technological procedures and improving the quality management level of the enterprise, to reduce the time, the amount of required technological procedures and tools, to increase labor productivity by more than 3 times, but provided that vulnerabilities and threats to information security are neutralized, due to internal subjective factors, such as poor organizational support for data processing and protection, and errors in equipment maintenance.

Keywords: CNC systems; planning; qualimetric ranking; technology of ASSOR-decision support; human factor; organizational and technical protection of information.

Числовое программное управление по CNC-технологиям активно применяется в современном оборудовании для обработки металлических, пластмассовых, деревянных и других изделий. Устройства с числовым программным управлением позволяют автоматизировать практически все функции и реализовать все возможности современного станочного оборудования.

Кроме всевозможных обрабатывающих инструментов дополнение станка пультом или консолью для ввода и изменения программного обеспечения в сочетании с дисплеем позволяет контролировать все технологические процессы изготовления практически любых по сложности деталей и устройств современного судового оборудования. Это обеспечивает качественно новый уровень выполнения технологических процедур наряду со значительным снижением негативного влияния человеческого фактора, соблюдением требований техники безопасности, повышением их точности, экономичности, уменьшением доли бракованной продукции.

Вместе с тем, для эффективного внедрения информационных технологий CNC-класса требуют своего внеочередного и одновременного решения задачи:

– обоснованного выбора по системному (интегральному, агрегированному) критерию и показателю качества соответствующего программного комплекса класса CNC, удовлетворяющего комплексу требований предприятия, его технологическому циклу и требованиям системы менеджмента качества;

– выявления, систематизации и своевременного освоения лучших практик внедрения новых технологических решений и программных комплексов их реализации;

– качественного обеспечения мероприятий по организации и технологии комплексной защиты информации как нового направления производственного обеспечения и следствия перехода на использование информационных технологий, спецификой которых является появление новых объективных и субъективных внутренних и внешних факторов, воздействующих на обрабатываемую информацию (ГОСТ Р 51275-2000, ГОСТ Р 50922-96).

Эту сложную системную, исследовательскую, комплексную задачу с принятием соответствующих организационных и технических решений предложено решать на основе современных средств информационно-аналитической и интеллектуальной поддержки принятия управленческих решений типа «АСОР 14.5» [1, 2], что позволит количественно оценивать, анализировать, синтезировать и оптимизировать принимаемые решения.

На основе сравнительного анализа с использованием программного комплекса (ПК) «АСОР 14.5» по интегральному показателю качества более 7 программных комплексов в CNC-классе типа «FANUC 30i», SINUMERIK 840D, Heidenhain itnc TNC 640 применительно к созданию судового трансформатора показано, что наиболее предпочтительным с показателем конкурентной способности порядка 1,7 следует считать ПК «FANUC 30i» (Осино, Минамицуру, Яманаси, Япония) [3]. Его преимуществами, как показали результаты квалиметрического QSWOT-анализа [4-8], следует считать:

– инвариантное решение CNC-задачи для широкого класса многофункциональных станков;

– большое количество рабочих осей для многоканальной, высокоточной и высокоскоростной обработки материалов;

– наличие инновационного программного обеспечения в защищенном исполнении;

– аппаратная часть обеспечивает высокую производительность, надежность, скорость, точность и качество обрабатываемых деталей;

– встроенный функционал расширенного профилактического обслуживания;

– практически неограниченные возможности модернизации и развития.

Вместе с тем, выполненный QSWOT-анализ среди слабых внутренних сторон ПК «FANUC 30i» наряду с высокой стоимостью закупки, обслуживания и поддержки (стоимости владения) отметил высокую сложность управления и необходимость высокой квалификации операторов по традиционно высоким японским «меркам».

Это накладывает особо жесткие требования к качеству организации в отечественных условиях технологий использования предлагаемого CNC-решения, процессов автоматизации сложных технологических процедур и повышения уровня менеджмента качества предприятия в целом.

В связи с резким возрастанием сложности управления и требований к обслуживающему персоналу для получения прогнозируемых результатов ресурсной отдачи (экономичности по критериям сокращения времени, объема требуемых технологических процедур и средств, повышения производительности труда более чем в 3 раза и других) принципиально необходимо также обеспечить условия нейтрализации уязвимостей и угроз, обусловленных внутренними субъективными факторами типа некачественного организационного обеспечения обработки информации (защиты данных), ошибок персонала по обслуживанию оборудования.

Для достижения данной цели применительно к решению задачи повышения проектного качества при создании объекта морской техники типа «Судовой трансформатор» и его эффективной эксплуатации предлагается решить следующие задачи цифровой трансформации на основе CNC-технологий:

1. Освоение навыков квалиметрического сравнительного анализа свойств и характеристик программных средств реализации ИТ класса CNC в интересах оценки и повышения конкурентной способности и перспективности развития создаваемой продукции и предоставляемых услуг в защищенном исполнении с учетом возможностей и регламентов разграничения доступа.

2. Поиск, выявление и квалиметрическое ранжирование с использованием научно-технической литературы и современных информационных ресурсов (Интернет, электронные библиотеки, информационно-поисковые сервисы) лучших информационных технологий, программных комплексов их реализации и практик освоения с формированием и актуализаций соответствующих баз данных и знаний в защищенном исполнении (БДЗ) по критериям достоверности (ценности) данных. их конфиденциальности, доступности, целостности.

3. Создание типовых интерактивных электронных технических руководств (по технологии IETM) и тренажерных комплексов по автоматическому контролю знаний-умений-навыков (ТКК) использования современных высоко технологических программных модулей (средств) и аппаратно-программных комплексов с целью ускоренного изучения и качественного освоения методов практического использования, технологий эффективной эксплуатации современных программно-аппаратных комплексов в защищенном исполнении.

Реализация данных предложений (квалиметрического ранжирования средств, актуализации их БДЗ, а также создания ТКК), по нашему мнению, позволит оптимизировать процессы системного освоения высокотехнологических инновационных решений, их безопасной эксплуатации, реализации инновационных возможностей и инвестиционных ожиданий с существенным снижением угроз негативного влияния субъективных свойств операторов, повышения их компетенций и квалификационного уровня.

СПИСОК ЛИТЕРАТУРЫ

1. Шавловский Г.В. Стартап-проект «Квалиметрическое ранжирование информационных технологий класса "CNC" в жизненном цикле объекта морской техники типа «Судовой трансформатор» / Санкт-Петербург, СПбГМТУ, ИТвЖЦ МТ, 2021 г.
2. Программный комплекс анализа, синтеза и оптимизации решений «АСОР 14.5» / Федеральная служба по интеллектуальной собственности, номер государственной регистрации 2013612649, 24.01.2013.
3. Официальный сайт производителя ПК «FANUC 30i» - www.fanuc.ru.
4. Числовое программное управление https://ru.wikipedia.org/wiki/Числовое_программное_управление#:~ (дата обращения: 25.04.2021).
5. ЧПУ https://www.1obl.ru/free-time/raznoe/dlya-chego-nuzhny-stanki-chpu/(дата обращения: 25.04.2021).
6. Системы Heidenhainhttps://www.heidenhain.ru/ru_RU/produkcija/sistemy-chpu/tnc-128/ (дата обращения: 18.04.2021).
7. Системы SINUMERIKhttps://simatic-market.ru/catalog/Siemens-CA01/10166050/info/ (дата обращения: 18.04.2021).
8. Система fanuchttps://www.fanuc.eu/ru/ru/чпу/cnc-system/series-30i-31i-32i-b-plus (дата обращения: 18.04.2021).

УДК 629.12

ПРЕДЛОЖЕНИЯ ПО ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЪЕКТА МОРСКОЙ ТЕХНИКИ «ПЛАВУЧИЙ ЭНЕРГОБЛОК» С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КЛАССА PDM В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Щербинина Анжелика Валерьевна
Санкт-Петербургский государственный морской технический университет
Лоцманская ул., 3, 190121, Санкт-Петербург, Россия
e-mail: anzhelika17-09-98@yandex.ru

Аннотация. Цифровая трансформация объектов морской техники предусматривает интеграцию современных информационных технологий во все сферы деятельности и преобразование производственных процессов организации, компании в интересах их прогрессивных изменений, повышения конкурентной способности выпускаемой продукции, предоставляемых услуг, повышения качества жизни ее сотрудников. На примере внедрения PDM-систем управления проектными данными объектов морской техники типа «Плавучий энергоблок» рассмотрены вопросы формирования единого защищенного информационного пространства управления производственными процессами. Показана возможность цифровой трансформации и сформулированы предложения по обеспечению принципиально нового качества структурированного PDM-хранения, распределения и использования информации по операциям на каждой стадии жизненного цикла типового плавучего энергоблока при обязательном условии соблюдения требований организационно-технических регламентов защиты данных, автоматизированного мониторинга и контроля их реализации.

Ключевые слова: PDM-система; плавучий энергоблок; защита данных; квалиметрический анализ; жизненный цикл; информационные технологии; регламент обеспечения информационной безопасности.

PROPOSALS FOR THE DIGITAL TRANSFORMATION OF THE MARINE ENGINEERING FACILITY "FLOATING POWER UNIT" USING PDM-CLASS INFORMATION TECHNOLOGIES IN A PROTECTED VERSION

Shcherbinina Anzhelika
St. Petersburg State Marine Technical University
3 Lotsmanskaya St, Saint Petersburg, 190121, Russia
e-mail: anzhelika17-09-98@yandex.ru

Abstract. The digital transformation of marine engineering facilities provides for the integration of modern information technologies into all spheres of activity and the transformation of the production processes of the

organization, the company in the interests of their progressive changes, increasing the competitive ability of products, services provided, improving the quality of life of its employees. Using the example of the introduction of PDM-systems for managing design data of marine equipment objects of the "Floating Power unit" type, the issues of forming a single protected information space for managing production processes are considered. The possibility of digital transformation is shown and proposals are formulated to ensure a fundamentally new quality of structured PDM storage, distribution and use of information on operations at each stage of the life cycle of a typical floating power unit, subject to mandatory compliance with the requirements of organizational and technical regulations for data protection, automated monitoring and control of their implementation.

Keywords: PDM-system; floating power unit; data protection; qualimetric analysis; life cycle; information technologies; information security regulations.

Интенсивное внедрение информационных технологий на предприятиях, автоматизация производственных процессов качественно изменяют управление предприятием, компанией в целом. Цифровая трансформация объектов морской техники предусматривает, прежде всего, интеграцию современных информационных технологий во все сферы и преобразование деятельности предприятия. Целью этих инновационных изменений, как правило, является прогрессивное развитие предприятия в интересах повышения конкурентной способности выпускаемой продукции, предоставляемых услуг, что, безусловно, должно приводить к повышению качества жизни сотрудников предприятия, компании, организации [1, 2].

Особая роль в этих процессах преобразований, по нашему мнению, принадлежит информационным технологиям класса Product Data Management (PDM), обеспечивающим интеграцию процессов управления проектными и эксплуатационными данными на всех стадиях жизненного цикла продукции и услуг [3-8].

Внедрение и эффективное использование PDM-систем повышает доступность всего массива необходимых данных, объединение сведений о продукции в единую, логически построенную систему с соответствующей научно обоснованной моделью. Тем самым формируется единая рабочая информационная среда (пространство), предоставляющая сотрудникам предприятия требуемую достоверную и актуальную информацию в удобной форме, в кратчайшее время с учетом специфики каждой стадии жизненного цикла продукции, обеспечением контроля конфиденциальности, доступности, целостности больших объёмов инженерно-технических данных проектирования, производства, эксплуатации и утилизации изделий.

Типовые структурированные данные, управляемые модулем PDM, включают: описание и характеристики; паспорт модели изделия; номера его частей; информацию о производителе; единицы измерений; стоимостные характеристики; схемы и чертежи изделия; технологические карты и многое другое.

Вместе с тем, в настоящее время существует настолько большой выбор программных средств и комплексов (ПК) класса PDM, что сам выбор для ряда компаний превращается в значительную проблему. Не менее значимой при этом проблемой следует считать реализацию в каждом из предлагаемых на рынке ПК класса PDM принятых в России требований и регламентов обеспечения безопасности продукции и услуг. Для информационных технологий, в первую очередь, – требований и регламентов по обеспечению информационной безопасности (ИБ). Следует подчеркнуть, что основным средством обеспечения ИБ, как известно, является наличие у предлагаемых на рынке ПК сертификатов, что практически обеспечивается лишь для отдельных ПК.

На примере внедрения PDM-систем управления проектными данными объектов морской техники (ОМТ) типа «Плавучий энергоблок» рассмотрены вопросы формирования единого защищенного информационного пространства управления проектными и эксплуатационными данными, приведены соответствующие уязвимости, угрозы и риски. Для доказательства возможности эффективного решения данной проблемы в процессе цифровой трансформации ОМТ типа «Плавучий энергоблок» был использован ПК «АСОР 14.5» (разработка СПбГМТУ), что позволило на основе количественной оценки и анализа интегрального показателя проектного качества и эффективности эксплуатации оценить соответствующие угрозы, риски, выявить перспективные направления обеспечения ИБ данного ОМТ.

В том числе, на основе сравнительного анализа 5 программных комплексов класса PDM типа «Teamcenter (PDM/PLM)», «ЛОЦМАН:PLM», «PDM STEM Suite» показано, что наиболее предпочтительным с учетом реализации требований по ИБ и показателем конкурентной способности порядка 1,54 следует считать ПК «ЛОЦМАН:PLM» разработки компании «АСКОН».

Показана возможность и сформулированы предложения по обеспечению при использовании ПК «ЛОЦМАН:PLM» принципиально нового качества структурированного PDM-хранения, распределения и использования информации по операциям на каждой стадии жизненного цикла типового плавучего энергоблока при обязательном условии соблюдения требований организационно-технических регламентов защиты данных, их автоматизированного мониторинга и контроля.

Для повышения проектного качества при создании ОМТ типа «Плавучий энергоблок» и его эффективной эксплуатации предложены следующие мероприятия по его цифровой трансформации:

В процессе проектирования изделий и их модернизации - использование накопленного, в том числе опыта в СПбГМТУ, и обязательное выполнение квалиметрической сравнительной экспертизы в рамках ранговой сертификации свойств, параметров и характеристик предлагаемых проектантами инновационных предложений и проектов с обязательной квалиметрической экспертизой наряду с оценкой конкурентной способности,

перспективности развития также реализации требований по ИБ, рисков ИБ на всех стадиях жизненного цикла каждого из ОМТ, включая плавучие энергоблоки.

В процессе управления развитием предприятия, выпускаемой продукции и предоставляемых услуг, реализации маркетинговой деятельности - формирование и непрерывную актуализацию квалиметрических баз данных и знаний (КБДЗ) в защищенном исполнении с квалиметрическим ранжированием выпускаемой продукции и услуг, их конкурентной способности.

В процессе подготовки и переподготовки кадров - создание типовых интерактивных электронных технических руководств и тренажерных комплексов по автоматическому контролю знаний-умений-навыков использования персоналом используемых ПК, включая реализующие PDM-технологии, с целью ускоренного изучения и качественного освоения передовых практических методов.

Реализация данных предложений позволит систематизировать разработку, хранение и актуализацию документации, минимизировать временные и трудовые ресурсы, исключить ошибки проектирования, повысить качество планирования и управления предприятием в целом, его конкурентной способностью.

СПИСОК ЛИТЕРАТУРЫ

1. Щербинина А.В. Стартап-проект «Квалиметрическое ранжирование информационных технологий класса PDM в жизненном цикле объекта морской техники типа «Плавучий энергоблок» и их практическое освоение» / Санкт-Петербург, СПбГМТУ, ИТвЖЦ МТ, 2021 г.
2. Электронный журнал: Управляем предприятием № 7 (7), август 2011, «PDM-СИСТЕМЫ: ВЧЕРА, СЕГОДНЯ, ЗАВТРА...» /А.Тимошин
3. PDM-система: что это такое, её назначение. [Электронный ресурс] URL: https://www.zwsoft.ru/stati/pdm-sistema-chto-eto-takoe-eyo-naznachenie (18.04.2020).
4. ЛОЦМАН PLM. [Электронный ресурс] URL: https://ascon.ru/products/889/review/ (Дата обращения: 18.04.2020).
5. Teamcenter (PDM/PLM). [Электронный ресурс] URL: https://nslabs.ru/programmnoe-obespechenie/resheniya-siemens-plm-software/teamcenter-pdm-plm/ (Дата обращения:18.04.2020).

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 123.1

СВОБОДА КАК УСЛОВИЕ ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

Артюхин Антон Сергеевич
Ленинградский государственный университет им. А.С. Пушкина, Институт экономической безопасности
Подгорная ул., 17, Выборг, 188800, Россия
e-mail: antsart@yandex.ru

Аннотация. Рассматривается проблема свободы в контексте обретения человеком психологической уверенности в личной безопасности. Приводятся взгляды великих философов прошлого на свободу как главную жизненную ценность человека.

Ключевые слова: потребность; безопасность; личная свобода; жизненная ценность; психологическая безопасность личности; социальная ответственность.

LIBERTY AS A CONDITION OF THE PERSONAL PSYCHOLOGICAL SECURITY

Artyuhin Anton
The Leningrad State University, named after A.S. Pushkin, The Institute of the economic security
17 Podgornaya St, Vyborg, 188800, Russia
e-mail: antsart@yandex.ru

Abstract. The problem of liberty is considered in the context of gaining psychological confidence in personal security. The views of the great philosophers of the past on liberty as the main value of human life are presented.

Keywords: need; security; personal liberty; vital value; personal psychological security; social responsibility.

Одной из базовых потребностей человека, как указал ещё А. Маслоу, является обеспечение своего физического выживания и безопасности в обществе [1]. Без решения этой задачи всё остальное (потребности в познании, социальном общении, духовном развитии, нравственном совершенствовании и др.) теряет свой смысл. Важным показателем удовлетворённости потребности в безопасности как защищённости от разного рода социальных угроз является реальное обладание личной свободой, под которой понимается уверенность в сохранности своей жизни и имущества, отсутствие серьёзных социальных страхов и тревоги, поддержание социального порядка.

Свобода представляет собой жизненно важную ценность для каждого человека. Внешняя сторона свободы в современном обществе гарантируется правовой системой государства. Действующая российская Конституция в ст. 22 закрепляет личную свободу и неприкосновенность личности [2]. Помимо этого, в Конституции гарантируются различные проявления гражданской свободы: свобода совести и вероисповедания (ст. 28), свобода мысли и слова (ст. 29), свобода политического выбора и деятельности общественных объединений (ст. 30), свободное использование своих способностей (ст. 34), свобода творческого самовыражения (ст. 44). Правовые нормы, отстаивающие права и свободы личности, содержатся во всём массиве нормативно-правовых актов РФ. Современное правовое государство берёт на себя обязательство по предоставлению юридических гарантий защиты личности, обеспечивая тем самым приемлемый уровень личной безопасности.

Но сколь бы ни были совершенными законодательная и судебная системы государства, они не могут добиться состояния полной безопасности и свободы личности. Следует учитывать ещё и внутреннюю сторону свободы, которая определяется субъективно, на основе психологических ощущений своего положения в обществе. Тем самым свободу следует рассматривать как важное условие психологической безопасности личности. Потеря свободы или её ограничения, воспринимаемые людьми как чрезмерные, вызывают массовый протест, который может принять и деструктивные формы.

В чём же заключается сущность свободы, если исходить из субъективно-психологического подхода? Обычно люди воспринимают свободу как возможность самостоятельно принимать решения и выбирать формы своего социального поведения, увязывая её с волевыми психическими процессами.

Древнегреческий философ Платон, противопоставляя свободу рабству, заметил, что свобода прекрасна сама по себе и является главным благом государства. Но ценя свободу, тем не менее он указывает на возникающее противоречие, приводящее к общественному вреду. Рассматривая любое принуждение как недопустимое, люди перестают считаться с требованиями закона, перестают подчиняться властям. «Опьянение свободой» ведёт к снисходительности к собственным порокам и при одновременном ужесточении претензий к

окружающим [3, с. 413]. Обретение полной свободы становится несовместимым с каким-либо государственным управлением, что ведёт либо к распаду государства, либо установлению тирании.

В эпоху Нового времени утвердилось представление о свободе как важном естественном праве человека. По определению Т. Гоббса, «свободный человек – тот, кому ничто не препятствует делать желаемое, поскольку он по своим физическим и умственным способностям в состоянии это сделать» [4, с. 145]. Т. Гоббс рассматривает свободу более широко, это не просто подчинение законам и установленным нравственным принципам, важность которых им не отрицается, но и возможность что-либо говорить и делать сверх того, без какого-либо внешнего принуждения. Ограничением свободы человека является, в первую очередь, не государственное принуждение, а уровень развития его личности и те цели, которые он сам перед собой ставит. Истинная свобода человека, по Т. Гоббсу, заключается в том, что «он не встречает препятствий к совершению того, к чему влекут его воля, желание или склонность» [4, с. 146].

Ж.-Ж. Руссо исходит из того, что свобода является главной жизненной ценностью человека, без обладания которой он теряет всякий смысл своего существования: «Отказаться от своей свободы – это значит отречься от своего человеческого достоинства, от прав человеческой природы, даже от её обязанностей. Невозможно никакое возмещение для того, кто от всего отказывается. Подобный отказ несовместим с природой человека; лишить человека свободы воли – это значит лишить его действия какой бы то ни было нравственности» [5, с. 156]. Общество по мере исторического развития всё больше ограничивает свободу человека, превращая его в покорного раба. Опасность рабства как абсолютной несвободы Ж.-Ж. Руссо видит в том, что «в оковах рабы теряют всё, вплоть до желания освободиться от них, они начинают любить рабство» [5, с. 153-154].

Мысль о том, что угроза свободе личности исходит не столько от государства, сколько от общества развивает Дж. С. Милль: «тирания коллектива над отдельными личностями» намного страшнее государственной власти даже в условиях самого жестокого политического режима. Это умозаключение он обосновывает так: такая «тирания куда сильнее любых политических репрессий, и хоть дело не доходит до крайностей, но ускользнуть от наказаний труднее, они проникают в детали жизни глубже и порабощают саму душу. Законов против тирании чиновников недостаточно; нужна защита от тирании господствующих мнений и чувств, от стремления общества навязать свои идеи как правила поведения» [6, с. 11]. Единственная причина, которую Дж. С. Милль признаёт в качестве убедительного довода для ограничения свободы действий человека со стороны государства и общества – предотвращение ущерба общественной жизни. Он отмечает важную мысль о том, что совершенно недостаточно каждому человеку предоставить свободу, и тогда она утвердится в обществе. Свободой надо уметь правильно пользоваться, что зависит от уровня исторического прогресса общества: «Свобода неприменима как принцип при таком порядке вещей, когда люди ещё не способны к саморазвитию путём свободы» [7, с. 622].

Многие известные философы обосновывали мысль о том, что существование свободы должно обязательно иметь социальные границы своей реализации: «Свобода сама себя упраздняет, если она не ограничена. Неограниченная свобода означает, что сильный человек способен запугать того, кто слабее, и лишить его свободы. Именно поэтому мы требуем такого ограничения свободы государством, при котором свобода каждого человека защищена законом» (К. Поппер) [8, с. 145]; «свобода – это, в первую очередь, не привилегии, а обязанности» (А. Камю) [9, с. 172]; «Свобода не состоит в одном приобретении и расширении прав. Человек только потому имеет права, что он несёт на себе обязанности, и наоборот, от него можно требовать исполнения обязанностей единственно потому, что он имеет права… человек есть существо разумно-свободное, которое носит в себе сознание верховного нравственного закона и в силу свободной своей воли способно действовать по представлению долга… верховный нравственный закон, идея добра, это непременное условие свободы…» (Б. Н. Чичерин) [10, с. 632-633]; «Свобода есть не всегда только право, но и обязанность, обязанность относительно другого», поэтому «по-настоящему любит свободу и защищает её тот, кто хочет дать другому и другим реальную возможность воспользоваться свободой и осуществить её в жизни» (Н. А. Бердяев) [11, с. 65, 64] и др. Парадокс свободы заключается в одновременном стремлении человека уйти от ограничений и необходимости их принятия. Свобода желаний и устремлений неминуемо должна сопровождаться осознанием человеком социальной ответственности за средства и последствия их осуществления.

Для психологического обретения внутренней свободы вовсе недостаточно избавиться от излишнего внешнего принуждения. Свобода должна обрести собственное внутреннее содержание, иначе человек, не зная, что делать с данной ему свободой, предпочитает избавиться от неё вообще. Этот психологический феномен Э. Фромм назвал «бегством от свободы». Обретение свободы, как показывает Э. Фромм, у многих людей порождает чувство психологической неустойчивости: «Свобода от внешних сил ведёт к росту внутренних препон, принуждений и страхов, которые готовы лишить всякого смысла все победы, одержанные ради свободы» [12, с. 105], что заставляет людей подчиняться диктаторским политическим режимам. Осознание человеком ответственности перед другими людьми, осознание своих социальных обязанностей, даёт ему ощущение подлинной свободы. Если это качество оказывается утраченным большими массами людей, то и возникают различные негативные социальные последствия, превращающие свободу в фикцию, пародию на саму себя. Стремясь к обретению свободы, люди нередко оказываются в совершенно противоположной ситуации крайней несвободы, но предпочитают заниматься самообманом и даже находят в этом определённое удовольствие: «Человек ищет свободы, в нём есть огромный порыв к свободе, и он не только легко попадает в рабство, но он и любит рабство» [13, с. 51].

Чтобы в обществе утвердилась свобода и демократия, и можно было пользоваться вытекающими из них социальными благами, необходимо приложить длительные усилия, связанных с перестроением всех социальных отношений сквозь призму свободы. В очередной раз приходится убедиться в мудрости слов, написанных полтора столетия назад Б. Н. Чичериным, что «свобода основывает своё жилище только там, где люди умеют ценить её дары, где в обществе утвердились терпимость, уважение к человеку и поклонение высшим силам, в которых выражается свободное творчество человеческого духа» [10, с. 634].

СПИСОК ЛИТЕРАТУРЫ

1. Маслоу А. Теория человеческого мотивирования // Маслоу А. Мотивация и личность. – СПб.: Евразия, 1999. С. 77-105.
2. Конституция Российской Федерации. – М.: Проспект, 2021. 64 с.
3. Платон. Сочинения в четырёх томах. Т. 3. Ч. 1 / Под общ. ред. А. Ф. Лосева и В. Ф. Асмуса. – СПб.: Изд-во С.-Петерб. ун-та; «Изд-во Олега Абышко», 2007. 752 с.
4. Гоббс Т. Левиафан. – М.: Мысль, 2001. 478 с.
5. Руссо Ж. Ж. Об Общественном договоре, или Принципы политического права // Руссо Ж. Ж. Трактаты. – М.: Наука, 1969. 703 с.
6. Милль Дж. О свободе // Наука и жизнь. 1993. №11. С. 10-15.
7. Милль Дж. Ст. О свободе // Политология: Хрестоматия / Сост. М. А. Василик, М. А. Вершинин. – М.: Гардарики, 1999. 843 с.
8. Поппер К. Открытое общество и его враги: В 2 т. Т.2. Время лжепророков: Гегель, Маркс и другие оракулы. – М.: Международный фонд «Культурная инициатива»: Феникс, 1992. 525 с.
9. Камю А. Бунтующий человек. Философия. Политика. Искусство. – М.: Политиздат, 1990. 415 с.
10. Чичерин Б. Н. Различные виды либерализма // Политология: Хрестоматия / Сост. М. А. Василик, М. А. Вершинин. – М.: Гардарики, 1999. 843 с.
11. Бердяев Н. А. Парадоксы свободы в социальной жизни // Новый Град. 1931. №1. С. 59-66.
12. Фромм Э. Бегство от свободы. – М.: АСТ, 2009. 284 с.
13. Бердяев Н. А. О рабстве и свободе человека. Опыт персоналистической философии. – Париж: YMCA-Press, 1939. 224 с.

УДК 323.2

ОСОБЕННОСТИ ТЕХНОЛОГИЙ ПОЛИТИЧЕСКОГО МАНИПУЛИРОВАНИЯ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Борщенко Виктор Владимирович
Северо-Западный институт управления РАНХиГС
Средний пр., В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: boss-victor@yandex.ru

Аннотация. Статья посвящена анализу политического манипулирования в информационном пространстве. Манипулирование рассматривается как один из базовых способов управления в социальных системах. Представлены различные виды и методы политического манипулирования.

Ключевые слова: информационно-политическое манипулирование; информационное пространство; дискурс; инфокоммуникационные структуры; методы политического манипулирования.

FEATURES OF TECHNOLOGIES OF POLITICAL MANIPULATION IN THE INFORMATION SPACE

Borshenko Viktor
The North-West Institute of Management of RANEPA
57/43 Sredny Av, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: boss-victor@yandex.ru

Abstract. The article is devoted to the analysis of political manipulation in the information space. Manipulation is considered as one of the basic methods of management in social systems. Various types and methods of political manipulation are presented.

Keywords: information and political manipulation; information space; discourse; infocommunication structures; methods of political manipulation.

Манипулирование в психологии означает тайное психическое воздействие, с целью причинения ущерба [3]. Также манипулирование может рассматриваться в качестве отношения к другому участнику взаимодействия, как к средству, объекту, орудию [7]. Чаще всего определяют следующие виды психологического манипулирования:

– создание эффекта единения путем формирования «мы» - дискурса;

– повышение статуса адресата, то есть предписывание положительных характеристик только тем акторам, которые разделяют авторскую точку зрения;

– ссылка на безымянный и обобщенный источник (утверждения в стиле «всем известно…», «ученые установили…», «высокопоставленный источник сообщил…» и т.п.);

– создание оппозиции «свой-чужой», стигматизация тех, кто выражает оппозиционное мнение, их дегуманизация, а также объективизация, то есть сведение личностных характеристик оппонента до функциональных составляющих [2].

Как метод управления персоналом манипулирование подразумевает использование наиболее аттрактивных, то есть привлекательных, стимулов для мобилизации трудового потенциала коллектива. Однако в управлении, в отличие от психологического подхода, манипулирование может рассматриваться и как конструктивная социальная практика, которая может способствовать более эффективному достижению цели за

счет мобилизации на основе общности целей и ценностей [4]. Основным критерием определения управленческого воздействия как манипулирующего признается его неочевидность, скрытость от адресата. То есть в том случае, если адресат осознает манипуляционность применяемых к нему коммуникативных практик, воздействие переходит в явную форму и приобретает черты насилия или договора.

К основным методам политического манипулирования относят: методы обмана, сокрытия информации, ухода от обсуждения темы, аргументации, внушения, убеждения, подчинения, мистификации, дозирования, информационной перегрузки, введения в заблуждение, отравления сознания, дезинформации, отчуждения, просеивания, индокринации, пропаганды, агитации, хитрости, тенденциозного представления, подрывной деятельности, терроризма и другие. Эти методы могут быть классифицированы по таким важным признакам как достижение конкретных политических целей и воздействие на аудиторию.

В зависимости от преследуемых целей можно выделить следующие виды политической манипуляции:

– действия, которые направлены на убеждение и вовлечение групп людей и организаций в проект или цель, которая была поставлена;

– действия, которые проводятся для достижения цели.

В зависимости от воздействия на аудиторию можно выделить:

– действия, направленные на изменение поведения отдельных личностей;

– действия, направленные на изменение взглядов и поведения групп людей (политических партий, общественных и религиозных организаций и т.п.);

– действия, направленные на изменение политических взглядов общества в целом» [1].

В процессе политического манипулирования *групповым сознанием* в качестве ситуаций оказания информационно-политических воздействий со стороны некого «коммуникатора» (индивидуального или группового, преследующего определенную цель) на общность людей (общественное объединение, партию и так далее), выступают собрания, митинги, различные зрелищные мероприятия совещания, и так далее.

В процессе политического манипулирования *общественным сознанием* наиболее значимым является влияние интернета и других электронных средств массовой информации, например, телевидения. Политически значимые воздействия с помощью этих информационных ресурсов осуществляются практически на всё население страны или ее части [5]. Это коммуникативное воздействие носит односторонний характер, т.е., направление движения информации только от конкретного источника к аудитории [9].

«В каждой манипуляционной технологии совокупность применения методов политического манипулирования и их последовательность зависят от:

– цели, которую они преследуют;

– средств, которые имеются в распоряжении политических манипуляторов;

– политической и информационной обстановки, в которой они реализуются» [4].

К числу основных манипуляционных технологий в политической сфере можно отнести массированное, систематическое и ситуационное информационно-политическое манипулирование.

Политическое манипулирование представляет собой особый вид управленческого воздействия, направленный на скрытое формирование в общественном и/или в индивидуальном сознании политических установок или на закрепление особых паттернов политического поведения для достижения целей организаторами соответствующего воздействия. Основой является формирование и навязывание информационных контентов. Их целью является изменение политических взглядов различных категорий людей. Влияние может распространяться как на от отдельных обывателей, так и на представителей политического истеблишмента. В нынешнем информационном обществе, доведение модифицированной информации приобретает глобальный характер и осуществляется практически в реальном масштабе времени, благодаря развитию инфокоммуникационных структур [6]. Это создает объективные предпосылки для повышения эффективности методов политического манипулирования.

СПИСОК ЛИТЕРАТУРЫ

1. Борщенко, В.В., Раскин, А.В., Романович, А.А., Тарасов, И.В. Оценка возможностей методов политического манипулирования в современном информационном пространстве. Информационные войны. 2018. – № 3 (47). – С. 42-49.
2. Гудина, Р., Клингеманна, Х.-Д. Политическая наука: новые направления / Ин-т «Открытое общество» / под ред. Гудина Р., Клингеманна Х.-Д., Науч.ред. рус. изд. Шестопал Е.Б. – М.: Вече, 1999. – 118 с.
3. Кара-Мурза, С.Г., Смирнов, С.Г. Манипуляция сознанием 2. – Москва : Алгоритм. – 2015. – 528 с.; Franke, H.W. Der Manipulierte Mensh. Grundlagen der Meinungsbildung / H. W. Franke – Wiesbaden, 1964. – p. 4.
4. Кефели, И.Ф., Мальмберг, С.А. Информационный потенциал как решающий фактор в информационном противоборстве государств // Управленческое консультирование. – 2019. – № 3. – С. 24–33.
5. Мельник, Г.С., Мисонжников Б.Я. Свобода слова и угрозы информационной безопасности. Рецензия на монографию «Свобода слова и медиабезопасность» // Управленческое консультирование. – 2019. – № 10. – С. 110–115.
6. Морозов, И.Л. Безопасность политических коммуникаций в современной России // Вестник Волгоградского государственного университета. Серия 4: История. Регионоведение. Международные отношения. – 2013. – № 1 (23). – С. 127–131; Национально-специфические особенности электронной коммуникации на английском и русском языках. - URL: https://studwood.ru/1341452/literatura/vvedenie (дата обращения: 03.07.2020).
7. Сагатовский, В.Н. Социальное проектирование (к основам теории) / В. Н. Сагатовский // Прикладная этика и управление нравственным воспитанием. – Томск, 1980. – С. 84–85.
8. Федотова, Н.А. Рекреативная функция СМИ: содержание и стратегия реализации : специальность 10.01.10 «Журналистика» : диссертация на соискание ученой степени кандидата филологических наук. – Московский государственный университет. – Москва, 2010. – С. 101–119.
9. Blanchet, B. Automatic verification of security protocols in the symbolic model: The verifier ProVerif, Foundations of Security Analysis and Design VII // Springer, Cham, 2014. – p. 54–87.
10. Hoffman, S. Engineering global consent. The Chinese Communist Party’s data-driven power expansion, Report No. 21/2019. – p. 29–35.

УДК 355.23

ВОПРОСЫ ПРЕПОДАВАНИЯ ПРАКТИКИ ИСПОЛЬЗОВАНИЯ СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ КОРАБЛЕЙ

Воробьева Диана Евгеньевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: vrbyug@mail.ru

Аннотация. Рассматриваются вопросы переподготовки кадров в организациях, занимающихся проектированием кораблей.

Ключевые слова: киберпространство; базы данных; добавленная реальность; киберполигон.

ISSUES OF TEACHING THE PRACTICE OF USING COMPUTER-AIDED DESIGN SYSTEMS FOR SHIPS

Vorobieva Diana
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: vrbyug@mail.ru

Abstract. The issues of retraining of personnel in organizations engaged in the design of ships are considered.

Keywords: cyberspace; databases; added reality; cyberpolygon.

Проект создания защищенного киберпространства как техногенной среды существования человека предполагает создание и переход к новым способам обучения на основе цифровизации и использования новейших технологий обучения.

Проблема обучения использованию систем автоматизированного проектирования кораблей упирается в отсутствие подготовленных специалистов-преподавателей с высшим образованием имеющих нужные компетенции в составе компаний.

При этом требуется переработка государственных стандартов обучения, создание лабораторной базы и многое другое.

В области информационной безопасности обучение в рамках специалитета предполагает преподавание систему управления базами данных, программирования и создания информационных систем, при этом наполнение дисциплин уже не отвечает реально внедряемым технологиям проектирования в компаниях реального сектора экономики.

В настоящее время имеется научно-методический задел, который позволяет рассчитывать на быструю доработку учебных пособий и материалов лабораторных и практических работ в требуемой области, с учетом требований ФУМО ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Алтухов А.И., Багрецов С.А., Капинчук Н.А., Чебурков М.А. Методика оценивания временных затрат на изучение курса учебной дисциплины с применением автоматизированных обучающих систем//Известия «ЛЭТИ». —2016. —№7.
2. Петлин М. А. Социально-философские аспекты киберпространства //Вестник Омского университета. — 2014. — №. 3 (73).
3. Одинцов С. А., Ващенко А. В. Развитие теорий информационного общества и понятия «Киберпространство» //Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. — 2016. — №. 121.
4. Добринская Д. Е. Киберпространство: территория современной жизни //Вестник московского университета. Серия 18. Социология и политология. — 2018. — Т. 24. — №. 1.
5. Дейнеко А. Г. Право киберпространства: pro et contra //Право в сфере Интернета. — 2018. — С. 246—255.

УДК 070.15

ЛИНГВИСТИЧЕСКИЕ ИНСТРУМЕНТЫ ЭМОЦИОНАЛЬНО-ПСИХОЛОГИЧЕСКОГО ПОРТРЕТИРОВАНИЯ В ПРОПАГАНДИСТСКОМ ДИСКУРСЕ

Глущенко Олеся Анатольевна
Северо-Западный институт управления РАНХиГС
Средний пр., В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: oag.kam@mail.ru

Аннотация. Рассматриваются совокупность разноуровневых лингвистических средств, способов и технологий, применяемых для описания эмоций и чувств отправителя и получателя сообщения в пропагандистском дискурсе вакцинации в социальной сети ВКонтакте (https://vk.com/stopcoronavirusrf).

Ключевые слова: лингвистическое портретирование; эмоции; концепт; дискурс; пропаганда.

LINGUISTIC TOOLS OF EMOTIONAL AND PSYCHOLOGICAL PORTRAITURE IN PROPAGANDA DISCOURSE

Glushchenko Olesya
The North-West Institute of Management of RANEPA
57/43 Sredny Av, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: oag.kam@mail.ru

Abstract. The article considers a set of multi-level linguistic tools, methods and technologies used to describe the emotions and feelings of the sender and recipient of the message in the propaganda discourse of vaccination in the social network VKontakte (https://vk.com/stopcoronavirusrf).

Keywords: linguistic portraiture; emotions; concept; discourse; propaganda.

Введение. Эмоционально-психологическое состояние человека отражается в его речи с разной степенью достоверности и объективности, но максимально корректно – в непринужденной речи, когда отправителем сообщения движут порыв и стремление быстро обозначить свою позицию в связи с актуальным информационным поводом [1-2]. В сегменте письменной ситуативной коммуникации в социальных сетях (отклики-комментарии на посты в ленте) мы черпаем материал для лингвистических наблюдений. В центре изучения социальная сеть ВКонтакте «СтопКоронавирус.РФ» (https://vk.com/stopcoronavirusrf), отражающая фрагмент пропагандистского дискурса вакцинации. Материалом исследования послужила сплошная выборка эмоциональных репрезентаций из текстов комментариев к постам о вакцинировании и постам со статистикой по коронавирусу общим объемом порядка 3500 контекстов. Противоковидная вакцинация стала тем самым информационным поводом, по отношению к которому сейчас российское общество расколото и на фоне которого публично оцениваются достижения и провалы государственной социальной политики [3]. Исследование эмоционального пространства именно разговорных текстов в этой сфере позволяет выявить основные, так сказать, узлы конфликтности и прогнозировать вектор развития гражданской дискуссии. Кроме того, языковой материал определенным образом коррелирует с данными социальных опросов и отражает латентные аспекты обсуждаемой проблемы (делать или не делать отечественную прививку против ковида).

Мы предполагаем, что характер использования и «семантическая конфигурация» лингвистических инструментов для эмоционально-психологической характеристики человека зависит не только от сущности объекта описания (свой или чужой удачный или неудачный опыт вакцинирования, качество российских вакцин, проявление побочных эффектов вакцинирования и т.п.), но и от заявленных и скрытых целей отправителя сообщения. Другими словами, активно распространяемый противниками вакцинации негативный опыт вакцинирования (часто вымышленный или основанный на слухах) с описанием серьезных побочных проявлений не только объясняется желанием поделиться с другими информацией и предостеречь или напугать получателей информации, но и отражает общую неудовлетворенность российской действительностью, усиливающиеся протестные настроения на фоне единого события – вакцинации.

В центре внимания лингвистические инструменты как совокупность разноуровневых средств, способов и технологий, применяемых для описания эмоций и чувств отправителя и получателя сообщения как основных объектов портретирования. Лингвистические инструменты мы рассматриваем вне установок корпусной лингвистики.

1. Лексические номинативные средства используются для обозначения таких базовых эмоций и чувств, как радость, страх, отвращение, злость, гнев, возбуждение, стыд, жалость, тревога, спокойствие. Чувственно-эмоциональная шкала трехчленная: есть нейтральная зона (состояния равнодушия и/или спокойствия) и противоположные секторы положительных и негативных эмоций и чувств с доминированием последних. Самыми востребованными для номинации являются жалость, страх и раздражение, они представлены в градациях и вариациях: собственно жалость в разной интенсивности проявления – сострадание – соболезнование; страх – ужас – опасение; гнев – ярость – злость – раздражение. Основными источниками эмоций и чувств выступают люди (их слова, поступки) и информация.

2. Лексико-стилистические средства представлены в большинстве случаев сниженными наименованиями. Особую образную функцию выполняют уменьшительно-разговорные существительные, которые вносят положительную оценку в описание негативных обстоятельств (как правило, мы встречаем это в позитивных отзывах о вакцинации или в поучительных отзывах с призывом вакцинироваться).

3. Лексико-грамматические средства представлены оценочными новообразованиями и словами с эффектом семантизации морфем:

4. Графические средства встречаются более чем в трети текстов и построены на механизмах сингрефемики и супраграфемики. В замещающей и усиливающей функциях работают эмодзи всех поколений.

5. Лексические образные средства и риторические фигуры интересны с учетом семантики контекста. Антитеза, нанизывание синонимов, языковая игра, эпитеты, метафорические переносы способствуют наглядному представлению эмоций и чувств пишущего.

Обращают на себя внимание характерные ассоциативные сближения слов в тексте. Так, в текстах негативного посыла отвержение отечественных вакцин мотивируется недоверием к их качеству. Именование негативных эмоций в связи с вакцинацией соседствует в контексте с представлениями о медицинском произволе, принуждении к экспериментам на грани с насилием. За счет этого концепт вакцинации пересекается с концептом

насилия, и на уровне языковой картины мира формируется образ принудительной вакцинации как проявления полицейского государства:

… не понимаю, почему вы боитесь здоровых людей, которые не хотят быть подопытными кроликами. Мы не антипрививочники. Прививки делали и себе и детям. Но сейчас не хотим участвовать в тестировании малоизученных вакцин. Почитайте инструкцию к вакцинам. Там много чего неизвестно и не проводилось. Не бойтесь, вы же привиты и теперь бессмертные. Но это не точно. Как и все связанное с вакцинацией (комментарий 10.08.2021 к посту в 14.01);

То есть, оправдываясь сейчас, вы себя реально ПРИЗНАЛИ ВАКСАНУТОЙ :) А говорите, что в очереди за прививкой от глупости не были бы первой :) Или это прививка так на вас подействовала? Побочка такая, да?? (комментарий 06.08.2021 к посту в 15.00);

Алана, да кого интересуют твои медотводы? Сказано колоться!! Мыши кололись, плакали, но продолжали жрать кактус... (комментарий 06.08.2021 к посту в 15.00);

Никита, тебе, самому не стыдно? Почему я должна быть испытуемой? Причем добровольно? Вакцину делают до ... А не во время такой эпидемии... (комментарий 02.-8.2021 к посту в 19.01);

На большинство развернутых положительных отзывов-комментариев о вакцинировании в течение первого часа поступает ряд отрицательных комментариев антипрививочной направленности, в которых активированы такие концепты, как безумие, угроза, обман и иные, что искусственно подпитывает антипрививочные настроения. Противники вакцинирования применяют самый широкой спектр характеристик крайних эмоционально-психологических состояний человека по сравнению с теми, кто поддерживает вакцинацию.

Заключение. Степень насыщенности текста лингвистическими маркерами эмоционально-психического состояния может отражать особенности общественной дискуссии и важность смысловых аспектов темы (что именно страшит в вакцинации, с какими страхами и фобиями сопряжены переживания, каково ассоциативное поле для маркеров эмоций и настроения и т.п.). Изучение модуля лингвистических средств портретирования внутреннего состояния человека интересно для задач прогнозирования общественного отношения к любому социально значимому событию.

СПИСОК ЛИТЕРАТУРЫ

1. Бабенко Л.Г. Лексические средства обозначения эмоций в русском языке. – Свердловск: Изд-во Урал. ун-та, 1989. 184 с.
2. Романов Д.А. Языковая репрезентация эмоций: уровни, функционирование и системы исследований (на материале русского языка): автореф. дис…д. филол. наук – Белгород, 2004. 52 с.
3. Глущенко О.А. Организация агитационного дискурса вакцинации (на примере сообщества ВКонтакте «СтопКоронавирус.РФ») / Язык и речь в Интернете: личность, общество, коммуникация, культура: сборник статей V Международной научно-практической конференции. Москва, РУДН, 22-23 апреля 2021 г.: в 2 т. / под общ. ред. А.В. Должиковой, В.В. Барабаша. – М.: РУДН, 2021. 502 с. С 236-242.

УДК 32.019.51

КОРРУПЦИЯ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дейнека Ольга Сергеевна
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: osdeyneka@yandex.ru

Аннотация. Статья посвящена угрозам использования коррупции как ярлыка, закрепляемого за властью и государством, и может стать поводом цветных революций. Приведены результаты эмпирического исследования деформированного образа партии власти.

Ключевые слова: коррупция; манипулятивные технологии; экономическая интолерантность; протестная активность; информационная безопасность; имидж России.

CORRUPTION IN THE CONTEXT OF INFORMATION SECURITY

Deyneka Olga
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: osdeyneka@yandex.ru

Abstract. The article is devoted to the threats of using corruption as a label assigned to the authorities and the state, and can become a pretext for color revolutions. The results of an empirical study of the deformed image of the party in power are presented.

Keywords: corruption; manipulative technologies; economic intolerance; protest activity; information security; image of Russia.

В информационно-психологических войнах ярлык «коррупционной страны» используется для воздействия на экономическое, политическое и правовое сознание ее граждан. Если на внешнем контуре медиапространства в процессе имиджевых нападок на Россию чаще используется геополитическое клише «страна-агрессор» [5], то на внутреннем контуре в так называемой «имиджевой войне» активизируется моральный приговор обвинений власти в коррупции.

В возникающих против коррупции движениях, исследователи видят серьезный политико-протестный потенциал [2], которым пользуются в политической борьбе за власть. Среди технологий и приемов, применяемых во время цветных революций для дискредитации власти (уничижение, деморализация, выставление в смешном свете и, наконец, криминализация образа политических институтов и лидеров), часто используется апелляция к коррупции.

Уничижение, деморализация, выставление в смешном свете и, наконец, криминализация образа политических институтов и лидеров направлены на дестабилизацию общественно-политической ситуации в стране и ее поступательного развития вплоть до переворотов. На флаг протестных акций как правило вывешивается феномен коррупции. Кроме того, коррупция снижает уровень политической лояльности граждан к государству, доверие политическим лидерам и институтам, что небезопасно, в частности, в период выборных кампаний.

На фоне весеннего этапа реализации антигосударственного проекта «Навальный» нами было выполнено эмпирическое исследование доверия россиян (март 2021) к партии власти с использованием полупроективных методов. Общая выборка исследования составила 1330 респондентов из 82-х регионов РФ, 51,95 % женщины, 48,05 % мужчины от 18 лет с разным уровнем дохода и образования.

Результаты ассоциативного теста показали не благоприятную картину образа ведущей партии страны. Частотный анализ ассоциаций с партией «Единая Россия» по модальности показал, что среди оценочных характеристик партии власти оказалось 584 негативных и только 224 позитивных, а также 476 нейтрально окрашенных ассоциаций. Содержательно преобладающие негативные характеристики связаны с подозрениями в воровстве, коррупции, жульничестве, обмане. Таким образом, образ партии власти криминализируется в обыденном сознании у значительной части россиян. Политическому институту и его лидерам приписываются вредоносность обществу посредством воровства и коррупции.

В другом задании требовалось указать события, которые ассоциируются у респондентов с деятельностью партии «Единая Россия». Выделены пенсионная реформа, проведение выборов и конституционная реформа, а на втором месте по частоте упоминаний оказалась свободная ассоциация «никакие» (что является серьезным сигналом для руководства и членов партии). Однако и в этом тесте 25 упоминаний было о коррупции и еще 24 упоминания о воровстве. Еще в одном задании, где требовалось указать причины недоверия, партии власти у населения, обнаружено 131 упоминание воровства.

По мнению некоторых авторов, восприятие коррупции в России остается на высоком уровне, причем объективно уровень коррупции в стране явно преувеличен при сравнении с другими странами [1, 2].

В обыденном сознании установки криминализация и клеймения власти формируются не только и не столько на основе реальных фактов преступных деяний, которые часто носят точечный характер, но и на основе воздействия социальных сетей. Несмотря на имеющиеся позитивные изменения в экономической политике государства, в целом, эффективные меры по преодолению негативных последствий пандемии COVID-19, обнадеживающие сдвиги в отражении антикоррупционной политики (например, [3]), в обыденном сознании граждан инерционно сохраняется действие ярлыка «жулики и воры», навешанного на властные структуры в конце 90-х – начале 2000-х гг. Преувеличенные претензии к партии власти нашли отклик на фоне объективно высокого экономического расслоения граждан и экономической интолерантности определенной части населения страны. Наряду с коррупцией фактор расслоения и доступа ограниченного числа людей к ресурсам постоянно эксплуатируется в деструктивной деятельности социальных медиа, например, с элементами экономического терроризма и призывом не платить налоги [4].

Действительно, шлейф недоверия власти из 90-х очень сложно купировать, и прежде всего на фоне контрпропаганды в оппозиционных СМИ и социальных медиа. Обнаруженный по результатам нашего исследования факт «криминализации» партии «Единая Россия» в обыденном сознании, приписывания ей безусловного участия в коррупции и воровстве, был, очевидно, спровоцирован и распространенным в социальных сетях фильмом, запущенным после возвращения, выздоровевшего А. Навального из-за рубежа.

Полученные результаты корреспондируют с данными других авторов. Согласно результатам выполненного в филиале РАНХиГС социологического опроса [2], больше половины экспертов (54,2% из 1005 чел.) видят в коррупции угрозу национальной безопасности государства. При этом уязвимость государства существенно возрастает в связи с возможным подкупом государственных служащих со стороны иных государств, для работы в их интересах, а также подкупа агентов влияния.

Декриминалицация образа страны, власти и доминирующей партии требует не только дальнейшего совершенствования законодательства, но и координации работы по научно обоснованной активизации всех социальных регуляторов в обществе (закон, мораль, традиции, наука), которые находят преломление в ценностях и нормах граждан. Поскольку более подвержены дестабилизации посредством цветных революций государства, в которых отсутствует твердая власть, обратная связь между ней и народом, процветает коррупция и имеет место подмена национальных интересов личными [6], не отменяется также последовательная антикоррупционная деятельность и ее грамотное отражение в СМИ.

Исследование выполнено при поддержке гранта СПбГУ 26520757.

СПИСОК ЛИТЕРАТУРЫ

1. Алейников А.В., Стребков А.И., Газимагомедов Г.Г., Сунами А.Н., Карпенко А.Д. Конфликтно-криминологическая парадигма бытия коррупции (статья 2) // Всероссийский криминологический журнал. 2018. Т. 12, № 5. С. 622–633. DOI: 10.17150/2500-4255.2018.12(5).622-633.

2. Воронцов С.А., Понеделков А.В. О слабых звеньях коммуникативной деятельности по противодействию коррупции // Коммуникология. 2018.Том 6.№ 1. С.143-1543.
3. Дейнека О.С., Духанина Л.Н., Крылова Д.В., Максименко А.А. Представления о коррупции в системе высшего образования у выпускников ведущих российских вузов // Высшее образование в России. 2020. Т. 29. № 7. С. 64-74. DOI: https://doi.org/10.31992/0869-3617-2020-29-7-64-74
4. Дейнека О.С. Дискурс с признаками экономического терроризма против налоговой солидарности // Медиа в современном мире. 59-е Петербургские чтения: сб. матер. Междунар. научн. форума (9-12 ноября 2020 г.) / отв. ред. В.В. Васильева. В 3-х т., Т. 2. СПбГУ. 2020. С. 227-229. http://jf.spbu.ru/upload/files/file_1604510826_2378.pdf
5. Мельник Г. С., Мисонжников Б. Я. Лингвистические приёмы антироссийской пропаганды – новый тренд массмедиа Германии // Гуманитарный вектор. 2020. Т. 15, No 5. С. 99–109. DOI: 10.21209/1996-7853-2020-15-5-99-109
6. Семченков А.С. «Цветные революции» как угроза национальной и региональной безопасности: специфика и пути противодействия // Вестник Российской нации. 2016. № 6. с. 185-196.

УДК 070

ПРОТИВОДЕЙСТВИЕ РАСПРОСТРАНЕНИЮ ИДЕОЛОГИИ ЭКСТРЕМИЗМА В ЧЕЧЕНСКОЙ РЕСПУБЛИКЕ: МЕДИЙНЫЙ АСПЕКТ

Евсеев Александр Юрьевич
Северо-Западный институт управления РАНХиГС
Средний пр., В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: evseevau@mail.ru

Аннотация. В статье рассматриваются вопросы, связанные с глобальной проблемой современности – распространением идеологии терроризма и экстремизма. Автор анализирует роль медиа в работе по противодействию идеологии экстремизма на примере медийной политики Чеченской республики.

Ключевые слова: медиа; медийная политика; экстремизм; идеология; противодействие распространению идеологии экстремизма.

COUNTERING THE SPREAD OF THE IDEOLOGY OF EXTREMISM IN THE CHECHEN REPUBLIC: MEDIA ASPECT

Evseev Alexander
The North-West Institute of Management of RANEPA
57/43 Sredny Av, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: evseevau@mail.ru

Abstract. The issues related to the global problem of our time – the spread of the ideology of terrorism and extremism-are studied. The author analyzes the role of the media in countering the ideology of extremism on the example of the media policy of the Chechen Republic.

Keywords: media; media policy; extremism; ideology; countering the spread of the ideology of extremism.

Введение. В научном дискурсе актуализируется проблема противодействия негативным процессам глобализации; наблюдается рост интереса к деятельности российских государства и СМИ по предотвращению распространения идеологии терроризма и экстремизма. Экстремистские проявления в медиа (тексты, изображения, высказывания пользователей и фрагменты публикаций в СМИ, речи, музыка и пр.) способны оказывать влияние на формирование идеологии общественного разлада. Чеченская республика в этом отношении – показательный пример успешной борьбы с экстремизмом для многих регионов, так как она пережила военные конфликты и ситуацию нестабильности, достойно вышла из кризисного положения и сегодня, по мнению медиа-экспертов, является одним из самых безопасных регионов России [1]. Однако экстремизм относится к числу международных угроз, поэтому стратегия и тактика противодействия ему является приоритетной в информационной политике республики.

Исследование. Медийная политика Чечни строится на основе тщательного изучения тенденций и закономерностей функционирования экстремизма в мире и развития стратегий противодействия его проявлениям. В первую очередь это прогнозирование развития обстановки и своевременного принятия органами государственной власти мер, направленных на выявление, нейтрализацию и минимизацию возможных неблагоприятных последствий реализации исходящих угроз. Медиа остро и быстро реагируют на негативные материалы (публикации), а благодаря политике информационного просвещения населения таких текстов становится меньше. Об этом говорит статистика и мониторинг чеченских медиа.

Вместе с тем, тему терроризма и экстремизма нередко в СМИ и информационных лентах агентств связывают с Чечней. Приведем лишь несколько примеров.

Убийство французского учителя чеченцем: что говорят в Париже и в чеченской диаспоре. По всей Франции проводятся десятки спецопераций силовиков по выявлению исламистов. Столь решительно французские власти начали действовать после убийства преподавателя лицея под Парижем. Преступник – уроженец Чечни (https://www.dw.com/ru/ubijstvo-francuzskogo-uchitelja-chechencem/av-55327956);

По данным прокуратуры и источника в полиции, элитное подразделение французской рейдовой полиции арестовало пятерых чеченцев после четырех ночей беспорядков между бандами в городе Дижон. (https://www.aljazeera.com/news/2020/6/18/france-arrests-five-chechens-after-dijon-gang-violence);

По данным правозащитной группы ЛГБТК, родственники двух братьев, которые бежали от преследований на почве гомофобии в Чечне, но позже были схвачены, были задержаны и допрошены властями (https://www.nydailynews.com/news/world/ny-chechnya-salekh-magamadov-ismail-isayev-relatives-interrogated-detained-20210324-iqq6uphoyvgzhddy3iup3fhfeq-story.html).

Специалисты в области массовых коммуникаций отмечают, что в данном случае необходимо корректировать внешний медийный образ Чеченской республики, так как в настоящее время не отражается колоссальная работа медиа Чечни по противодействию терроризму и экстремистским проявлениям.

Экстремизм – это не только правовое или криминологическое явления, он имеет философские, политические и религиозные аспекты, оказывающее воздействие на международные отношения во всем мире, а также в отдельных странах и регионах. В связи с этим возникает необходимость объективного анализа различных факторов, влияющих на развитие таких явлений, и разработки механизмов их нейтрализации [1, с. 5-6].

Угроза экстремизма будет сохраняться до тех пор, пока существуют источники и каналы распространения экстремистской идеологии [2, с. 3475.]. В Российской Федерации экстремизмом признается: нарушение территориальной целостности России, отчуждение части ее территории, а также призывы к таким действиям. Сегодня экстремистское проявление может быть поводом для социальных и конфессиональных конфликтов. Об этом хорошо и не понаслышке знают в Чечне, и сегодня основным критерием ценностного потенциала медиа трансляции становится позиционирование равнозначных религиозных ценностей на фоне демонстрации традиционных устоев ислама как основной религии Чеченской республики. Такая позиция инициирует социальные преобразования в регионе.

Исследования экстремизма в контексте его проблемных предпосылок и последствий позволяет всесторонне осмыслить перспективы происходящих изменений, пути решения проблем [3, с. 66]. Проявления экстремизма обусловлены недовольством населения в целом или отдельной группой социальными условиями, или изменениями и сдвигами в политическом процессе.

В тех случаях, когда возможна угроза экстремистских актов, практика обеспечения безопасности людей на повседневном уровне изменяется [1, с. 8]. У российского государства накопился опыт деятельности по обеспечению территориальной целостности, на современном этапе это не только своевременное выявление и пресечение преступлений террористической и экстремисткой направленности, но и противодействие идеологии терроризма и экстремизма. Вопросы противодействия экстремистским проявлениям являются одними из наиболее важных и значимых в Чеченской республике.

В данном случае одной из эффективных стратегий противостояния экстремизму становится принцип, реализуемый в медийной политике Чечни: опереди негатив позитивом. В СМИ транслируются пути решения проблемы сохранения самобытности культуры Северного Кавказа и чеченского народа, в частности. Подчеркивается, что духовные ценности, выраженные в культуре этнического сообщества, оказывают значительное воздействие на все стороны его жизни. По мнению К.Х. Межиевой, «наряду с существующими правовыми нормами они выступают в роли регулятора общественной жизни» [4].

Роль государственной медийной политики заключается в том, чтобы не просто сформировать установки на недопустимость использования насилия/вражды/ненависти в общении, а способствовать воспроизводству полноценной традиции ценностного и значимого общения, которое всегда было превалирующим в регионе.

Заключение. В противовес агрессивной информации в социальных сетях, которая появляется время от времени, СМИ Чечни стараются формировать позитивный образ многонациональной республики с богатыми и древними традициями, отсутствием агрессивности и вражды, нацеленностью на развитие личностного потенциала человека. Особенно это касается молодежи, так как основные проявления экстремизма в социальных сетях происходят от имени молодых людей, не знакомых с традициями и жизнью на Кавказе. В 2013 г. утверждена Единая Концепция духовно-нравственного воспитания и развития подрастающего поколения Чеченской Республики. Медиа активно публикуют информацию о регулярных совещаниях, консультациях ведущих специалистов в области профилактики наркомании, экстремизма, асоциального поведения; ведущие СМИ республики делают попытку оценки современной ситуации для принятия эффективных решений. В развитии медиа духовно-просветительской направленности решающее значение имеет политика государства, так как учредителем СМИ является республиканское Министерство по национальной политике, внешним связям, печати и информации [5].

СПИСОК ЛИТЕРАТУРЫ

1. Противодействие международному терроризму: философские, политологические, социологические и религиозные аспекты: сборник материалов межведомственного круглого стола (13.11.2020). – СПб: Университет ФСИН России 2021. – 301 с.
2. Указ Президента РФ от 29.05.2020 № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // Собрание законодательства РФ. 2020. № 22. Ст. 3475.
3. Борисов А. С., Романенко Е. В. Факторы, оказывающие влияние на распространение идеологии терроризма и экстремизма в молодежной среде, и пути их устранения (на основе опыта проведенного исследования) // Вестник Национального антитеррористического комитета. 2019. № 1 (20). – С. 66–69.
4. Межиева К. Х. Духовные ценности чеченцев как регулятор общественной жизни и модернизационные процессы // Известия высших учебных заведений. Северо-Кавказский регион. Общественные науки. 2009. URL: https://cyberleninka.ru/article/n/duhovnye-tsennosti-chechentsev-kak-regulyator-obschestvennoy-zhizni-i-modernizatsionnye-protsessy (дата обращения 30.07.2021).
5. Единая концепция духовно-нравственного воспитания и развития подрастающего поколения Чеченской Республики. Грозный. 2013. URL: http://wunderkind95.ru/upload/files/%D0%BA%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D0%B8%D1%8F%20%D0%A7%D0%A0.pdf (дата обращения 29.07.2021).

УДК 001.94; 004.8; 009

ТРАНСГУМАНИЗМ И «ЦИФРОВОЙ РАЗУМ» – НОВЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ И КОГНИТИВНОЙ БЕЗОПАСНОСТИ

Кефели Игорь Федорович
Северо-Западный институт управления РАНХиГС
Средний пр., В.О., 57/43, Санкт-Петербург, 199178, Россия
e-mail: geokefeli@mail.ru

Аннотация. Анализируются скрытые угрозы, порождаемые деструктивным воздействием трансгуманизма и «цифрового разума» на ценностные ориентиры и мыслительную деятельность человека.

Ключевые слова: трансгуманизм; «цифровой разум»; идеальное; информационно-психологическая и когнитивная безопасность.

TRANSHUMANISM AND THE "DIGITAL MIND" – NEW PROBLEMS OF INFORMATION, PSYCHOLOGICAL AND COGNITIVE SECURITY

Kefeli Igor
The North-West Institute of Management of RANEPA
57/43 Sredny Av, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: geokefeli@mail.ru

Abstract. The hidden threats generated by the destructive influence of transhumanism and the "digital mind" on the value orientations and mental activity of a person are analyzed.

Keywords: transhumanism; "digital mind"; ideal; information; psychological and cognitive security.

Введение. Трансгуманизм, порождающий ценностные и медийные деструкции идеалов гуманизма, дошедших до нас из славной Античности и Возрождения, зародился в недрах зарождающейся цифровой эпохи, некоторые апологеты которой провозглашают могущество современной электронной техники (и не только), способной уподобить человека, Homo sapiens, представителям фауны в зоопарке (такой мрачный юмор уже встречается на страницах печати), которых будет созерцать постчеловек.

Стоит напомнить, что ход рассуждений о гуманизме как добродетели человеколюбия – humanitas – был задан еще Цицероном и Авлом Геллием (II в.н.э.). Геллий усматривал в humanitas греческий корень, обозначивший «учение и наставление в честных науках», ибо «старание о науках и упражнение в оных из всех животных дано одному человеку, и потому оно названо humanitas» [1, с. 98]. В эпоху Возрождения античный humanitas обогатился добродетелью человеколюбия (Марсилио Фичино), призывом Эразма Роттердамского «лучше меньше знать и больше любить, чем больше знать и не любить» [2, с. 137], а studia humanitas стала корневой основой развития собственно гуманитарного знания и социального утопизма. Утопийцы Т. Мора следуют гуманистическому принципу, согласно которому повседневный труд должен обеспечить «всем гражданам наибольшее количество времени после телесного рабства для духовной свободы и образования» [3, с. 126.]. Автором термина «трансгуманизм» был биолог-эволюционист Джулиан Хаксли, введшим его еще в 1927 г. в работе «Религия без откровения» (Huxley Julian. Religion Without Revelation, London, 1927: E. Benn), но лишь спустя 30 лет в работе «In New Bottles for New Wine» (Huxley Julian. In New Bottles for New Wine, London, 1957: Chatto & Windus) под воздействием разворачивающейся научно-технической революции и, в частности, в области биологии человека Хаксли стал интерпретировать трансгуманизм как «веру», единую для всего человечества и новую идеологию. Между тем, прообразом самого термина «трансгуманизм» явилось слово «trasumanar» из итальянского оригинала «Божественной комедии» Данте. Великий флорентиец описывает, как он, следуя за Беатриче, неожиданно оказывается в состоянии «Nel suo aspetto tal dentro mi fei» («Наблюдая за ней, я изменился внутри себя» [Paradiso 1.67]), которое вывело его «за пределы человеческого» (итал. «trasumanar») (Paradiso 1.70) [4]. Генри У. Лонгфелло в английском варианте «Божественной комедии» trasumanar перевел как transhumanise. Так трансгуманизм еще в конце XIX в. обрел в англоязычной литературе (в том числе, и научной) статус философской концепции, позитивистского миропонимания и широкого общественного движения, утверждающего значимую роль науки и передовых технологий в усилении физических, умственных и психических возможностей человека вне какого-либо социального контекста. Трансгуманистами также используется исходный глагол «transhumanise» для обозначения самого важного для них процесса – технического и биологического совершенствования человека, изменения его природы в лучшую сторону [5].

Ключевая идея трансгуманизма опирается на тезис о необходимости продолжения эволюции человека как вида на основе синтеза биологического и технологического и, соответственно, продления продолжительности жизни человека. В очередном варианте «Манифеста трансгуманистов» (2020 г.) торжественно заявляется: «Я лучше буду трансчеловеком, чем киборгом», поскольку киборг позиционируется как конечная точка интеграции человека, машины и компьютера, а трансчеловек – это непрерывная человеческая эволюция, включающая в себя слияние органического человека, технологических достижений в области искусственного интеллекта, наномедицины, генной терапии и осознание личной идентичности через новые технические коммуникационные системы. Но при этом в «Манифесте» четко оговаривается: «вместо того, чтобы разделять религиозные и политические взгляды, трансгуманизм стремится сосредоточиться на здоровом долголетии, а не на пути, по которому каждый человек идет, чтобы достичь этого». Но человек – существо социальное, политическое, которому ничто человеческое не чуждо.

Следуя идеологии трансгуманизма, образ трансчеловека, уподобляется элементарной частице, нейтрино, не встречающей никого и ничто в микромире и, тем более, в социуме.

Трансгуманизм претендует на статус идеологии построения будущего мироустройства, что наглядно прослеживается, к примеру, в Манифесте стратегического общественного движения «Россия 2045», авторы которого заявляют о необходимости разработки идеологии, объясняющей правомерность создания «технологий совершенствования самого человека, а не только его среды обитания», преодоления фундаментальных пределов физических и психических возможностей «биологического тела и способных обеспечить создание прототипа искусственного тела человека». Страна, заявляется далее, «которая первой заявит о намерении объединить эти технологии и создать работающий кибернетический организм, станет лидером самого главного мирового технологического проекта современности. Этой страной должна быть Россия». Авторы призывают нас поверить их заверениям о том, «с помощью нейроинтерфейса человек будет способен дистанционно управлять несколькими телами различных форм и размеров». Невольно возникает вопрос к читателям, а они хотели бы оказаться среди подобных «тел» со своими «формами и размерами»? В таком ракурсе предлагается «реализовать не просто механистический проект по созданию искусственного тела, а целую систему взглядов, ценностей и технологий, которые помогут человеку развиваться интеллектуально, нравственно, физически, психически и духовно». Так определена одна из задач построения нашего недалекого «светлого будущего» – «формирование культуры, связанной с идеологией будущего, техническим прогрессом, искусственным интеллектом, мультителесностью, бессмертием, киборгизацией» [6]. Великое заблуждение современных трансгуманистов, по всей видимости, заключается в том, что они избегают какого-либо признания социальной и политической природы современного (и не только) человека разумного, не желающего уподобляться создаваемым им же роботам и иным искусственным автоматам. Ценности гуманизма всегда были и, очевидно, должны оставаться жизнеутверждающими для человека, вовлеченного в паутину социальных и политических отношений реального мира, а не наполненного «телами различных форм и размеров», которых некоторые горячие головы от медиаиндустрии (и не только) пытаются внедрить в коллективное сознание.

И последнее, на что следует обратить внимание – это об идеальном, той ключевой категории философии, которая почему-то исчезла из дискурса об искусственном интеллекте. Главная трудность (потому и главная проблема философии) заключается, как заявлял в свое время Э.В. Ильенков, в том, чтобы разграничить мир коллективно исповедуемых представлений, т.е. весь социально-организованный мир духовной культуры, со всеми устойчивыми и вещественно-зафиксированными всеобщими схемами его структуры, его организации, – и реальный, материальный мир, каким он существует вне и помимо его выражения в этих социально-узаконенных формах «опыта», в объективных формах «духа». Вот здесь-то, и только здесь, различение «идеального» от «реального» («материального») и приобретает серьезный научный смысл, – и именно потому, что на практике массы людей то и дело путают одно с другим» [7, с. 41]. Идеальное, идеальность есть продукт общественных и межличностных отношений во всем их бесконечном многообразии. Идеальность имеет чисто социальную природу и происхождение. Между тем, по непонятным причинам проблема идеального (а отсюда – идеи, идеологии) как-то незаметно ушла из философского, общенаучного и политического дискурса. Для категории «идеальное» не нашлось места даже в «Большой Российской Энциклопедии», а в «Философском энциклопедическом словаре» (2010 г.) мы встречаем такой „шедевр“: «идеальность – бытие как голая идея или представление, в противоположность реальности – бытию в объективной действительности». Правда, в современной медиафилософии наметился довольно оригинальный и весьма перспективный ход в интерпретации идеального в ракурсе «цифрового разума». «Все стянулось в нуль, – восклицают составители очередного тома трудов Центра медиафилософии, – а мы стянуты цифрой, как тело – сердцем. Мы подходим к собственному разуму как разуму цифры или – цифровому разуму» [8, с. 5]. Так философия сознания трансформировалась в медиафилософию – ту самую философскую антропологию разума, которая исходит из понимания реальности (и человека, в том числе) как лингвистический, иконический, медиальный повороты в культурной истории, на смену которым пришел тот самый цифровой поворот, утверждающий наступление господства цифрового кода, «цифрового разума» [8, с. 92, 105-106]. «Цифровой разум» как раз и заключает в себе те самые скрытые угрозы, по отношению к которым должна выстраиваться система обеспечения информационно-психологической и когнитивной безопасности.

Заключение. Категория «идеальное» – такая же фундаментальная в социально-философском осмыслении окружающего мира и человеческой жизнедеятельности, как и «материальное», «пространство», «время», «движение», «развитие». Каждое из них конкретизируется в исследованиях искусственного интеллекта как «цифрового разума», его места и роли в социуме и потому взывает к необходимости включения категории идеального в эпицентр исследований и дискуссий об искусственном интеллекте и медиапространстве.

СПИСОК ЛИТЕРАТУРЫ

1. Геллий Авл. Афинских ночей записки, содержащиеся в двадцати книгах. В 2-х ч. Ч. 2. М., 1787.
2. Эразм Роттердамский. Руководство христианского воина // Философские произведения. М.: Наука, 1986. – 703 с.
3. Мор Т. Утопия. М.: Изд-во Академии наук СССР, 1953. – 302 с.
4. [Электронный ресурс]. URL: https://digitaldante.columbia.edu/dante/divine-comedy/paradiso/paradiso-1/
5. Громова И.А., Кольцова О.Н. Роль аллюзии в создании образа Бертрана Зобриста в романе «Инферно» Дэна Брауна // Филология и литературоведение. 2015. № 2 [Электронный ресурс]. URL: https://philology.snauka.ru/2015/02/1183 (дата обращения: 12.04.2021).
6. [Электронный ресурс] URL: http://2045.ru/manifest/
7. Ильенков Э.В. Диалектика идеального // Логос. 2009. № 1. С.6-62.
8. Критика цифрового разума / Гл. редактор В.В. Савчук. – СПб.: Академия исследования культуры, 2020. – 295 с.

УДК 327.8

К ВОПРОСУ ОБ ИНФОРМАЦИОННОМ ПРОТИВОБОРСТВЕ В КАТЕГОРИЯХ ВОЙНЫ

Лабуш Николай Сергеевич
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: ns_labush@mail.ru

Аннотация: Статья посвящена концептуализации понятия «война» применительно к проблеме противоборства между государствами в современном мире, характеристике войн различного характера и уровня.

Ключевые слова: массмедийные войны; средства воздействия; информационные войны; медиаметрия.

TO THE QUESTION ABOUT INFORMATION COUNTER-FIGHTING IN THE CATEGORIES OF WAR

Labush Nikolay
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: ns_labush@mail.ru

Abstract. The article is devoted to the conceptualization of the concept of "war" in relation to the problem of confrontation between states in the modern world, the characteristics of wars of different nature and level.

Keywords: mass media wars; means of influence; information wars; mediametry.

Введение. Борьба между государствами – явление характерное для всех этапов общественного развития, охватывающая все его сферы и принимающая различные формы. В политической сфере эти отношения носят наиболее острый характер и протекают преимущественно в виде войн разнообразного характера и уровня (международные, внутренние, коалиционные, мировые, региональные, религиозные, гражданские и т. д.).

Конвенциональная (обычная) война настолько прочно заняла место в арсенале средств международных отношений, что даже в относительно цивилизованное время коллективный разум ООН не смог запретить ее как орудия внешней политики национальных государств, а ученым – классифицировать войны по признакам агрессивности, справедливости из-за полярности позиций государств и расхождения национальных интересов. А политики, используя «двойные стандарты», маневрируя между интересами и потребностями правящих классов государств, манипулируют общественным мнением при вынесении вердиктов современным международным конфликтам и их результатам.

Вместе с тем, развитие военного дела все больше и больше вовлекало в вооруженное соперничество все другие составляющие общественной жизни. Экономика, политика, дипломатия и даже культура не только работали на военную машину, но и соперничество в этих областях приобретало самостоятельный характер и по результатам в достижении целей сравним с победой в войне. Недаром в XX1 в. противоборства государств (политических сил) в широкой литературе стало носить названия сопряженное с войной – экономическая война, дипломатическая война. Использование категории «война» стало настолько удобным для обозначения решительного, переломного воздействия на оппонента (противника), его последствий, что появились «нефтяные войны», «тресковые войны», «дорожные войны» и т. д.

Несомненно, помощью войны было возможным достичь намеченной цели быстро, эффективно, но опасно и с непредсказуемыми последствиями. Победы часто оказывались «пирровыми». Но достичь победы над оппонентом/врагом стало возможными с помощью иных, не военных средств. Несомненно, что военная мощь в том или ином виде будет использована – потенциально, или в прямом предназначении на завершающем этапе. Но значительная ставка делается на другие компоненты. В частности, на информацию.

Информация всегда использовалась в военных целях, как и любое социальное действие не обходится без нее. Но одно дело – использование информационных свойств как характеристики и атрибутивного свойства материи, но другое – как самостоятельное средство воздействия на волю и сознание противника, орудие информационной войны.

Говоря о первом варианте, некоторые ученые утверждают о появлении информационных войн чуть ли не с первых шагов человечества и борьбы за существование. Да, действительно, информация использовалась для управления войсками, руководства боевыми действиями, обмана противника и введения его в заблуждение, для формирования боевого духа своих войск и разложения противника. Но совсем иное, когда информация становится самостоятельным средством воздействия для достижения победы. А уж тем более, когда меняются все основные координаты и параметры этого воздействия. Задействуется информация, создаваемая средствами массовой информации, а значит, объектом воздействия становиться массовая аудитория и не только в виде войск противника, но и весь социум. И это приводит к принципиальным особенностям применения информации как орудия воздействия на противника не только для подавления его воля в ходе войны, но и для переформатирования его менталитета, навязывания чуждых ценностей. Производится «обезболивание» внесения чуждых идей и взглядов, они воспринимаются как добровольное согласие с ними. Разработан целый арсенал приемов и способов воздействия на противника.

Если при конвенциональных войнах информационное сопровождение осуществляется преимущественно во время боевых действий, то информационные войны характерны и для мирного, и для военного периода, когда

и завершается противоборство победой одной из сторон. Оба эти явления «сближает» категория «гибридная война».

Современное понимание информационной войны стирает грань фронта и тыла. Более того, для внешнего успеха в первую очередь необходимо обеспечить успех по «внутреннему контуру». Данная закономерность была характерна и для конвенциональных войн, но в них она носила иной характер, который объясняется изменением динамических свойств социальной информации, изменением роли идеологической (мотивационной), составляющей в информационном обеспечении боевых действий.

Отличает информационную войну от обычного (традиционно характерного для борьбы государств на международной арене) информационного воздействия друг на друга его интенсивность и степень ожесточенности. К сожалению, медиаметрия по этому аспекту весьма слабая и может лишь предложить выявлять степень агрессивности, которая в значительной степени субъективна [3].

Информационная война характеризуется и чисто формальными признаками, к которым можно отнести объявление о ее начале и завершении. Как еще по-иному можно объяснить факт празднования Соединенными Штатами победы в «холодной» войне, или объявление России теми же США и Украиной врагом [1].

Роднят обычную (конвенциональную) и информационную войну не только содержательные признаки, но и формальные, в частности терминология. Исследуя информационную войну, ученые использую такие понятия, как «фронт», «тыл», «кампания», «орудие», «атаки», «враг» и т. д.

Несколько ранее ученые основной акцент делали на психологической, моральной, идеологической стороне процесса использования массовой информации в военных целях. Поэтому и разработки были посвящены идеологической войне, психологической, морально-психологической. Поля научного исследования здесь не только близки, но они и пересекаются.

Информационно-психологическая безопасность – атрибут как конвенциональной (обычной) войны [2], так и собственно информационной. Причем при последней, в двух вариантах, как организационно-технической (кибервойны), так и собственно гуманитарной. К сожалению, некоторые ученые гуманитарного профиля «приватизируют» исследование данного феномена, не разделяя организационно-технические и морально-психологические (гуманитарные) аспекты, считают свои аспекты приоритетными.

Заключение. На наш взгляд, то явление, которое возникает как результат целенаправленного, массированного воздействия массовой информации на волю, сознание и психику населения и войска противникам как в мирное, так и военное время с целью достижения политических целей целесообразно было бы именовать массмедийной войной.

СПИСОК ЛИТЕРАТУРЫ

1. Глава Госдепа США назвал Россию врагом Соединенных Штатов // Военное обозрение. 2020. 19 декабря. URL: https://topwar.ru/178311-glava-gosdepa-ssha-nazval-rossiju-vragom-soedinennyh-shtatov.html
2. Митрофанов А. Какой она может быть? Сценарии конвенциональной войны // Военное обозрение. 2020.12 августа. IRL: https://topwar.ru/173967-kakoj-ona-mozhet-byt-scenarii-konvencionalnoj-vojny.html
3. Николайчук И.А. Политическая медиаметрия. Зарубежные СМИ и безопасность России: Моногр. Рос. ин-т стратег. исслед. – М.: РИСИ, 2015. – 230 с.

УДК 070

ПРОБЛЕМЫ СЕТЕВОЙ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ И МЕРЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ В УСЛОВИЯХ ЭПИДЕМИИ COVID-19

Ли Инин
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: yingyingli2701@outlook.com

Аннотация. В условиях эпидемии COVID-19 значительно увеличились сетевые слухи, утечки секретов и конфиденциальности, сетевое мошенничество и другие инциденты. Существуют искусственные причины, такие как поиск незаконных интересов, удовлетворение эгоистических потребностей и недостаточная грамотность в области сетевой информационной безопасности, а также объективные причины, такие как несовершенная система управления, несовершенный механизм управления ЧС и «лазейки» в технологиях безопасности. Необходимо принять соответствующие меры для скорейшего устранения недостатков информационной безопасности сети в ЧС.

Ключевые слова: эпидемия COVID-19; сетевая информационная безопасности; механизм управления чрезвычайными ситуациями.

PROBLEMS OF NETWORKED INFORMATION AND PSYCHOLOGICAL SECURITY AND COVID-19 THREAT CONTROL MEASURES

Li Yingying
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: yingyingli2701@outlook.com

Abstract. In the context of the epidemic COVID-19, network rumors, leaks of secrets and privacy, network fraud and other incidents with network information security have focused. There are artificial reasons, such as the search for illegal interests, the satisfaction of selfish needs and insufficient literacy in the field of network information security, as well as objective reasons, such as an imperfect management system, an imperfect emergency management mechanism and loopholes in security technologies. It is necessary to take appropriate measures to eliminate the shortcomings of the information security of the network in an emergency as soon as possible.

Keywords: the epidemic COVID-19; network information security; emergency management mechanism.

Введение. В начале 2020 г. разразилась эпидемия коронавируса. Распространение инфекции COVID-19 является первой в истории пандемией, в которой наблюдается массовое использование социальных сетей для обеспечения безопасности, информированности, продуктивности действий людей и поддержания связи между ними [2]. В то же время технологии, с помощью которых мы можем общаться и получать информацию, порождают и усиливают инфодемию, которая продолжает ослаблять глобальные ответные меры и угрожает сорвать усилия по борьбе с пандемией. Для эффективной борьбы с эпидемией и обеспечения безопасности общественного здоровья открытая и прозрачная информация стала хорошим лекарством от эпидемии [3]. Тем не менее, проблема сетевой информационной безопасности также приближается, выявляя недостатки в работе сетевой информационной безопасности в ЧС, что создает большие проблемы для работы по предотвращению и контролю эпидемий.

Результаты исследования проблемы. Во время эпидемии COVID-19 проявились некоторые типичные проблемы сетевой информационной безопасности. Некоторые пользователи сети намеренно распространяют слухи в интернете, проводят кибератаки и интернет-травлю, не считаясь с интересами других и общества. Мотивами этих действий становятся по психологические причины такие, как удовлетворение собственного гнева, ненависть к богатым, эпатаж, времяпрепровождение и так далее.

Клевета в интернете и подстрекательские речи.

Клевета в интернете является самым частым инцидентом в области кибербезопасности во время эпидемии COVID-19. Соответствующие сетевые платформы и авторитетные СМИ по всему миру своевременно распространяли бюллетени о клевете в интернете. По состоянию на 1 апреля 2020 г. более 1000 единиц информации о эпидемии COVID-19 были помечены как «ложные слухи» в «Китайском совместно-сетевом сайте для опровержения слухов». Различные слухи, сбивающие людей с толку, искажающие факты и разжигающие ненависть, оказывали крайне негативное влияние на аудиторию. В условиях инфодемии, мы склонны к стрессовым реакциям, таким как бессонница и сердцебиение.

Утечка личных данных и секретов.

Согласно сообщению китайского СМИ «Южный Метрополис Дейли», информационные документы, зарегистрированные на более чем 7000 людей, которые вернулись в Хубэй из других провинций внезапно были отправлены на социальные сети, такие как WeChat и Weibo. Содержание документов включали имена, фотографии, места работы, домашние адреса, номера мобильников и номера удостоверения личности. Многие из них даже получали спам-звонки и оскорбительные СМС. Они утверждали, что это заставляет их долгое время жить в страхе и неуверенности в себе. Разумеется, это не способствует развитию здоровой психики людей. Статистические отделы, занимающиеся этой информацией, включают органы контроля в сфере образования, общественной безопасности, уличные комитеты, квартальные комитеты жителей и т. д.

Электронные атаки с использованием сетевых вирусов.

Преступники с помощью психологического воздействия на общественность использовали кризис COVID-19 для проведения атак, используя социальную инженерию, а именно фишинг электронной почты посредством спам-ресурсов и более целенаправленных попыток вмешательства, таких как компрометация деловой электронной почты [4].

Интернет-травля.

Некоторые пользователи сети использовали анонимные учетные записи социальных программ в Интернете, и огульно критиковали других людей, оказывая на них психологическое давление. Например, некоторые артисты испытали на себе интернет-травлю во время эпидемии COVID-19. Даже их безосновательно обвиняли в том, что они не пожертвовали деньги или материальные ценности в сильно пострадавшие районы, и в том, что сумма пожертвования была слишком маленькой.

Происшествия информационной безопасности в дистанционном образовании.

Во время эпидемии COVID-19 школы проводили дистанционное образование и столкнулись с трудностями в области информационной безопасности. Учитель сделал неуместные замечания в классе, что привело к тому, что трансляция была запрещена. Тем более, утечка информации из платформы дистанционного образования стала серьезной уязвимостью. Оригинальные ресурсы на платформе дистанционного образования были незаконно присвоены, что является нарушением права интеллектуальной собственности. Это серьезно подрывало активность учителей в создании дистанционных образовательных ресурсов.

Таким образом, всевозможные слухи и ложная информация, вызывали социальную панику, увеличивали общественное психическое напряжение. Эти факторы стали значительным препятствием для согласованных усилий по борьбе с эпидемией COVID-19. Раскрытие конфиденциальной информации может привести к стигматизации и дискриминации соответствующих регионов и персонала и нарушить нормальную жизнь,

производство и социальный порядок. Электронные атаки с использованием сетевых вирусов могут привести к экономическим потерям, психологическому расстройству и нарушению соответствующих сетевых функций. Интернет-травля посягает на физическую и психическую безопасность определенных субъектов. Происшествия информационной безопасности в дистанционном образовании приведут к тому, что сетевое обучение не сможет проводиться нормально, и будут искажать среду обучения молодежи, угрожать физическому и психическому здоровью молодежи.

Проблемы сетевой информационной безопасности, выявленные в условиях эпидемии COVID-19, вызвали у людей тревогу. Мы должны глубоко задуматься и извлечь уроки, как можно скорее исправить недостатки и предотвратить повторение ЧС (чрезвычайные ситуации).

Совершенствование многоуровневой системы управления сетевой информационной безопасностью.

В условиях ЧС будут увеличивать случая созданной информационной безопасности. Все заинтересованные стороны сетевой информационной безопасности, которые включают правительственные ведомства, общественные организации и пользователей Интернета, должны дружно создать системы совместного управления сетевой информационной безопасностью, чтобы обеспечить безопасность всех видов конфиденциальной информации в чрезвычайных ситуациях. Кроме того, странам по всему миру следует сосредоточить внимание на укреплении построения верховенства закона для сетевой информационной безопасности [5]. И постоянно улучшать правовую систему сетевой информационной безопасности и усиливать борьбу с нарушениями и преступлениями в области сетевой информационной безопасности.

Усиление технического барьера сетевой информационной безопасности.

Соответствующие технические департаменты различных стран должны продолжать продвигать передовые технологические исследования и технологические инновации в области сетевой информационной безопасности, внедрять передовые технологии сетевой информационной безопасности, своевременно обновлять и модернизировать информационную инфраструктуру, функции терминального оборудования, сетевые информационные системы, аппаратные и программные системы платформ, усиливать проверку и тестирование технологии сетевой информационной безопасности, укреплять основы технологии сетевой информационной безопасности и создавать надежный «брандмауэр» технологии сетевой информационной безопасности.

Укрепление национального доверия к властям.

Инфодемия несет в себе немало опасностей. Она не только подвергает угрозе здоровье отдельных граждан, но и способна порождать ксенофобию, ненависть и отчуждение, которые в долгосрочной перспективе могут повлечь за собой последствия для общественного здоровья и для прав человека. Правительства, организации и правительства должны действовать открыто, стремясь к консенсусу и укрепляя общественное доверие, чтобы взять эту тенденцию под контроль. Это требует регулярного и открытого общения и динамичного партнерства [1].

В целом, сетевая информационная безопасность всегда была важной частью аварийного управления ЧС, и всегда играет важную и незаменимую роль. Существуют различные риски, аварии и опасности при ЧС и их управлении. Уточнение важной роли и характеристик работы по обеспечению сетевой информационной безопасности и повышение способности работы по сетевой информационной безопасности при ЧС являются важной частью улучшения национальной системы управления ЧС. Главное, что каждый из нас несет ответственность за распространение и поддержание надежной и обоснованной на фактах информации. Каждый нуждается в понимании, уважении и защите в цифровую эпоху [1].

СПИСОК ЛИТЕРАТУРЫ

1. Бороться с инфодемией вместе [Электронный ресурс] / Всемирная Организация Здравоохранения. URL: https://www.euro.who.int/ru/health-topics/Health-systems/digital-health/news/news/2020/6/working-together-to-tackle-the-infodemic (дата обращения: 29.06.2021).
2. Борьба с инфодемией на фоне пандемии COVID-19: поощрение ответственного поведения и уменьшение пагубного воздействия ложных сведений и дезинформации [Электронный ресурс] / Всемирная Организация Здравоохранения. URL: https://www.who.int/ru/news/item/23-09-2020-managing-the-covid-19-infodemicpromoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation (дата обращения: 01.03.2021).
3. Лян Л. Открытая и прозрачная информация – хорошее лекарство от «эпидемии» [N]. / Л. Лян // Economic Daily. 2020-02-22: 2.
4. Спекуляция пандемией, как преступники используют кризис COVID-19. [Электронный ресурс] URL: https://xn--b1aew.xn--p1ai/upload/site1/folder_page/019/882/802/Evropol_Spekulyatsiya_pandemiey1.pdf (дата обращения: 07.04.2021).
5. Цзюньён С. Исследование верховенства закона в безопасности информационных сетей с точки зрения общей концепции национальной безопасности. / С. Цзюньён, М. Дахуам. // Безопасность киберпространства. – 2019. – № 5. – С. 7-11.

УДК 004.05.5

КОММУНИКАЦИОННЫЕ СТРАТЕГИИ МЕДИАИСКУССТВА В УСЛОВИЯХ ГЛОБАЛЬНОЙ ПАНДЕМИИ

Марьина Людмила Петровна
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: lmarjina@mail.ru

Аннотация. В статье рассматриваются коммуникативные стратегии медиаискусства, обеспечивающие психологическую безопасность деятелей искусства и массовой аудитории в период глобальной пандемии.

Коммуникативные стратегии направлены на цифровизацию искусства, создание креативных социальных проектов, изменение редакционной политики изданий в контексте психологической безопасности.

Ключевые слова: культурные коммуникации; креативные проекты; медиаискусство; психологическая безопасность; цифровое искусство.

STRATEGIES OF RELIGIOUS-POLITICAL MASS MEDIA IN THE WAR OF CIVILIZATIONS AND MEANINGS

Marjina Ludmila
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: lmarjina@mail.ru

Abstract. The article examines the communication strategies of media art that ensure the psychological safety of artists and the mass audience during the global pandemic. Communication strategies are aimed at digitalizing art, creating creative social projects, changing the editorial policy of publications in the context of psychological safety.

Keywords: cultural communication; creative projects; media art; psychological safety; digital art.

Введение. Современное искусство непосредственно связано с медиасферой, что и послужило причиной возникновения новых тенденций его репрезентации в массмедиа, принципов коммуникации с аудиторией, психологической составляющей диалогичности медиаискусства. Безусловно, главные трансформации связаны с технологическим оснащением, которое сегодня привносит в произведение искусства новые смыслы [1]. Именно антропологический подход осмысления ценностного потенциала современного общества позволяет оценить изменения коммуникаций, тенденцию к виртуализации повседневной жизни [2]. Понимание сути социокультурной динамики помогло нам изучить процессы, которые привели к синтезу медиа, искусства и технологий, к становлению медиаискусства как феномена психологической безопасности в условиях кризисных явлений, таких как глобальная пандемия коронавируса. В свою очередь, под медиаискусством принято понимать совершенно новую форму искусства, возникающую под влиянием времени как экспериментальная художественная практика, в которой применяются медиасредства и медиатехнологии. По этой причине исследовательский интерес вызывает, в первую очередь, процесс цифровизации искусства, а во вторую – репрезентация объектов искусства в массмедиа и виртуальные коммуникационные стратегии. Эмпирической базой исследования послужили публикации специализированных и досуговых изданий Vogue, Harper's Bazaar и The New Yorker за январь 2020 – март 2021 гг., что частично совпало с временем глобальной пандемии коронавируса и локдауна. Это позволило выявить основные аспекты функционирования современных печатных медиа в актуальном социокультурном контексте, охарактеризовать направления редакционной политики по обеспечению психологической безопасности деятелей искусства, аудитории, журналистов. Также мы изучили процесс цифровизации искусства и его синтезирования с передовыми технологическими новшествами при помощи анализа работ художников Дианы Бургойн, Нам Джун Пайка и Билла Виолы в области синтетического искусства, мультимедийных проектов Эрмитажа, Лувра, Лондонской Национальной галереи, Пушкинского музея, Третьяковской галереи, музеев Пия-Климента и Кьярамонти, галерей Tate Britain и Tate Modern, Лондонского симфонического оркестра, технологии Motion Capture в кинематографе и примеров урбанистического медиаискусства в архитектуре и ландшафтном дизайне от компании Art + Com Studios и криейторов Питера Марино, Жана-Марка Гади. Прослеживая тематику основных статей, публикуемых в журналах во время пандемии, можно отметить лозунг "We all in this together" («Мы все вместе в этом») как побуждение аудитории к тотальному объединению перед лицом общей проблемы на протяжении прошлого и текущего годов: "How Fashion And Beauty Companies Are Giving Back During The Pandemic" («Как компании, связанные с красотой и модой, отдают в период пандемии»), "Mutual Aid Groups Supported Communities When the Government Wouldn't" («Группы взаимопомощи поддерживали общины, когда правительство не стало»), "Bulgari Sponsors COVID-19 Research Fellowships at The Rockefeller University" («Bulgari спонсирует исследования в области COVID-19 в Рокфеллеровском университете»), "The Virus, the Vaccine, and the Dark Side of Wellness" («Вирус, вакцина и тёмная сторона благополучия»), "What a Year Off from My Beauty Routine Taught Me About Aging" («Чему год без привычной бьюти-рутины научил меня о старении»). Таким образом, тематика изданий посвящена личному опыту переживания эпидемии, осмыслению коронавируса как явления, которое навсегда изменило жизнь каждого читателя журнала. Период глобальной пандемии коронавируса показал фундаментальную трансформацию в области искусства и массмедиа, которая привела к их более интенсивному сотрудничеству за прошедший год. Это взаимодействие способствовало созданию креативных социальных проектов и материалов, направленных на освещение важных событий, происходящих в мире: героизму врачей и людей других профессий, работавших на протяжении пандемии в тяжёлых условиях и подвергавших свою жизнь ежедневной опасности. Так, во время пандемии Bomb опубликовал на своём сайте список жизненно важных ресурсов для всех художников, который включил в себя адреса сайтов для самопроверки на предмет заражения коронавирусом, контакты фондов, помогающих темнокожим, квир, латиноамериканским авторам, художникам, фрилансерам. Также среди ресурсов значатся ссылки на гранты, бесплатные ресурсы для помощи в работе творцов. Изменяется редакционная политика анализируемых изданий в сторону обеспечения психологической безопасности: 1. Освещение остросоциальных тем коронавируса. 2. Поддержание надежды и призывы ко всеобщему объединению в непростые времена. 3. Сотрудничество с художниками через создание ярких и запоминающихся визуальных образов и

обложек. 4. Создание профильных платформ, посвящённых культурной жизни мирового сообщества в новой, изменённой коронавирусной реальности. К примеру, онлайн-платформа Kooness выпустила несколько важных постов – в частности, о том, как творцы со всего света сумели сплотиться и направить своё творчество на благо общества. Благодаря деятельности этих людей появился проект The Covid Art Museum – своеобразное творческое объединение художников, авторов и дизайнеров из разных уголков мира, которые смогли создать атмосферу постоянной поддержки в своих блогах и распространить жизненно важную информацию об изоляции, мерах предосторожности во время борьбы с инфекцией, банальном мытье рук и прочем. Все эти элементы так или иначе отразились в их творчестве, что в дальнейшем сопутствовало повышению востребованности и популярности объединения, призванного поддержать авторов и расширить их аудиторию. Новых членов координаторы искали при помощи хэштега #CovidArtMuseum в социальных сетях (преимущественно, в Инстаграмме), а главной задачей проекта стало впоследствии собрать настоящую физическую выставку и выпустить бесплатную электронную книгу со всеми работами участников, выпущенными за период пандемии. В статье были отмечены работы таких художников, как Хуан Деклан, Хавьер Хаэн, Сара Шакил, Франческо Феццоли, Ева и Марта Ярца (Yarza Twins), а также Хорге Табанера Редондо [3]. Многие досуговые, лайфстайл и модные издания ввели в свою ежегодную практику специальные тематические номера, полностью посвящённые искусству, а также стали периодически сотрудничать с популярными или малоизвестными, но талантливыми современными художниками. Такая совместная работа чаще всего приводит к созданию эксклюзивных и уникальных обложек номеров, как правило, приуроченных к какому-либо событию. Символично, что Vogue впервые за историю существования журнала решил объединить все свои 26 выпусков единой тематикой – надежда («hope»). Международный греческий художник Димитрис Папайоанну изображает лицо надежды на обложке первого номера Vogue Greece September и считает, что, если бы надежда была человеком, у неё не было бы определенного пола, цвета кожи или возраста. Стоит отметить, что этот же символ надежды выбрала для тематической обложки и редакция российской версии журнала Vogue. На ней представлена работа известного художника Эрика Булатова в стиле соц-арт. Издания и зарубежные, и отечественные вселяют в своих читателей надежду на лучшие времена, создают психологический комфорт.

Выводы. Период глобальной пандемии коронавируса показал фундаментальную трансформацию в области искусства и массмедиа. Тотальный локдаун простимулировал арт-среду быстрее и глубже уйти в цифровое пространство, в результате чего на свет появилось множество креативных проектов, направленных как на индивидуальную помощь самим художникам, так и на популяризацию музеев мира, симфонических оркестров, картинных галерей. Медиаискусство активно участвует в социокультурных коммуникациях. Важно отметить, что в периоды общественных потрясений, каким стала пандемия Covid-19, усиливается направленность коммуникационных стратегий на обеспечение психологической безопасности общества. Подтверждается гипотеза о том, что массмедиа являются важной и неотъемлемой частью массовой культуры и наделены не только функциями репрезентации и популяризации искусства, но также активно участвуют в социокультурных коммуникациях, осмыслении важных общественных событий.

СПИСОК ЛИТЕРАТУРЫ

1. Максунова А. А. Понятие современного искусства: определение, социальные институты, направления // Вестник научной ассоциации студентов и аспирантов исторического факультета Пермского государственного гуманитарно-педагогического университета. Серия Studis historica juvenum. Пермь, 2018. С. 315.
2. Мельник Г.С., Мисонжников Б.Я. Антропология медиапространства в поисках ценностных ориентиров. // Глобализация: на грани реального и виртуального. Коллективная монография / отв. ред. Н. А. Баранов. – СПб: ООО «Геополитика и безопасность», ИД «ПЕТРОПОЛИС», 2020. – 292 с. С. 170- 200.
3. Even during COVID-19, art “brings us closer together than ever” // Kooness. [Электронный ресурс]. URL: https://www.kooness.com/posts/magazine/art-in-the-time-of-corona (дата обращения: 30.03.2021)

УДК 070; 004.05.5

ВАКЦИННЫЕ ВОЙНЫ В МЕДИА КАК ФАКТОР УГРОЗЫ ИНФОРМАЦИННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ

Мельник Галина Сергеевна
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: melnik.gs@gmail.com

Аннотация. В статье анализируются причины и последствия «вакцинных» войн на международной арене и внутри государства, негативное влияние СМИ, провоцирующих фобии в отношении вакцинации в России, разрушающих социальную поддержку властей.

Ключевые слова: СМИ; когнитивная безопасность; вакцинация; вакцинные войны; медиавоздействия.

VACCINE WARS IN MEDIA AS A THREAT FACTOR OF INFORMATION AND PSYCHOLOGICAL SECURITY IN RUSSIA

Melnik Galina
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: melnik.gs@gmail.com

Abstract. The article analyzes the causes and consequences of "vaccine" wars in the international arena and within the state, the negative impact of the media, provoking phobias in relation to the vaccination campaign in Russia, destroying the social support of the authorities.

Keywords: media; cognitive safety vaccination; vaccine wars; media exposure.

Введение. Вакцинную войну называют первым грандиозным геополитическим сражением XXI в. Как показывает анализ массива дискурсов о COVID-19, вакцинация в них рассматривается как разновидность войны, разворачивающейся на двух уровнях – межгосударственном и внутреннем. Президент Франции Эммануэль Макрон заявил, что Европа столкнулась с «мировой войной нового типа», связывая при этом ситуацию со «стремлениями России и Китая оказать влияние с помощью вакцин» (URL: khttps://news.rambler.ru/politics/46485509-zaharova-rasskazala-o-vaktsinnoy-voyne-evropy-s-rossiey/).

Результаты исследования. Информационный портал Российского института международных политических и экономических стратегий (Russtrat) ежедневно размещает на своих ресурсах аналитические материалы, подтверждающие усилия объединенного Западного мира не допустить на рынок российские вакцины. Огромные масштабы приобретают попытки скомпрометировать производителей страны, а бездоказательные обвинения о вредности этих вакцин идут от авторитетных изданий и мировых агентств – Reuters, же Deutsche Welle, The Bell, журнала Der Spiegel. Однако, подтверждая свой образ передового государства, Россия использует пропаганду вакцины «Спутник V» как «мягкую силу». В материалах на портале Russtrat определяются перспективные цели России: «Покажем всем, кто здесь главный – гиперзвук, вакцина, нейронный интерфейс человека и машины, квантовый компьютер – вот новые имена наших побед, о которых будет знать весь мир» [4].

На внешнем контуре информационной войны вокруг вакцины намечен переворот: ряд западных медиа начинают признавать эффективность и безопасность российской вакцины (медицинская газета The Lancet, «Радио Свобода. Европа»), благодаря чему наблюдается рост стран, желающих приобрести вакцину для своего населения.

Вакцинная война разворачивается на экономическом, политическом и социальном поле; усиливается противостояние фармацевтических гигантов и государств-производителей вакцин. Наблюдается рост фармакологического рынка в мире – в Америке в 2020 г. он достиг 530 млрд долл., а Азиатско-Тихоокеанский рынок оценивается в более чем в 300 млрд. [2].

Так, медийные атаки против AstraZeneca нанесли ей сокрушительный удар: применение вакцины было остановлено в Дании, Норвегии, Исландии, Нидерландах, Австрии, Дании, Эстонии, Латвии, Литве, Болгарии, Ирландии, Люксембурге, Германии, Франции, Италии, Испании, Словении, Португалии, Кипре и ряде других стран [2].

Информационный рынок наполнился ложными данными и дезинформацией, о чем свидетельствуют заявления пресс-секретаря Белого дома и пресс-секретаря президента России о недопустимости политизации темы вакцин и ведении информационных войн на этой почве. Спецслужбы США вычисляют «вредных агентов» влияния, в их числе называются малоизвестные в России медиаресурсы – News Front, New Eastern Outlook, Oriental Review, Rebel Inside, якобы контролируемые ФСБ, которые ведут антипропропаганду (Первая мировая вакцинная война. Вечерняя Москва. 2021. 16 марта). Конкуренция вакцин ведется и внутри Западного мира. ЕС оплатила миллионы доз компаниям Pfizer и AstraZeneca. В интервью германскому изданию Sueddeutsche Zeitung Билл Гейтс озвучил сумму вложений его фонда в вакцину от коронавируса – 1,7 млрд долларов (Süddeutsche Zeitung, 2021. 27 Jaguar). Книга, написанная им в соавторстве с Тьерри Мальре (2020 г.) «COVID-19. Великая перезагрузка», ставшая манифестом глобалистов, породила в прессе огромное количество футуристических прогнозов. Муссируется тема искусственности происхождения вируса, который рассматривается как биологическое оружие для проведения масштабного социального эксперимента (чипирования) с целью изменения управления глобальным обществом и перехода к модели цифрового либерального тоталитаризма. Так, в статье Елены Паниной, опубликованной на портале Regnum, находим утверждение: «имеющиеся сегодня данные позволяют предположить, что COVID-19 имеет искусственное англо-американское происхождение, а его утечка была организована в интересах глубинных элит Британии и США, ищущих выхода из отработанной модели сохранения мирового господства» [3]. Выдвигаются идеи распада общего мира на изолированные кластеры, распад Евросоюза и НАТО; ставится под сомнение устойчивость демократических режимов, находятся аргументы в пользу того, что эффективность патерналистских обществ и государств выше демократических.

В экономическом плане предлагается идея тотального сноса финансовой мировой системы; в военном (под предлогом коронавируса США) – наращивания военного присутствия на Балканах и в Европе, вытеснение Германиия из словенского стратегического плацдарма.

Пандемия коронавируса дает возможность разного рода аналитикам и экспертам, используя теории мирового заговора, публично высказывать ключевую идею необходимости глобального изменения (передела) мира. А испытание COVID-19 – считать системой тестирования на предмет жизнестойкости всех государственных структур, начиная со здравоохранения [8].

Второй вакцинный фронт разворачивается внутри России. Медиа и социальные сети наводняются страшными историями, связанными с вакцинацией. Только за одну неделю июля 2021 г. популярный информационный портал «Царьград» разместил более 20 публикаций и видеосюжетов с устрашающими заголовками, направленными против вакцинации («”Вот Вам и прививка”: признание властей Петербурга вызвало панику» (Общество 29.07.2021); «Чиновник не побоялся сказать правду о смертях среди вакцинированных в

России» (Вакцина правды 29.07.2021); «Вакцина от ковида не работает: Тестировавшие препарат в России обратились к Путину» (Политика 27.07.2021); «Такого честного признания о вакцинации еще не было: тысячи людей стали жертвами двух роковых ошибок» (Вакцина правды 29.07.2021), «Жидкий чип»: профессор раскрыл всю правду о вакцине» (21.07.2021); «Врач пошел против вакцинации от коронавируса» (Вакцина правды 29.07.2021); «Даже полная вакцинация не гарантирует выживание: Неудобный факт вскрыл питерский чиновник (Общество 29.07.2021); «Чиновнику, призвавшему вакцинировать людей как баранов, ответили медики: «Лучше бы не раскрывал рот» (Общество 29.07.2021); «Врачи против вакцинации – 1: об эффективности, качестве, опасности» (Расследования Царьграда 29.07.2021); «Миф о безвредности вакцин решительно разрушил русский профессор: «Это вранье» (Вакцина правды 27.07.2021); «Вот Вам и прививка»: признание властей Петербурга вызвало панику (Общество 29.07.2021) и др. В медийных материалах подрываются основы государственной политики России, направленной на преодоление эпидемии. Нередко факты либо преувеличены, либо искажены, а ссылки на авторитеты подогревают напряженность в обществе, ведут к расколу порождают различные фобии. В самом содержании текстов нет жестких аргументов против вакцинации. Профессор и чиновник, на которых есть ссылка в публикациях, говорят лишь о том, что у 5 % населения есть противопоказания против вакцинации, а умирают люди из-за серьезных сопутствующих коронавирусу болезней. Но заголовки безапелляционны и безальтернативны. Мощная антивакцинная кампания дискредитирует предпринимаемые в области здравоохранения меры. Вопросы вакцинации связываются в медиа с проблемой свободы выбора гражданина. Медиа не ограничиваются информированием населения в вопросах вакцинации, а становятся организационными центрами для проведения публичных акций протеста против вакцинации. Так, широко разрекламированы экспертные заключения некой независимой ассоциации врачей, утверждающих, что прививки – это «эксперимент и политическое действо», а «вакцины являются опасными для здоровья человека и абсолютно бесполезны для профилактики коронавирусных инфекций, и при этом вызывают тяжёлые аутоиммунные патологии» [5].

Вместе с тем, журналистские расследования показывают заказной характер статей и акций, заявлений не зарегистрированной так называемой независимой Ассоциации врачей [7]. Не имеющие специализированного образования врачи дают в медиа и социальных сетях неквалифицированные заключения о воздействии негативных свойств вакцины на человека. Обязательная вакцинация от коронавируса спровоцировала активность движения антипрививочников. «Часть из них объединили вокруг себя сторонники находящейся в международном розыске самарской Лады-Русь. Она возглавляла местный Центр народной медицины “Путь к Солнцу”, “Академию развития Светланы Пеуновой” и собственную политическую партию “Воля”, которую суд ликвидировал в 2016 году за экстремистскую деятельность» [5].

Анализ смыслового и эмоционально-экспрессивного содержания текста показал, что и «Новая газета» открыла кампанию против вакцины «ЭпиВАкКорона» публикацией спецкора Ирины Тумаковой «Операция “Э”» (2021. 4 июля). Результат потока противоречивой информации: «одна половина страны готова пережить очередной локдаун, только бы не прививаться, а другая скоро начнет отлавливать и бить антипрививочников» [5]. Противостояние достигло высокой степени напряжения.

Проблемы вакцинации завязываются на политические задачи оппозиционных групп, направленных на дискредитацию власти. В прессе делаются громкие заявления: «Россия погрузилась в совершенно новую реальность. Собянин и чиновники Роспотребнадзора захватили тоталитарную власть в стране, отменив Конституцию, законы, законодательную власть, под предлогом заботы о здоровье населения...» [5].

Сама постановка проблемы вакцинации ставит людей по обе стороны баррикад. В лидах текстов обозначаются линии раскола общества. «Пандемия спутала систему координат политических партий в России. Тем временем общество ждет от политиков четкой позиции по вопросам вакцинации и борьбы с инфекцией. Против кого на выборах в Госдуму сыграет коронавирус, а кто сможет привлечь новых сторонников из среды ковид-диссидентов и ковид-лоялистов?» [1].

Заключение. В совокупности подобные публикации формируют у аудитории негативные установки в отношении не только вакцинации, но и государства, которое последовательно проводит прививочную кампанию, а также подрывают социальную опору власти. Государственная пропаганда нередко проигрывает в вакцинной войне.

Исследование выполнено при поддержке РФФИ «Медиаобраз России в контексте национальной безопасности», №19-013-00725 2021.

СПИСОК ЛИТЕРАТУРЫ

1. Коронавирус поставил политиков в замешательство. URL: https://novorossiia.info/koronavirys-postavil-politikov-v-zameshatelstvo/
2. Ненароков П., Иванов А. Война вакцин и игры фармацевтов. URL: 30 мая 2021 https://topwar.ru/183416-vojna-vakcin-i-igry-farmacevtov.html
3. Панина Е. Битва за коронавирус или проверка боем // ИА REGNUM. URL: https://regnum.ru/news/2955808.html
4. «Спутник V» как пример эффективности российской «мягкой силы». 2021. 12 февраля. URL:https://russtrat.ru/comments/26-fevralya-2021-0010-3262
5. Ульянов, А. Вакцина ненависти: Чиновники толкают народ к прививочной войне https://ekb.tsargrad.tv/experts/antivakcinnaja-grazhdanskaja-vojna-zachem-chinovniki-raskachivajut-narod_380434 //
6. Цыганов А. 2021. 28 июня. Обязательная вакцинация как инструмент госпереворота в России. URL: http://путин.ru-an.info/новости/обязательная-вакцинация-как-инструмент-госпереворота-в-россии/
7. «Это геноцид, фашизм и эвтаназия»: как антпрививочники стали ядром сомнительного политического движения. URL: https://www.fontanka.ru/.
8. Matthew Lynn. Vaccine wars: the global battle for a precious resource // The Spectator (Великобритания). 30.01.2021.

УДК 004

РЕЛИГИОЗНЫЙ ЭКСТРЕМИЗМ КАК СРЕДСТВО ПОЛИТИКО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ

Мисонжников Борис Яковлевич
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: misonzhnikov.boris@gmail.com

Аннотация. Рассматриваются механизмы формирования идеологии религиозного экстремизма и его роль в борьбе с христианством. Исследуются факты фальшивого происхождения манускрипта «Хроника Ура Линда», роль секты свидетели Иеговы в осуществлении нацистской политики. Доказывается необходимость современного критического отношения к попыткам подмены христианства псевдорелигией.

Ключевые слова: религиозный экстремизм; языческая ариософия; «Хроника Ура Линда»; свидетели Иеговы.

RELIGIOUS EXTREMISM AS A MEANS OF POLITICAL AND PSYCHOLOGICAL INFLUENCE

Misonzhnikov Boris
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: misonzhnikov.boris@gmail.com

Abstract. The mechanisms of the formation of the ideology of religious extremism and its role in the fight against Christianity are considered. The facts of the false origin of the "Chronicle of Ur Linda" manuscript, the role of the Jehovah's Witnesses sect in the implementation of Nazi policy are investigated. The necessity of a modern critical attitude towards attempts to substitute pseudo-religion for Christianity is proved.

Keywords: religious extremism; pagan ariosophy; Chronicle of Ur Linda; Jehovah's Witnesses.

Введение. Религия как сфера духовной жизни, обращенная к самым сокровенным и глубоким сторонам существования человека, всегда становилась предметом обостренного внимания в политическом противостоянии. В XX веке использование религиозной идеологии в корыстных целях стало особенно изощренным и беспринципным, причем этот процесс обрел системные признаки и институционализировался, подчас принимая формы религиозного экстремизма. Возникла особая область крайнего напряжения и агрессии, ловкого и изобретательного манипулирования, и ее социальные, идеологические, психологические, организационные императивы требуют всестороннего изучения.

Объектом негативистского воздействия становятся традиционные авраамические религии, и с этой целью адепты религиозного экстремизма идут на любые ухищрения, подмену духовно-нравственных ценностей, подлог исторических документов. Так, во второй половине XIX века обретает известность якобы фризский манускрипт «Хроника Ура Линда» – религиозно-националистический и крайне евроцентрический текст, интерес к которому усиливается в определенные исторические периоды. В 1933 г. его публикует этнолог, теоретик и идеолог национал-социализма, руководитель оккультной организации «Аненербе» Г. Вирт. Это вызвало критику ряда специалистов. Подделку разоблачил А. Хюбнер, германист, член Прусской академии наук, причем и сам являвшийся сторонником национал-социализма. Он, в частности, отмечал: «Прежде всего, бумага рукописи, которая производит впечатление, что она из XIII века. Ее исследовали голландские и немецкие специалисты по материалам и пришли к единодушному мнению, что она едва ли старше 1850 года. Бумаге искусственно придали коричневый оттенок, по всей видимости, нанесением краски, поскольку на заломах она белая. Вне всякого сомнения, всех ждет разочарование» [5, S. 5]. Хюбнер называет создателя рукописи «фальсификатором», не без иронии говорит о том, что Вральда, центральная фигура, «самый старый по возрасту, старее всех, потому что он – это все вещи» [5, S. 19].

Несмотря на разоблачение, этот «документ» стал основой этнократического мифа Третьего рейха, провозгласившего превосходство «нордической расы» и отрицающего христианство. Протестантский теолог, профессор и библеист Э. Хэнхен писал: «Борьба против христианской веры обрела новое лицо. Отныне не довольствуются тем, чтобы критиковать христианские законы; потому что заметили: простое отрицание не приносит плодов» [3, S. 250]. Хэнхен очень точно определяет это явление как «эрзац веры», но общество без веры существовать не может, и на смену традиционной религии приходит религия другая, в основе которой лежат принципы дегуманизации.

Одним из самых яростных противников христианства стал рейхсфюрер СС Г. Гиммлер. Он называл христианство «величайшей чумой», с которой «надо покончить». Гиммлер обращался именно к «Хронике Ура Линда», на ней основывая свою веру: «Я сегодня на похоронах Гейдриха в своей речи преднамеренно выразил мое глубочайшее внутренне убеждение – веру в бога, веру в судьбу, в древних, в бога, как я его называю, и его можно выразить старинным германским словом – Вральда. Мы должны вновь в нашем народе обрести масштабы во всех начинаниях…» [2]. Казалось бы, все это уже в прошлом. Но языческая ариософия и в наше время находит почитателей, в том числе и в России, расовые архетипы вызывают интерес в контексте идей именно «Хроники Ура Линда», которая, кстати сказать, в 2007 г. была опубликована на русском языке, причем представленная в

редакции того же нациста Г. Вирта, которого А. Г. Дугин назвал «гениальным немецким профессором» [1]. Опубликованный перевод не был снабжен критическим научным комментарием, хотя критическая литература существует, в частности, достаточно серьезные работы И. В. Буккера, А. Е. Петрова, В. А. Шнирельмана, В. В. Эрлихмана.

Хотелось бы подчеркнуть: Гиммлер, один из высших чинов едва ли не самого зловещего режима, в своей ненависти к христианству создал, по сути, систему, направленную на уничтожение христианской веры. Это не только апологетика языческих мифов, но и поддержка экстремистских религиозных течений, существующих и ныне. Так, Гиммлер «занимался вопросом, который сводился к тому, как в психологическом аспекте использовать свидетелей Иеговы, прежде всего в борьбе против Советского Союза. Одной из самых главных забот Гиммлера было то, как после ожидаемой победы фашизма удерживать в низвергнутом положении огромную территорию Советского Союза и подавлять любое сопротивление, тем более восстание против нацистских оккупационных сил. Он вышел на приверженцев Общества сторожевой башни, на свидетелей Иеговы. Они в этом должны были играть одну из главных ролей» [4].

Заключение. Конечно, свидетели Иеговы нужны были Гиммлеру не только в решении его задачи разрушения Советского Союза. Идеи, а также нравственные, поведенческие максимы данной секты вписывались в антихристианскую идеологию, в формировании которой Гиммлер принимал самое активное участие.

Исследование выполнено при финансовой поддержке РФФИ: проект «Медиаобраз России в контексте национальной безопасности», №19-013-0072.

СПИСОК ЛИТЕРАТУРЫ

1. Дугин А. Г. К вопросу о русских рунах. URL: http://www.junik.lv/~time/dugin/index.htm.
2. Deutsche Geschichte in Dokumenten und Bildern. URL: https://ghdi.ghi-dc.org/sub_document.cfm?document_id=1573&language=german.
3. Haenchen E. Glaubensersatz? // Deutsche Theologie. 1934. Vol. 1. N 7. S. 250–263.
4. Hausler M. Himmlers Ideen leben weiter. Was hatte der «Reichsführer SS» Himmler mit den Zeugen Jehova vor. URL: http://www.manfred-gebhard.de/Urania9.pdf
5. Hübner A. Herman Wirth und die Ura-Linda-Chronik. Berlin; Leipzig: W. de Gruyter & Company, 1934. 40 S.

УДК 308; 316.6

К ВОПРОСУ О КЛАССИФИКАЦИИ ОБЪЕКТОВ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

Муминов Файзулла Абдуллаевич
Бухарский государственный университет
М. Икбола ул., 11, Бухара, 200114, Узбекистан
e-mail: famuminov@mail.ru

Аннотация. Статья посвящена проблеме классификации объектов информационно-психологической безопасности. Представлена концепция Республики Узбекистан.

Ключевые слова: информационно-психологическая безопасность; социальный институт; государство; негативная информация; аудитория.

TO THE QUESTION ABOUT THE CLASSIFICATION OF OBJECTS OF INFORMATION AND PSYCHOLOGICAL SECURITY

Muminov Faizulla
Bukhara State University
11 M. Ikbola St, Bukhara, 200114, Uzbekistan
e-mail: famuminov@mail.ru

Abstract. The article is devoted to the problem of classification of objects of information and psychological security. The concept of the Republic of Uzbekistan is presented.

Keywords: informational and psychological security; social institution; state; negative information; audience.

Введение. В качестве объектов информационно-психологической безопасности принято выделять личность, общество и государство. Такой подход свойственен двум документам стратегического характера – Концепции Национальной безопасности Российской Федерации и такого же документа, принятого в Республике Узбекистан. Исходя из их духа, становится ясно, что они были подготовлены под прямым руководством специалистов по государственной безопасности. В то же время значимость данного документа именно для общества не была принята в качестве ведущей их основы. Это видно хотя бы по тому, что общество и государство в глобальном плане (который соответствует подходу авторов концепций) близки между собой, тогда как в качестве объектов не выделены социальная группа и социальный институт. Данному вопросу и хотели бы мы посвятить настоящую статью.

Результаты исследования. Не будем не будем акцентировать внимание на том, верно ли выделение в качестве отдельных объектов и государства, и общества. На наш взгляд, было бы достаточно первого. Обратим внимание на то, что есть такие структуры как социальные группы и институт и следует ли выделить их в качестве

самостоятельных объектов информационно-психологической безопасности. Обратимся к толкованиям данных понятий.

«Группа общественная в социологии – в самом широком смысле, множество индивидов, связанных определенными отношениями… Формирование и распад, свойства, структура и поведение реальных групп общественных лучше изучены на формальных и неформальных малых группах. Группы возникают спонтанно или под влиянием внешних сил для достижения определенных целей. Приверженность группе рассматривается как наиболее базовый процесс, основанный на сравнении затрат и пользы от вхождения в группу. В возникшей группе начинают действовать силы, обеспечивающие единство взглядов и поведений…» [1, с. 245].

К сожалению, авторы не привели и не охарактеризовали бытующие в социологии малые (до 20 чел., см. произведения Джекоба Морено по микросоциологии [2]), средние (до 150 чел.) и большие группы (до 1500 чел.) Цифры, разумеется, условные и приводятся для общей оценки ситуации. К примеру, семья, которая насчитывает от 2 до 10-12 человек, является одним из главных социальных институтов любого общества, несмотря на столь малый ее размер [3]. Все зависит от социальной значимости данной группы. Но в целом данный подход общепринят и нет необходимости его пересматривать. Мы ставим другой вопрос – следует ли выделять группу в качестве отдельного объекта информационно-психологической безопасности?

Полагаем, что да, это необходимо. С группой нельзя работать теми же методами, что и с личностью или обществом, она имеет свои специфические особенности и параметры. Дело в том, что, во-первых, информация от членов группы распространяется по обществу с большой скоростью, особенно, если учитывать возможности современных информационных технологий, например, Telegram. Во-вторых, обилие информации вынуждает значительную часть аудитории ограничиваться небольшим (иногда одним) числом каналов информации (тот же Telegram.). Акцентировка в столь основополагающих документах внимания на индивиде и обществе (с пропуском группы) вынуждает специалистов обращать меньше внимания на специфику коммуникационной жизни социальных групп и их влияние на общественное мнение граждан государства. В-третьих, некоторые особые группы играют столь значительную роль, что игнорирование методов их функционирования в обществе может привести к немалым промахам в жизни любой страны.

Обратимся к социальным институтам. Здесь положение еще сложнее. «Социальный институт – относительно устойчивая форма организации социальной жизни, обеспечивающая устойчивость связей и отношений в рамках общества… Основные функции, которые выполняет социальный институт:

1) создает возможность членам этого института удовлетворять свои потребности и интересы;

2) регулирует действия членов общества в рамках социальных отношений;

3) обеспечивает устойчивость общественной жизни;

4) обеспечивает интеграцию стремлений, действий и интересов индивидов;

5) осуществляет социальный контроль.

Деятельность социального института определяется:

1) набором специфических социальных норм, регулирующих соответствующие типы поведения;

2) интеграцией его в социально-политическую, идеологическую, ценностную структуры общества, что позволяет узаконить формально-правовую основу деятельности;

3) наличием материальных средств и условий, обеспечивающих успешное выполнение нормативных предложений и осуществление социального контроля…

Успешное функционирование социального института связано с наличием в рамках института целостной системы стандартов поведения конкретных лиц в типичных ситуациях. Эти стандарты поведения нормативно урегулированы…

В зависимости от сферы действия и их функций социального института подразделяются на:

а) реляционные – определяющие ролевую структуру общества в системе отношений;

б) регулятивные, определяющие допустимые рамки независимых по отношению к нормам общества действий во имя личных целей и санкции, карающие за выход за эти рамки (сюда относятся все механизмы социального контроля);

в) культурные, связанные с идеологией, религией, искусством и т. д.;

г) интегративные, связанные с социальными ролями, ответственными за обеспечение интересов социальной общности как целого. Развитие социальной системы сводится к эволюции социальных институтов...” [1, с. 246].

Мы вынуждены воспроизвести определенную часть публикации из словаря, поскольку наша статья непосредственно адресована вышеупомянутым специалистам и требует доказательной базы. Насколько значимо для тех, кто занимается информационно-психологической обработкой населения, функционирование данных социальных институтов? Думаем, что ответ напрашивается сам собой. Это убедительно доказывается существованием тех социальных институтов, которые имеют службы внутренней безопасности (министерство внутренних дел, служба государственной безопасности и т.п.). Обработка негативной информацией служащих или предоставление данным институтам чрезмерно больших полномочий может привести к разложению в них дисциплины или к потере контроля государства над ними. Некоторые социальные институты часто играют роль государства в государстве. Примером этому может послужить служба безопасности бывшего СССР, возглавляемая в то время Лаврентием Берия.

Заключение. В приведенные выше государственные документы особой важности следует включить в качестве возможных объектов информационно-психологического воздействия социальные группу и социальный институт с переработкой положений этих концепций с учетом данных нововведений.

СПИСОК ЛИТЕРАТУРЫ

1. Коростелева Е.А. Социологический институт // Новейший социологический словарь / сост. А. А. Грицанов, В. Л. Абушенко, Г. М. Евелькин и др. – Мн.: Книжный Дом, 2010. – С. 245.
2. Социометрия Дж. Морено – методика, процедура, обработка результатов. Социограмма. URL:https://psyfactor.org/lib/sociometriya_moreno.htm
3. Пьянов, А.И. Социальный институт семьи как структурный и ценностно-нормативный компонент социума // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – 2011. №3(9). – С. 160-167. 2011. №3(9). – С. 160-167.

УДК 0.70; 159.99

СИМУЛЯКРЫ КАК СРЕДСТВО МАНИПУЛЯЦИИ: АСПЕКТ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

Олешко Владимир Федорович
Уральский федеральный университет имени первого Президента России Б.Н. Ельцина
Мира ул., 19, Екатеринбург, 620002, Россия
e-mail: vladimir.oleshko@urfu.ru

Аннотация. В условиях развития информационных технологий всё больше актуализируется проблематика реализации в системе медиаобразовательных технологий. А распространение в медийной практике фейк-симулякров, доказывает автор, предполагает рассмотрение данного рода контента не только в контексте этических противоречий и противодействий новейшего времени.

Ключевые слова: симулякр; фейк; манипуляция; информационно-психологическая безопасность.

SIMULACARS AS A MEANS OF MANIPULATION: ASPECT OF INFORMATION AND PSYCHOLOGICAL SECURITY

Oleshko Vladimir
Ural Federal University named after the first President of Russia B.N. Yeltsin
19 Mira St, Yekaterinburg, 620002, Russia
e-mail: vladimir.oleshko@urfu.ru

Abstract. In the context of the development of information technologies, the problem of implementation in the system of media education technologies is becoming more and more relevant. And the dissemination of fake simulacra in media practice, the author argues, presupposes the consideration of this kind of content not only in the context of ethical contradictions and oppositions of modern times.

Keywords: simulacrum; fake; manipulation; information and psychological security.

Введение. В массмедийной деятельности в информационную эпоху всё большую роль играют эмоции индивидов, которые являются одной из доминант восприятия мультимедийных текстов. Уже не просто реальный факт, а, к примеру, «оболочка» сенсационности или желаемой иллюзорности определяют его эффективность. Симулякр же как изображение без оригинала, репрезентация того, что на самом деле может и не существовать, имеют свойство рождаться, существовать и распространяться прежде всего при посредстве массмедиа, как раз в таких условиях.

Фальшивые новости и фейки можно назвать разновидностями симулякров. Именно благодаря искаженному отражению реальности они способны сформировать у индивида на уровне оперативной памяти абсолютно иное видение каких-то отдельных аспектов мира, нежели то, которое порой в течение десятилетий складывалось при посредстве как журналистики, так и других социальных институтов – прежде всего институтов семьи и образования. Проанализировав 18 публикаций массмедиа, вызвавших в 2020-2021 гг. широкий общественный резонанс, а также более 50 текстов их обсуждения в наиболее популярных социальных сетях, мы выявили ряд закономерностей, которые можно, на наш взгляд, характеризовать как системообразующие при манипулировании сознанием массовой аудиторией, и прежде всего молодёжи.

Сознание как «интегративный способ бытия человека, проявляющийся в способности человека осознавать условия и формы своей жизнедеятельности» [2: 10], определяет таким образом практические преобразования, осуществляемые, или которые могут быть осуществлены, отдельным индивидом и представителями тех или иных социумов в целом. Инфантилизм, свидетельствуют новейшие исследования социологов [1], характеризует, к сожалению, многих современных молодых людей. И как стиль жизни он реализуется всё чаще как раз под воздействием медиатекстов симулятивного характера. Получая основную часть информации из глобальной Сети, но не овладев при этом элементарными навыками медиаобразования [3] молодые люди всё чаще становятся объектами, наиболее уязвимыми для различных манипулятивных интенций. Приведём несколько примеров.

То, что в современной пропагандистской деятельности симулякры стали одним из наиболее распространенных орудий информационно-психологического воздействия, уже не является открытием. Причём

у наиболее образованной части молодёжи это может, как свидетельствуют данные ВЦИОМ, вызывать отторжение не только от текстов массмедиа политического характера, но и в целом подрывать авторитет отдельных властных структур или тех или иных лидеров и медийных персон (*URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/vliyanie-sredstv-massovoj-informaczii-na-politicheskie-vzglyady-rossiyan*).

Результаты. В телеграм-канале Артемия Лебедева в феврале 2021 г. был опубликован пост, подтверждающий наличие немецкого гражданства у жены Алексея Навального Юлии (*https://t.me/temablog/3949*). Для подтверждения данного факта, тут же как новость распространенного многими отечественными сетевыми изданиями, к записи была прикреплена фотография одного из документов, якобы выданного ещё в 2019 г. То, что это фотошоп, было легко проверить любому пользователю Twitter, просто загрузив фотографию удостоверения в поиск по изображениям Яндекса. Только после того, как пользователями было указано на данные действия, Лебедев дописал в публикацию: «UPD. Это фейк. Факт проверен». Другие СМИ не сделали даже этого.

Откровенная ложь, помноженная на политические амбиции, характеризовала симулятивную историю с так называемым «дворцом В.В. Путина в Сочи» в апреле 2021 г. Поскольку разоблачение технологии создания и реализации данного фейка уже широко освещено не только массмедиа, но и исследователями, лишь констатируем, что, как и в первом случае, неосторожные или умышленно предпринятые действия манипуляторов ничего, кроме, потери доверия и уважения к субъекту информационной деятельности в таком случае не приносят.

Хотя в некоторых случаях авторами явно предопределяется отнюдь не пассивное восприятие фейков или симулякров. В январе 2021 г., к примеру, в социальной сети TikTok появилось ныне удалённое видео о человеке, погибшем во время несанкционированной акции в России (*https://lenta.ru/news/2021/01/24/tiktok/*). В сюжете, якобы из больницы, был представлен снимок мужчины с перебинтованным носом, который авторы позиционировали как его последнее фото. Надписи под фото гласили: «Зверски убит оппозиционер», «После нападения на сотрудников полиции Виталий Цаль скончался в районной поликлинике». Авторы также просили аудиторию максимально распространить эту информацию. На деле же оказалось, что на снимке был изображен украинский стример Виталий Цаль (Папич). Фото в больнице было сделано в июне прошлого года, когда мужчине проводили плановую операцию на носу. Об этом сам Цаль рассказал в своем аккаунте в Instagram. В этой публикации умело был использован прием стереотипизации и деления на «своих» и «чужих» в удобной транскрипции.

Хотя в последнее время некоторые субъекты информационной деятельности активно используют такого рода манипулятивные приёмы для элементарной самопрезентации себя как авторов, для повышения рейтингов просмотров текстов и даже как элемент умело выстроенной маркетинговой кампании. В последнем случае можно привести историю о «девушках, умерших от коронавируса накануне фестиваля "Кинопроба"» в декабре 2020 г. Первоисточником этой псевдоновости являлась страница в социальной сети Facebook куратора фестиваля, шеф-редактора студии «Союзмультфильм» Сергея Капкова. Он тогда написал, что из 15 участников, которых допустили к защите в Петербурге анимационных проектов перед жюри, пятеро заразились коронавирусом. Из этих пятерых двое – 21-летняя Александра Грушина и 26-летняя Наталья Мальгина – умерли, а еще трое перестали выходить на связь. СМИ тут же растиражировали новость о том, что «коронавирус не щадит молодых». Например, об этом происшествии сообщило первым сетевое издание «Фонтанка», а далее – E1.RU, «Комсомольская правда» и ряд других. Оказалось, что это было дело рук некоего социального педагога, признавшегося позднее корреспонденту «Фонтанки» (*https://www.fontanka.ru/2020/12/09/69615261*), что он выдумал фамилии участников конкурса, скомпилировал биографии и даже представил «фото девушек». Но отправив один проект от своего имени, и еще один – от имени своего знакомого, тем самым добился того, что их заявки получили семь из десяти мест в шорт-листе анимационной секции фестиваля, а о них самих «узнали теперь все».

Заключение. Вместе с тем, во всех вышеописанных и ряде других проанализированных нами случаев против авторов не были применены меры правового воздействия. Но поскольку ложная информация тогда превращается в фейк-симулякр, когда авторы заведомо скрывают её ложность, искажая представление о реальности, а в некоторых обстоятельствах даже создавая гиперреальность, на наш взгляд, в медийной практике возникает необходимость рассматривать данного рода контент не только в контексте этических противоречий и противодействий новейшего времени.

Исследование выполнено в рамках гранта РНФ: проект № 19-18-00264 «Цифровизация коммуникативно-культурной памяти и проблемы её межпоколенческой трансляции».

СПИСОК ЛИТЕРАТУРЫ

1. Ардельянова Я. А. Факторы и условия инфантилизации современной молодёжи / Я. А. Ардельянова, Б. Ш. Саидов. // Теория и практика общественного развития. – 2018. – № 4. URL: https://doi.org/10.24158/tipor.2018.4.6.
2. Немов Р. С. Психология. Второе издание. – М.: «Просвещение», 1995. – 376 с.
3. Олешко В. Ф. Психологические особенности молодёжной аудитории медиа в контексте исследования пользовательских реакций / В.Ф. Олешко, О. С. Мухина О. С. // Материалы I Междунар. науч.-практ. конф. «Пользовательский контент в современной коммуникации» (ЧелГУ, 22–23 апреля 2021 г.). – Изд-во Челябинского ун-та, 2021. – 481 с.

УДК: 304.9; 009

BIG DATA VERSUS BIG KNOWLEDGES: АВЕРС И РЕВЕРС ЦИФРОВИЗАЦИИ ОБРАЗОВАНИЯ

Плебанек Ольга Васильевна
Университет при Межпарламентской Ассамблее ЕвАзЭС,
Смолячкова ул., 14/1, Санкт-Петербург, 194044, Россия
e-mail: plebanek@mail.ru

Аннотация. В статье анализируются положительные стороны цифровизации образования и связанные с ними риски, своевременная рефлексия которых и разработка адекватных образовательных технологий поможет избежать негативных тенденций в когнитивной и психологической сфере.

Ключевые слова: искусственный интеллект; клиповое мышление; псевдоинформация; on-line образование; self-образование; туторинг.

BIG DATA VERSUS BIG KNOWLEDGES: OBVERSE AND REVERSE OF DIGITALIZATION OF EDUCATION

Plebanek Olga
University at the Interparliamentary Assembly of the Eurasec,
14/1 Smolyachkova St, St. Petersburg, 194044, Russia
e-mail: plebanek@mail.ru

Abstract. The article analyzes the positive aspects of digitalization of education and the risks associated with them, the timely reflection of which and the development of adequate educational technologies will help to avoid negative trends in the cognitive and psychological sphere.

Keywords: artificial intelligence; clip thinking; pseudo-information; on-line education; self-education; tutoring.

«…Мы упёрлись в очень сложный момент развития человечества в целом. Темпы развития техники сегодня очень высоки. А наша способность это всё осмыслить и разумно в этой технической и информационной среде жить от этих темпов отстаёт. Мир переживает сейчас очень глубокий кризис в сфере культуры.», – так писал С.П. Капица [1]. Мир находится в переходном состоянии, мы вступаем в новую фазу социального развития – общество знания, но так ли это? Будет ли общество Big Data обществом Big Knowledges? Термин «общество знания», введенный в оборот П.Друкером [2] еще в середине XX в. для обозначения общественной системы, в которой знание занимает центральное место в деятельности человека, не совсем точно отражает суть происходящих процессов. По сути, именно уходящая индустриальная цивилизация, которая и породила феномен науки и отделение естественно-научных знаний от целостного знания, до этого момента существовавшее на теоретическом уровне в форме философии. Индустриальная технология для своего функционирования впервые в истории человечества потребовала универсального, открытого и стандартизированного знания и институциализированной системы образования. Цифровая технология, с одной стороны, предоставляет большие возможности человеку, которыми он еще никогда не обладал. С другой стороны, общество знания предъявляет требования как субъекту, который участвует в деятельности по обеспечению существования и безопасности популяции, так и к субъекту, который обеспечивает производство самого человека – его свойств и качеств, необходимых в осуществлении материальной деятельности. Эта новая ситуация, в которую втягивается человечество, требует осмысления как свойств и качеств системы, в которой придется существовать, так и свойств и качеств человека, которые потребуются в этой системе.

Прежде всего, самое очевидное достоинство цифровой технологии – доступность информации. Современный человек не пойдет в библиотеку за новой информацией, но он не обязательно пойдет и к специалисту, к компетентному источнику. Уже давно стала обыденной сентенция – «я беру информацию там, где она находится», подразумевая, что теперь человек не нуждается в посредниках – специалистах или образовательной системе. Однако, в сети не существует маркеров добросовестной информации и недобросовестной. Видимой приметой нашего время стало ученое невежество и информированное суеверие. Даже в научных статьях приходится встречать ссылки на источники, опубликованные в сети, но не прошедшие рецензирования. Приметой нашего времени становится рациональное суеверие – заблуждение, верифицированное псевдоинформацией. Примером чему является ситуация с вакцинированием, когда сознательный отказ от вакцинации мотивирован недобросовестной информацией, циркулирующей в сети.

Наличие большого объема информации, циркулирующей в сети (объем знаний удваивался в 90-е гг. – ежегодно, в начале XXI в. объем знаний увеличивается каждые 2 часа) провоцирует когнитивный кризис. Современная наука располагает данными о том, что объем человеческой памяти может быть «соизмерим с объемом всемирной паутины» [3], но объем знаний продолжает увеличиваться, а всемирная паутина и возможности искусственного интеллекта продолжают расти, в то же время биологические возможности человеческого мозга как бы не были велики, все же ограничены. Видимо, следствием этого противоречия – возросший объем информации и когнитивные возможности является феномен, о котором в настоящее время говорят и пишут исключительно в негативном контексте. Это феномен так называемого клипового мышления. Так называемое «клиповое» мышление в литературе [4] описывается как мозаичное, нелинейное, иррациональное. И эти его особенности имеют корреляцию с описанием формирующейся среды,

детерминированной информационной технологией – нелинейность, стохастичность, эмерджентность, (см., например: [5]). Функционирование субъекта в этих условиях не может быть обеспечено линейным картезианским мышлением, для которого, помимо уже указанных особенностей, характерна еще номотетичность. Возможно, именно эти особенности среды спровоцировали кризис картезианской рациональности и разрушение привычных, естественных для мира модерна, форм мышления и формирование непривычных мыслительных стратегий, а потому субъективно оцениваемых как деградация. Так называемое «клиповое» мышление является ответом на формирование стохастической среды и необходимости принимать решения в условиях недостатка информации. Однако, образовательные институты не готовы не только формировать соответствующие свойства и качества, но и не готовы работать в таких условиях – классическая образовательная модель ориентируется на поступательность, последовательность усвоения знаний, а в познавательной деятельности, в идеале, на полную индукцию.

Информационные технологии меняют не только форму коммуникаций, сетевое общество меняет форму образования как социального института. Информационная технология не только расширяет возможности дистанционного образования, предоставляя возможности онлайн обучения и комбинировать источники образовательных услуг от библиотек до университетов и научных центров. Информационная технология может стереть границы между образовательными структурами и потребителями образовательного продукта, предоставляя возможность, а также обусловливая необходимость постоянно приобретать к непроверенным источникам. В такой, постоянно меняющейся среде становится невозможно создать постоянный источник знаний, обладающий необходимым, при этом все возрастающим объемом информации, субъект-получатель образовательного воздействия вынужден самостоятельно достраивать образы мира, обращаясь к распределенным, сетевым источникам. В таких условиях образование становится самопроектируемым процессом, а субъект становится автопоэтическим субъектом, не нуждающимся во внешних институтах образования. Однако, этот тренд формирует недоверие к классической системе образования, одновременно разрушая вообще системность знания, так как, во-первых, клиповое мышление является оппонентом системного рационального мышления, а во-вторых, проектировщик образовательного процесса – и объект и субъект этого процесса, и он не может находиться видеть и весь процесс, и его структуру, находясь в начале и внутри процесса. Такое мышление в отсутствии системного характера знания приводит к распаду рационализма.

Информационная технология меняет саму структуру знания. Теперь, прежде всего, нужны не интериоризированные знания, которые теперь доступны всем, но представляют собой экстериоризованную форму, а фрагментированные умения и навыки, которые без необходимой составной части классических ЗУНов (знания, умения и навыки) неуклюже названы в современных образовательных программах компетенциями. Уже сегодня многие люди не нуждаются в стандартизированном образовании, не нуждаются в университете как источнике знания, они берут знания непосредственно там, где они складируются, «зиппуются» и циркулируют. Знания становятся внешним гаджетом, отделенным от человека. Ключевой ценностью становятся не сами по себе знания, которые находятся в открытом доступе, а способность включить их в деятельность. В связи с этим появился феномен, обозначаемый термином, этимологически восходящий к хорошо известному tutor – учитель, наставник, но семантическое поле которого смещено: это слово «туторинг», и оно не охватывает привычные Знания, Умения и Навыки. Под туторингом понимается своего рода инструкция по освоению некоторого элемента деятельности (навыка), без освоения всего комплекса сопряженных знаний и умений. Но отсутствие системности, фундамента в self-образовании может привести к обрушению когнитивного базиса технологии.

В обзоре обозначены не все риски и обратные стороны позитивных качеств и свойств информационной технологии, но то, на что нужно обратить внимание в образовательной системе в первую очередь, так как эти явления уже дают о себе знать в настоящем и свидетельствуют о рисках информированного суеверия или псевдоинофрмации, распаде классической модели образования, а вместе с ней системности образовательного процесса и пострационализму.

СПИСОК ЛИТЕРАТУРЫ

1. Капица С.П. Как Россию намеренно превращают в страну дебилов/.URL: http://izbrannoe.com/news/mysli/sergey-kapitsa-kak-rossiyu-namerenno-prevrashchayut-v-stranu-debilov/?fbclid=IwAR0cJ_Xf3L8Qnro4889cBykmnwZ8xfba_sePMyMORObr5NjacX3qEX-bPU. Дата обращения 10.08.2021.
2. Друкер П. Эпоха разрыва: ориентиры для нашего быстро меняющегося общества / перевод с англ. Б.Л. Глушакова. – М.: Издательский дом “Вильямс”, 2007. – 332 с.
3. Memory capacity of brain is 10 times more than previously thought. Salk News. Опубликовано на salk.edu 20 января 2016 г. URL: https://creationist.in.ua/reading/articles/260-brain-memory-capacity. Дата обращения 10.08.2021
4. Фрумкин К. Г. Клиповое мышление и судьба линейного текста // Ineternum. – 2010. – № 1. URL: http://nounivers.narod.ru/pub/kf_clip.htm. Дата обращения: 10.08.2021.
5. Князева Е.Н. Сложные системы и нелинейная динамика в природе и обществе // Вопросы философии. 1998. №4. – С.138-144.

УДК 316.334.3

ПОРТРЕТ УЧАСТНИКА ПРОТЕСТНОГО ОНЛАЙН-СООБЩЕСТВА

Сапон Ирина Валерьевна
Сибирский государственный университет телекоммуникаций и информатики
Бориса Богаткова ул., 51, Новосибирск, 630008, Россия
e-mail: irina.sapon@bk.ru

Аннотация. В работе представлен социологический портрет участника крупного протестного онлайн-сообщества в российской социальной сети «ВКонтакте». Результаты контент-анализа открытых данных личных страниц пользователей показали: участник протестного сообщества — это мужчина, житель Москвы или Санкт-Петербурга в возрасте 35 лет, с высшим образованием, придерживающийся либеральных взглядов.

Ключевые слова: интернет; протест; социальные движения; социальные медиа; «ВКонтакте».

A TYPICAL PARTICIPANT OF AN ONLINE PROTEST COMMUNITY

Sapon Irina
The Siberian State University of Telecommunications and Informatics
51 Borisa Bogatkova St, Novosibirsk, 630008, Russia
e-mail: irina.sapon@bk.ru

Abstract. The paper shows a sociological portrait of a participant in a large protest online community in the Russian social network VKontakte. The results of the content analysis of the open data of the community members showed this is a male resident of Moscow or St. Petersburg at the age of 35, who has a higher education and adheres to liberal views.

Keywords: internet; protest; social movements; social media sites; VKontakte.

Социальные медиа сегодня играют важную роль в организации протестной активности [1]. Цифровые технологии используются для агитации, информирования и координации участников протеста. Они выступают в роли СМИ, влияя на повестку дня и формируя общественное мнение, а также в качестве площадки для наращивания социального капитала, поиска единомышленников и формирования коллективной идентичности. К примеру, в российских митингах 2011-2012 годов социальные медиа, такие как *LiveJournal, Facebook* и *Twitter*, стали площадками для объединения протестующих, обмена эмоционально-заряженным контентом (фото и видео с мест событий), обсуждения и согласования дальнейших действий [1, 2].

Сегодня мобилизация протестных сил в России проходит с помощью «ВКонтакте», *Telegram, Instagram, TikTok* и *YouTube* [3]. В данной работе мы рассмотрим социальную сеть «ВКонтакте», которая остаётся лидером среди социальных медиа по объёму ежемесячно публикуемого контента и числу активных авторов [4]. Мы опишем социально-демографический портрет участника одной из самых многочисленных протестных групп данной социальной сети — «РосПил — война коррупции — Алексей Навальный» (https://vk.com/rospil).

С помощью API «ВКонтакте» и автоматизированной системы сбора данных мы собрали открытые данные личных страниц участников данной группы. На момент сбора (июнь 2021 года) в рассматриваемом сообществе числилось 338650 участников. После отсева удалённых (deleted) и заблокированных страниц (banned) пользователей, итоговый массив составил 183295 аккаунтов.

Количественный контент-анализ показал: типичный участник исследуемого сообщества — это житель крупного российского города (Москвы или Санкт-Петербурга) мужского пола в возрасте 35 лет, либеральных взглядов, имеющий в среднем 317,5 подписчиков, негативно относящийся к курению и компромиссно к алкоголю, ценящий в людях доброту и честность, а в жизни — саморазвитие.

С помощью сервиса частоты встречаемости слов [5] мы проанализировали информацию, указанную в поле «Образование». Мы выяснили, что типичный участник данного сообщества — это студент одного из столичных вузов (МГУ, СПбГУ, ВШЭ, МГТУ), закончивший экономический, технический или механико-математический факультет, интересующийся музыкой, спортом, путешествиями, кино, психологией, историей, книгами, футболом, фотографией, политикой, бизнесом. В целом, описанный нами социологический портрет совпадает с результатами опроса участников митинга 2011 года в Москве [6], а также с результатами исследования других протестных групп «ВКонтакте» [7].

Исследование выполнено при финансовой поддержке РФФИ и ЭИСИ в рамках научного проекта № 21-011-32247 «Российские протестные онлайн-сообщества: характеристики и особенности».

СПИСОК ЛИТЕРАТУРЫ

1. Ваньке А. В., Ксенофонтова И. В., Тартаковская И. Н. Формы протестной интернет-коммуникации в России (на примере движения «За честные выборы») // Пути России. Новый старый порядок-вечное возвращение? 2016. С. 98-129.
2. Платонов К. А., Юдина Д. И. Повестка протестных онлайн-сообществ Санкт-Петербурга во «ВКонтакте» // Мониторинг общественного мнения: Экономические и социальные перемены. 2019. № 5 (153). С. 226-49.
3. Гаеткулов Э. Н. Политический протест в цифровую эпоху: основные способы самоорганизации граждан // Общество: политика, экономика, право. 2021. №. 7 (96). С. 27-30.
4. Социальные сети в России: цифры и тренды, осень 2020 [Электронный ресурс]. – Режим доступа: https://br-analytics.ru/blog/social-media-russia-2020/ (дата обращения: 30.08.2021).
5. Site.Projects e [Электронный ресурс]. – Режим доступа: https://www.siteprojects.ru/?article=seo-kolichestvo/ (дата обращения: 30.08.2021).
6. Соколова А. Д., Головина М. В., Семирханова Е. К. «Бандерлоги» на проспекте Сахарова: социологический портрет // Антропологический форум. 2012. №. 16-online.
7. Ушкин С. Г. Вовлеченность пользователей социальных сетей в протестное движение // Власть. 2014. №. 8. С. 138-142.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЭКОЛОГИИ

УДК 502.175:556.53

ТРАНСГРАНИЧНЫЙ ПЕРЕНОС ЗАГРЯЗНЯЮЩИХ ВЕЩЕСТВ В РЕКЕ УРАЛ

Биненко Виктор Иванович[1], Рябинина Валерия[2]

[1] Федеральное государственное бюджетное учреждение науки Санкт-Петербургский научно-исследовательский центр экологической безопасности Российской академии наук
Корпусная ул., 18, Санкт-Петербург, 197110, Россия

[2] Санкт-Петербургский государственный университет промышленных технологий и дизайна
Большая Морская ул., 18, Санкт-Петербург, 191186, Россия
e-mails: vibinenko@mail.ru, leraryabinina99@gmail.com

Аннотация. Анализируются тренды изменчивости эколого-гидрологических характеристик загрязняющих веществ в воде на основных створах р. Урал, которая протекает через три субъекта РФ (Оренбургская и Челябинская области, республика Башкортостан) и три субъекта Республики Казахстан (Актюбинская, Западно-Казахстанская и Атырауская области) за период 2007 – 2020 годов. Отмечается связь понижения уровня р. Урал (обмеление) с современным изменением климата. Индекс загрязнённости воды в р. Урал на отдельных водозаборах по концентрации тяжёлых металлов, нефтепродуктов, нитратов, фосфатов, хлоридов, органических веществ подчас значительно превышает соответствующие предельно допустимые концентрации.

Ключевые слова: река Урал; тренд; эколого-гидрологические характеристики; концентрация; загрязняющие вещества; изменение климата.

TRANSBOUNDARY TRANSFER OF POLLUTANTS TO THE URAL RIVER

Binenko Viktor[1], Ryabinina Valeriya[2]

[1] St. Petersburg Research Center for Environmental Safety of the Russian Academy of Sciences
18 Korpusnaya St, St. Petersburg, 197110, Russia

[2] Saint Petersburg State University of Industrial Technologies and Design
18 Bolshaya Morskaya St, St. Petersburg, 191186, Russia
e-mails: vibinenko@mail.ru, leraryabinina99@gmail.com

Abstract. The trends of variability of ecological and hydrological characteristics of pollutants in water on the main channels of the Ural River, which flows through three subjects of the Russian Federation (Orenburg and Chelyabinsk regions, the Republic of Bashkortostan) and three subjects of the Republic of Kazakhstan (Aktobe, West Kazakhstan and Atyrau regions) in the period 2007 – 2020, are analyzed. There is a connection between the decrease in the level of the Ural River (shallowing) and the modern climate change. The index of water pollution in the Ural River at individual water intakes for the concentration of heavy metals, petroleum products, nitrates, phosphates, chlorides, organic substances sometimes significantly exceed the corresponding maximum permissible concentrations.

Keywords: Ural River; trend; ecological and hydrological characteristics; concentration; pollutants; climate change.

На основе собранных данных мониторинга поверхностных вод и донных отложений [1-8] анализируются тренды изменчивости эколого-гидрологических характеристик загрязняющих веществ в воде на основных створах р. Урал, которая протекает через три субъекта РФ (Оренбургская и Челябинская области, республика Башкортостан) и три субъекта Республики Казахстан (Актюбинская, Западно-Казахстанская и Атырауская области) в период 2007 – 2020 годов. Индекс загрязнённости воды в р. Урал на отдельных водозаборах по концентрации тяжёлых металлов, нефтепродуктов, нитратов, фосфатов, хлоридов, органических веществ подчас значительно превышает соответствующие предельно допустимые концентрации. Например, в створе р. Блява – 1,0 км ниже г. Медногорск – превышения ПДК загрязняющими веществами составили [4]: по цинку – 93,0 ПДК (в 2019г. – 38,4 ПДК) – уровень Экстремально Высокого Загрязнения; по меди – 18,5 ПДК (в 2019г. – 31,8 ПДК); по ХПК – 2,1 ПДК (в 2019 г. – 2,3 ПДК); по БПК5 – 1,2 ПДК (в 2019 г. – 1,5 ПДК); по железу общему – 1,7 ПДК (в 2009 г. – 1,1 ПДК); по никелю – 4,3 ПДК (в 2019 г. – 1,1 ПДК); по мышьяку – 1,5 ПДК (в 2019 г. – 1,8 ПДК). Массовая концентрация взвешенных веществ составила 16,3 мг/л [4]. Вода р. Урал в районе г. Магнитогорска характеризовалась повышенным содержанием фосфатов – в среднем 1,3 ПДК, азота нитритов – 1,2 ПДК,

нефтепродуктов – 2 ПДК, меди – 3 ПДК, цинка – 3,6 ПДК, марганца – 5,2 ПДК, при этом промышленные и коммунальные стоки очищаются только на 2%.

В то же время встворе р. Урал – 22,5 км ниже г. Орск (5,4 км ниже устья ручья Известковый Дол, г. Новотроицк) – превышения ПДК загрязняющими веществами составили: по ХПК – 1,9 ПДК (в 2019 г. – 1,9 ПДК); по БПК5 – 1,1 ПДК (в 2019 г. – 0,8 ПДК); по меди – 4,6 ПДК (в 2019 г. – 3,5 ПДК); по цинку – 1,7 ПДК (в 2019 г. – 0,9 ПДК). Массовая концентрация взвешенных веществ составила 27,0 мг/л [5-8].

Рост концентрации азота и фосфора поверхностных вод р. Урал приводит к её эвтрофикации, появлению водорослей и заиливанию русла реки. Снижение содержания растворённого кислорода, увеличение концентрации хлоридов и других токсичных веществ приводит к истощению водно-биологических ресурсов. В начале декабря 2018 г сброс химических веществ в Урал коммунальным предприятием «Атырау Су Арнасы» привёл к массовой гибели рыбы.

Среди парниковых газов двуокись углерода CO_2 играет наиболее важную роль в изменении климата, и за период 1976 – 2020 г, при скорости потепления 0,18 °С, глобальная температура выросла на 0,8 °С, а за последующее десятилетие рост температуры может достигнуть 1,5 °С [9]. По оценке Росгидромета скорость потепления за тот же период в РФ составила 0,51 °С / 10лет, а для бассейна среднегодовая аномалия приземного воздуха для Уральского федерального округа 4,36 °С при среднеквадратическом отклонении 1,16°С [10], что приводит к уменьшению влагообеспеченности и к увеличению риска засухи (до 3-4 недель в июле месяце) и обмелению р. Урал. В начале осени 2019 года г. Уральск, административный центр Западно-Казахстанской области, город, который ежесуточно потребляет 32–33 тысячи кубометров воды из реки Урал, остался без водоснабжения из-за снижения уровня воды в Урале. Тренды изменчивости и сравнение эколого-гидрологических характеристик загрязняющих веществ в воде на основных створах р.Урал в России и Казахстане свидетельствуют о росте загрязнённости за период от 2007 по 2020 годы, и поэтому р.Урал стала пятой самой загрязнённой среди европейских рек РФ.

Несмотря на существующее соглашение между Правительствами Российской Федерации и Республики Казахстан о совместном использовании и охране трансграничных водных объектов [11], какие-то конкретные действия по спасению реки Урал не реализованы. Сточные воды, поступающие в Урал и его притоки, обостряют экологическое состояние окружающей среды этих регионов, как в РФ, так и в Казахстане. Когда- то в 80-90-годы р. Рейн была «ночным горшком» Европы: рост промышленного производства сопровождался экологическими катастрофами, как, например, сброс в реку 30 тонн пестицидов, ртути и других сельскохозяйственных химикатов с завода фирмы «Sandoz» в швейцарском Базеле 1.11.1986г. Но принятые дальнейшие меры по её очистке сделали её безопасной. То есть современные технологии водоочистки и методы по рациональному водопользованию известны, и их можно и необходимо применить по отношению к р. Урал.

СПИСОК ЛИТЕРАТУРЫ

1. Государственный доклад «О состоянии и об охране окружающей среды Российской Федерации в 2019 году». М.: Минприроды России. – 1000 с.
2. Евстифеева Т.А., Глуховская М.Ю. Анализ качества воды р. Урал в границах г. Оренбург // Современные научные исследования и инновации. 2020. № 1 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2020/01/91351 (дата обращения: 26.08.2021)
3. Курмангалиев, Р. М. Гидроэкологические проблемы трансграничных водотоков Урало-Каспийского бассейна и пути их решения / Р. М. Курмангалиев, М. К. Онаев // Проблемы воспроизводства осетровых в среднем течении реки Урал и пути их решения: Материалы междунар. науч.-практ. конф. – Уральск, 2009. – С. 11–16.
4. Министрство природных ресурсов,экологии Оренбургской области: «О состоянии и об охране окружающей среды Оренбургской области в 2007-2017годах» режим доступа: http//mpr.orb.ru/ecology/129
5. Сивохип, Ж.Т. Эколого-географические проблемы трансграничного бассейна реки Урал и пути их решения / Ж. Т. Сивохип // Вестник Оренбургского государственного педагогического университета. – 2017. – №2. – С. 75–88.
6. Тулемисова, Г.Б. Экологическое состояние реки Урал / Г.Б. Тулемисова, Р.Ш. Абдинов, Г.Ж. Кабдрахимова, Т.Б. Жанетов // Вестник КазНУ. Серия химическая. – 2017. – №2(85). – С. 19–24.
7. Чибилёв А.А. Бассейн Урала: история, география, экология / отв. ред.: Ж. Т. Сивохип, О. А. Грошева; Институт степи УрО РАН. — Екатеринбург: УрО РАН, 2008. — 312 с. — ISBN 978-5-7691-1960-6.
8. Шайфутдинова, А.А. Оценка экологического состояния реки Урал в пределах г. Оренбурга // Экология и промышленность России. – 2018. – Т. 22 – № 1. – С. 68-71.
9. Шестой оценочный доклад МГЭИК «Изменение климата» 2021. Режим доступа: https://www.ipcc.ch/report/ar6/wg1/
10. Доклад об особенностях климата на территории Российской Федерации за 2020 год. – Москва, 2021. – 104 стр.
11. Соглашение между Правительством Российской Федерации и Правительством Республики Казахстан о совместном использовании и охране трансграничных водных объектов [Электронный ресурс] / Соглашение между Правительством Российской Федерации и Правительством Республики Казахстан о совместном использовании и охране трансграничных водных объектов от 04.04.2011 – Режим доступа: http://docs.cntd.ru, свободный.

УДК 004.67; 004.89; 621.3.068

ЦИФРОВИЗАЦИЯ – ОПАСНОСТИ ВНЕДРЕНИЯ И РАЗВИТИЯ

Витковский Владимир Валентинович[1], Горохов Владимир Леонидович[2], Бузников Анатолий Алексеевич[2]

[1] Специальная астрофизическая обсерватория РАН

пос. Нижний Архыз, Карачаево-Черкесская республика, 369167, Россия

[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия

e-mails: vvv@sao.ru, vlgorohov@mail.ru

Аннотация. Рассматриваются опасности трактовок термина «цифровизация», принятые различными научными направлениями.

Ключевые слова: Цифровизация; телекоммуникационные сети; интернет; браузеры; сайты; блоги; коды с открытыми ключами; облака; машинное обучение; системы распределённого реестра.

DIGITALIZATION – THE DANGERS OF IMPLEMENTATION AND DEVELOPMENT

Vitkovsky Vladimir[1], Gorokhov Vladimir[2], Buznikov Anatoly[2]
[1] Special Astrophysical Observatory of the Russian Academy of Sciences
Nizhny Arkhyz village, Karachay-Cherkessia, 369167, Russia
[2] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: vvv@sao.ru, vlgorohov@mail.ru

Abstract. The dangers of interpretations of the term digitalization adopted by various scientific directions are considered.

Keywords: Digitalization; telecommunication networks; Internet; browsers; websites; blogs; public key codes; clouds; machine learning; distributed registry systems.

Цифровизация закреплена правительственными постановлениями и поддержана государственным финансированием. И уже на этом этапе существует опасность непонимания и радикально отличающейся трактовки смысла термина цифровизация в точных и гуманитарных науках. Первоначально, бурное развитие вычислительной техники и техники связи позволило инженерам и математикам ввести термин информатика, который отразил сущность технических явлений. Огромное влияние информационных технологий на социум заставило социологов и политологов ввести социологический термин информационное общество, коммуникации в социуме. В рамках социологических и политологических наук этот термин отразил определенный круг социальных явлений. Аналогично поступили и экономисты, введя термин цифровая экономика. Здесь опасности заключаются в том, что эти термины в разных науках трактуются по-разному, что приводит к возможным трагическим недоразумениям, которые могут привести к серьезным технологическим, экономическим и социальным катастрофам.

Возникают угрозы безопасности жизнедеятельности на уровне социума, экономики, экологии и техники. Дело в том, что достижения вычислительной техники и компьютерных наук (обработка и передача данных в цифровом представлении) создали такие технические новации (информационно-телекоммуникационные сети, интернет, браузеры, сайты, блоги, коды с открытыми ключами, облака, машинное обучение, системы распределённого реестра), которые привели к фундаментальным социальным явлениям типа социальных сетей и криптовалюты, которые при неправильном понимании сути этих достижений могут привести к техносферным, экологическим и социальным катастрофам.

Принятый обществом термин цифровизация коварно включает в себя оба эти явления (технику обработки цифровых данных и социальные последствия внедрения этой техники). Однако не следует забывать, что эти социальные явления помимо положительных последствий несут и огромную, пока плохо предсказуемую угрозу для социума. Отчасти причина многих негативных социальных последствий, кроется в природе технических новаций. Недопонимание гуманитариями технических особенностей, а подчас и технической сути процессов цифровизации является серьезной техносферной опасностью. Этот факт был отмечен в работе Ричарда Кларка и Роберта Нейка «Третья мировая война, какой она будет?». Аналогичная ситуация уже возникала в атомной промышленности и потребовались серьезные усилия со стороны инженеров и физиков для разъяснения этого недопонимания гуманитариям.

Данный доклад может считаться скромной попыткой разделения технической сути термина цифровизация и гуманитарной интерпретации этого термина. Для преодоления сформулированных выше опасностей требуется, прежде всего, тщательно установить особенности трактовки ряда терминов, принятых в гуманитарных и технических науках. Требуется внимательное прочтение и адекватная трактовка ключевых административных документов, определяющих процессы цифровизации. Разумеется, это трудная задача, требующая междисциплинарной эрудиции, но другого пути похоже нет! Сделаем первые робкие усилия, чтобы начать решение этой трудной задачи с термина ставшего ключевым-цифровизация на примере анализа текстов ряда руководящих административных документов.

Заключение. Национальный проект задаёт общую архитектурную логику взаимодействия людей, государства и бизнеса в цифровой экономике. В том числе логику так называемых цифровых профилей. И общая логика — это правильно не только с точки зрения обеспечения безопасности, но и с точки зрения обеспечения обмена данными, как между государственными органами, так и между бизнесом и гражданами. Основной игрок цифровизации — это бизнес. Средства, которые вкладывает бизнес, входящий и не входящий в государственные программы, в разы превосходит максимально возможные государственные расходы. Объёмы и темпы инвестирования в цифровизацию будут стремительно расти. Цифровизация — это историческая неизбежность, а не пожелание людей, бизнесменов, политиков или государства. Не вовлечённый в цифровизацию субъект обречён. Что же делать политикам? Ответ давно известен – Если движение нельзя остановить, его нужно возглавить! Но возглавить, вникая в естественнонаучный смысл этих процессов!

Теперь можно сделать основной вывод из представленного выше – цифровизация неизбежна, но для осознания этого потребуются ещё очень многие усилия человеческого разума.

СПИСОК ЛИТЕРАТУРЫ

1. PowerPoint Presentation (tufts.edu)
2. Место России в мировых рейтингах цифровизации (fa.ru).
3. PowerPoint Presentation (tufts.edu).
4. https://ru.wikipedia.org/wiki
5. https://intalent.pro/interview/sergey-shishkin-o-budushchem-neyrotehnologiy-i-interfeysah-mozg-kompyuter.html
6. https://dic.academic.ru/dic.nsf/ruwiki/681778
7. (http://goverment.ru/dep_news/34005/
8. СТРАТЕГИЯ РАЗВИТИЯ (digital.gov.ru)
9. Digital colonialism is threatening the Global South | Science and Technology | Al Jazeera

УДК 004.67; 004.89; 621.3.068

АНАЛИЗ ВРЕМЕННЫХ РЯДОВ ДАННЫХ МОНИТОРИНГА АГРЕГАТОВ ГАЗОКОМПРЕССОРНОЙ СТАНЦИИ СРЕДСТВАМИ НЕЙРОННЫХ СЕТЕЙ

Горохов Владимир Леонидович, Бузников Анатолий Алексеевич, Шабалин Александр Игоревич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: vlgorohov@mail.ru

Аннотация. Данная работа описывает модель прогноза состояния газокомпрессорной станции, рассматриваются её конкретные агрегаты. Газокомпрессорная станция является опасным техногенным объектом, нагнетающим давление в газотранспортную систему, поэтому существует система мониторинга, отслеживающая состояние труб. На основании такого параметра как напряжение труб делается вывод о состоянии трубопровода. Для обеспечения безопасности этот параметр можно спрогнозировать.

Ключевые слова: искусственный интеллект; нейронная сеть; анализ временных рядов; газокомпрессорная станция.

ANALYSIS OF TIME SERIES OF MONITORING DATA OF GAS COMPRESSOR STATION AGGREGATES BY MEANS OF NEURAL NETWORKS

Gorokhov Vladimir, Buznikov Anatoly, Shabalin Aleksandr
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: vlgorohov@mail.ru

Abstract. This work describes a model for predicting the state of a gas compressor station, its specific aggregates are considered. The gas compressor station is a dangerous man-made object that pumps pressure into the gas transmission system, so there is a monitoring system that monitors the condition of the pipes. Based on such a parameter as the pipe voltage, a conclusion is made about the condition of the pipeline. To ensure security, this parameter can be predicted.

Keywords: artificial intelligence; neural network; time series analysis; gas compressor station.

Введение. Прогнозирование в газонефтяной области с целью предотвращения аварий в настоящее время достаточно актуально. В результате мониторинга на газокомпрессорных станциях собирают огромные массивы данных, что создаёт сложность для непосредственной обработки. Поэтому было решено обратиться к такому средству обработки данных, как нейронные сети [1]. Газокомпрессорная станция – комплекс оборудования и сооружений для повышения давления природного газа при его транспортировке и хранении [2]. Соответственно, она является опасным техногенным объектом, состояние агрегатов которой необходимо тщательно отслеживать, для чего и было решено использовать такой инструмент как нейронная сеть.

1. Подготовка данных. Данные мониторинга агрегатов газокомпрессорной станции были получены в виде таблиц, в которых соответствующему агрегату были представлены данные в некоторых точках, таких как "катушки", "тройники", "отводы". Как уже было указано выше, данные образовывали временной ряд, в котором значения из этих точек снимались почасово. Каждой точке соответствовало три значения напряжения, возникающих под действием механических нагрузок – кольцевое напряжение, осевое напряжение и эквивалентное напряжение. Значения напряжений выражены в мегапаскалях. Эквивалентное напряжение было выбрано для дальнейшего обучения модели нейронной сети и прогнозирования, так как оно являлось совокупностью кольцевого и осевого напряжений, а также потому, что именно оно сравнивается с расчётным сопротивлением трубы – оно не должно превышать его, иначе труба разрушится. Для обработки было взято 500 значений эквивалентного напряжения, снятых со следующих агрегатов: газоперекачивающий аппарат ГПА-2, аппарат воздушного охлаждения АВО-1, пылеуловительная установка ПУ-5.

2. Обработка данных нейронной сетью многослойного перцептрона. Для построения и обучения нейронных сетей я воспользовался таким программным обеспечением как STATISTICA. Первый вариант рассматриваемой модели был выбран в виде многослойного персептрона. Соответственно, в своей структуре он

имеет входной слой, один скрытый и выходной слой. Через анализ Фурье построили периодограмму, определили, что значения возникают с периодичностью в 24. Периодичность использовал как размер окна. Под тестовую выборку было отведено 15% всех значений, которые нейронная сеть моделировала уже самостоятельно. Далее, указал количество нейронов в скрытом слое до 30 нейронов, функцию ошибки как сумму квадратов, функции активации скрытого слоя – тождественную и логистическую, функцию выходного слоя – тождественную, исходя из соображения рассмотрения прогнозирования временного ряда как решения задачи регрессии. По итогам обучения, из нескольких сетей была выбрана сеть, наиболее хорошо моделирующая значения, MLP 24-18-1. Соответственно, данная сеть имеет 24 входных нейронов, 18 скрытых и 1 выходной, так как предсказывает лишь одно значение. В данном случае, обучение проводилось на данных газоперекачивающего аппарата ГПА-2. Нейронная сеть моделирует значения достаточно точно. Временной ряд напоминает синусоиду, что говорит о двух режимах работы АВО-1. Отдельные пики можно считать выбросами, однако, они могут указывать на неисправности в работе агрегата.

Заключение. В итоге показано, что технология нейронных сетей позволяет достаточно точно моделировать процессы, происходящие в трубовой обвязке агрегатов газокомпрессорной станции. С помощью нейронной сети многослойного перцептрона можно делать адекватный прогноз состояния агрегатов, таким образом, получая возможность предотвратить опасную техногенную ситуацию. Сеть, настроенная на моделирование временного ряда одного агрегата пригодна для моделирования других агрегатов. Однако, неполнота данных может существенно повлиять даже на уже настроенную сеть, затрудняя анализ и прогнозирование временного ряда.

СПИСОК ЛИТЕРАТУРЫ

1. Николаенко С., Кадурин А., Архангельская Е. Глубокое обучение. Погружение в мир нейронных сетей. СПб: Питер, 2018.
2. Горная энциклопедия // http://www.mining-enc.ru. URL: http://www.mining-enc.ru/g/gazokompressornaya-stanciya/ (дата обращения: 12.10.2021).

УДК 004.67; 004.89; 621.3.068

КОГНИТИВНАЯ ВИЗУАЛИЗАЦИЯ МНОГОМЕРНЫХ РАСПРЕДЕЛЕНИЙ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛЬНОГО ИЗМЕНЕНИЯ ХАРАКТЕРИСТИК СЛОЖНОЙ СИСТЕМЫ

Горохов Владимир Леонидович, Бузников Анатолий Алексеевич, Шинкевич Артем Дмитриевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: vlgorohov@mail.ru

Аннотация. Рассматриваются методы и средства когнитивной визуализации многомерных распределений данных мониторинга совокупности агрегатов для предотвращения аварийных ситуаций на газокомпрессорных станциях.

Ключевые слова: когнитивные методы визуализации; многомерные временные ряды.

COGNITIVE VISUALIZATION OF MULTIDIMENSIONAL DISTRIBUTIONS TO DETECT ABNORMAL CHANGES IN THE CHARACTERISTICS OF A COMPLEX SYSTEM

Gorokhov Vladimir, Buznikov Anatoly, Shinkevich Artem
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: vlgorohov@mail.ru

Abstract. Methods and means of cognitive imaging of multidimensional distributions for of the aggregates for environmental monitoring are considered.

Keywords: cognitive imaging techniques; multidimensional timelines.

Введение. В настоящее время регулярно возрастает количество чрезвычайных ситуаций на природных и промышленных объектах, происходят несанкционированные вторжения в информационных системах. Для своевременного выявления и предупреждения чрезвычайных ситуаций необходимо обеспечить обнаружение и прогноз аномальных состояний объектов по многомерной совокупности характеристик объектов. Когнитивная компьютерная графика позволяет представить многомерные данные в виде когнитивных псевдотрехмерных образов многомерных распределений, которые стимулируют эмпирическую интуицию человека-оператора, которая помогает обнаруживать синхронные взаимные корреляции и тренды в многомерных данных, с последующей их объективацией.

В данной работе приводятся модернизированные алгоритмы динамического проецирования, обеспечивающие генерацию когнитивных образов многомерных распределений. Когнитивные образы многомерных распределений позволяют визуализировать многомерные взаимные корреляции параметров сложных систем и тем самым обнаруживать экстремальные состояния объектов мониторинга. Хочется отметить, что форма когнитивного образа многомерного распределения помогает обнаруживать малые, но синхронные изменения многомерных характеристик объектов мониторинга. Отметим, что эти малые, но синхронные

изменения характеристик носят синергетический характер и часто являются предвестниками чрезвычайных ситуаций и вторжений.

Алгоритм когнитивной визуализации многомерных распределений. Осуществляется мониторинг набора характеристик совокупности *n*-однотипных сложных систем (объектов мониторинга). По результатам мониторинга измеряется *p*-различных характеристик этих систем. Таким образом, для каждой системы измеряется набор характеристик d_j (j = 1, …, p), который образует в многомерном пространстве характеристик R^P облако точек ***T***, которые обозначают совокупность объектов мониторинга [1]. Эти характеристики в многомерном статистическом анализе обозначаются как переменные. Таким образом, совокупность (p, n) значений для всех остальных сложных систем (объектов мониторинга) задается матрицей $\mathbf{D} = \{d_{ij}\}$; $i = (1, n)$, $j = (1, p)$, где d_{ij} – действительные значения переменных (измеряемых параметров, признаков), n – число объектов мониторинга всех p характеристик объектов мониторинга, p – число измеряемых характеристик (признаков) объектов наблюдения. Как и в одномерном случае, **D** рассматриваются как многомерные совокупности случайных величин.

Идея алгоритма визуализации многомерного распределения состоит в том, что в исходную матрицу данных **D,** которая описывает облако точек ***T*** в многомерном пространстве R^P, добавляется еще один столбец, в котором приведены результаты оценивания многомерной плотности вероятностей появления измеряемых комбинаций значений характеристик. Другими словами, в качестве дополнительной координаты этого многомерного пространства добавляется вероятность совместного появления этих характеристик. Теперь полученная матрица данных $\mathbf{D}^*$ (и соответствующее ей облако точек ***T****) представляет собой многомерное распределение вероятностей. В общем случае $\mathbf{D}^*$, как многомерное распределение вероятностей, содержит статистические сведения о поведении характеристик сложных систем (корреляционные свойства, разброс, положение, тренд изменения характеристики в совокупности объектов, и осцилляции). Это отражается в геометрической форме этого распределения! Многомерные ковариации и корреляции, а также взаимные многомерные ковариации и корреляции в виде квадратных матриц описывают зависимости между характеристиками. Еще раз подчеркнем, что в качестве дополнительной координаты этого многомерного пространства добавляется вероятность совместного появления этих характеристик. Далее, будем полагать это *p+1*-мерное пространство координат эвклидовым $\boldsymbol{R}^P$, что упрощает дальнейшие рассуждения (рассмотренные далее алгоритмы остаются рабочими в подходящих базисах аффинного пространства и ряда других базисов).

Для когнитивной визуализации построим отображение Ф как проекцию этого облака T* на двумерную плоскость Q2, проходящую через начало координат пространства RP. Но при этом обязательно одной из осей плоскости будет ось значений многомерных плотностей вероятностей. Пусть в Q2 заданы единичные ортогональные вектора u и v, используя их, несложно вычислить координаты (x, y) проекции данных на двумерную гиперплоскость Q: $x_i = pr_{\mathbf{u}}\,\mathbf{d}_i = \mathbf{d}_i \cdot \mathbf{u}$, $y_i = pr_{\mathbf{v}}\,\mathbf{d}_i = \mathbf{d}_i \cdot \mathbf{v}$, где исходная матрица данных D* описывает облако точек T* в многомерном пространстве RP. Здесь используется алгоритм, который строит непрерывную последовательность положений Q2, образующих «траектории», вдоль которых и отслеживается динамика образа. Для этого строится процедура динамического вычисления последовательности пар векторов {u, v}. Каждая ортогональная пара векторов {u, v}|g будет определять двумерную плоскость Q|g и ее ортогональный базис, где g – набор управляющих параметров небольшой размерности. Определим гиперплоскость W (размерности p – 1), проходящую через начало координат пространства RP нормальным уравнением: $\mathbf{x} \cdot \mathbf{n} = 0$, где n={nj} - вектор нормали, x={xj} - независимые переменные p-мерного пространства. Используя приведенные формулы, можно осуществить динамическую проекцию многомерного распределения D* на двумерную плоскость, одной из осей которого в данном алгоритме является ось значений плотностей вероятностей. Например, выбрав ведущие оси, задав нормаль и направление вращения, изменяя с небольшим приращением угол поворота ϕ, получим динамический циклический «обзор» многомерного распределения D*.

Заключение. Таким образом, модернизированный алгоритм формирует на плоскости Q2 динамическую проекцию многомерного распределения. Эта проекция благодаря когнитивным возможностям человеческого сознания порождает в сознании человека-оператора динамический образ, который позволяет визуализировать особенности многомерного распределения вероятностей. Эти особенности отражают особенности поведения характеристик сложных систем (корреляционные свойства, разброс, положение, тренд изменения характеристики в совокупности объектов, и осцилляции). Именно эти особенности и позволяют осуществлять долговременный прогноз и диагностику аномалий и вторжений в сложные системы.

СПИСОК ЛИТЕРАТУРЫ

1. Горохов В.Л., Муравьев И.П. Когнитивная машинная графика. Методы динамических проекций и робастная сегментация многомерных данных. Методология, методики и интерфейсы. Монография. СПб.: Издательство ИНЖЭКОН. 2007, 173 с
2. Лазарев В.Л. Обработка наблюдений на основе информационных критериев /Труды международной конференции по мягким вычислениям, 25-27 мая 2016, (SCM – 2016), том 1, Санкт-Петербург. Издательство СПбГЭТУ 2016. С. 11-15.

УДК 004

ИССЛЕДОВАНИЕ УФ СПЕКТРОВ ПОГЛОЩЕНИЯ ПИТЬЕВОЙ ВОДЫ РАЗЛИЧНОГО ПРОИСХОЖДЕНИЯ

Коноплев Георгий Асадович, Степанова Оксана Сергеевна, Чернова Ольга Валерьевна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: gakonoplev@mail.ru, oksana_lopatenko@mail.ru

Аннотация. Измерены спектры пропускания питьевой воды в диапазоне 200–350 нм. Исследованы особенности спектральных характеристик поглощения образцов воды различного происхождения. Продемонстрирована потенциальная возможность применения прямого спектрофотометрического метода в УФ области для качественной оценки минерального и органического состава питьевой воды.

Ключевые слова: ультрафиолетовая спектроскопия; питьевая вода; абсорбционный спектральный анализ.

INVESTIGATION OF UV ABSORPTION SPECTRA OF DRINKING WATER OF DIFFERENT ORIGIN

Konoplev Georgii, Stepanova Oksana, Chernova Olga
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: gakonoplev@mail.ru, oksana_lopatenko@mail.ru

Abstract. Transmission spectra of drinking water in a wavelength range of 200-350 nm were measured. The spectral absorption characteristics of multiple water samples from various sources were analyzed. It was demonstrated that direct spectrophotometric method in the UV region could be used for the qualitative assessment of the mineral and organic composition of drinking water.

Keywords: ultraviolet spectroscopy; drinking water; absorption spectral analysis.

В современном мире все более значимой становится проблема контроля качества питьевых и природных вод. В соответствии с приятыми стандартами качество воды оценивается комплексом химических, физических и санитарно-бактериологических показателей, определяемых по общепринятым методикам. В настоящей работе для общей оценки содержания в воде различных примесей предлагается использовать прямой спектрофотометрический метод в ультрафиолетовом (УФ) диапазоне.

Целью исследования является изучение спектральных характеристик поглощения питьевой воды в интервале длин волн 200…350 нм и определение возможности применения УФ абсорбционного спектрального анализа для качественной оценки ее минерального и органического состава.

В общей сложности были исследованы 20 проб воды различного происхождения: водопроводная вода из разных районов г. Санкт-Петербурга; очищенная бытовыми фильтрами водопроводная вода; столовая и минеральная бутилированная вода; вода из пруда и родников, расположенных на территории Ленинградской области. Вид спектральных характеристик водопроводной воды и воды из пруда указывает на наличие большого количества примесей органического происхождения; в диапазоне 250…300 нм наблюдается заметное поглощение. Форма кривых спектрального поглощения образцов бутилированной воды с высоким содержанием хлоридов характеризуется значительным оптическим поглощением в области 200…210 нм. Питьевая вода, полученная из водопроводной путем фильтрации, является слабоминерализованной, уровень оптического поглощения в области 200…210 нм в десять раз меньше, чем для минеральных вод. Для одного из образцов бутилированной артезианской воды отмечено аномально высокое поглощение в коротковолновой области с максимумом на длине волны 210 нм, что может быть связано с наличием в воде нитратов.

Таким образом, абсорбционный спектральный анализ питьевой воды позволяет проводить ее классификацию по обобщенному критерию минерализации, устанавливать повышенное содержание нитратов по относительному уровню поглощения в области 210…220 нм, обнаруживать органические примеси по относительному уровню поглощения в области 260…270 нм. Следует отменить, что в большинстве случаев гладкий спектр и низкий общий уровень поглощения в УФ области говорит о малом содержании примесей в питьевой воде.

Полученные результаты могут быть использованы при создании оптических сенсоров на базе УФ-светодиодов для экспресс-оценки содержания органических веществ в воде. Указанная методика не требует сложной схемы пробоподготовки и использования реагентов.

СПИСОК ЛИТЕРАТУРЫ

1. Государственный контроль качества воды: Справочник технического комитета по стандартизации. – М.: Изд-во стандартов, 2001. 688 с.
2. UV-Visible spectrophotometry of water and wastewater: Techniques and instrumentation in analytical chemistry – volume 27 /edited by O. Thomas, C. Burgess. The Netherlands: Elsevier, 2007. 360 p.
3. Джугаева И.О., Еремина М.В. Нитраты в воде как проблема безопасности жизнедеятельности // Advances in current natural sciences. 2014, Выпуск 6. С. 88.
4. Thompson K.C., Blankley M. Automatic continuous-flow determination of nitrate in raw and potable waters, rivers and sewage effluents by ultraviolet absorption spectrometry // Analyst. 1984 №109. P. 1053-1056.
5. Karlsson M., Karlberg B., Olsson R.J.O. Determination of nitrate in municipal waste water by UV spectroscopy // Anal. Chim. Acta. 1995, №312. P. 107 – 113.

УДК 528.837

БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ: КРИТЕРИИ КЛАССИФИКАЦИИ И ВЫБОРА ДЛЯ РЕШЕНИЯ ЗАДАЧ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ

Мазоя Адам, Бузников Анатолий Алексеевич, Горяинов Виктор Сергеевич
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: mazoya19@gmail.com, aabuznikov@mail.ru

Аннотация. Рассмотрены параметры классификации и выбора беспилотных летательных аппаратов для решения задач дистанционного зондирования. Проанализированы некоторые современные тенденции в данной области техники. Рассмотрен пример модели инфракрасной камеры для дистанционной тепловой съемки животных.

Ключевые слова: беспилотные летательные аппараты; классификация; дистанционное зондирование; тепловая съемка; инфракрасная камера.

UNMANNED AERIAL VEHICLES: CRITERIA OF THEIR CLASSIFICATION AND SELECTION TO SOLVE THE PROBLEMS OF REMOTE SENSING

Mazoya Adam, Buznikov Anatoliy, Goryainov Viktor
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: mazoya19@gmail.com, aabuznikov@mail.ru

Abstract. Parameters for classification and choice of unmanned aerial vehicles for solving remote sensing problems are considered. Some modern tendencies in this field of technology are analyzed. An example model of infrared camera for remote thermal imaging of animals is considered.

Keywords: unmanned aerial vehicles; classification; remote sensing; thermal imaging; infrared camera.

Применение беспилотных летательных аппаратов (БПЛА) становится неотъемлемым элементом экономики развитых и развивающихся стран. Первоначально сфера их использования была ограничена военными целями, в том числе разведкой и наблюдением, а в дальнейшем и при использовании гражданскими операторами сводилась к аэрофотосъемке и дистанционному зондированию [1]. В настоящее время БПЛА применяются для решения задач геодезии, сельского хозяйства, исследовательских задач, для гуманитарной работы при устранении последствий катастроф, а также для перевозки грузов [2, 3].

Основным отличием БПЛА от «обычных» летательных аппаратов является отсутствие пилота непосредственно на борту аппарата; в зависимости от типа управления, БПЛА могут быть более или менее автономными или же полностью управляться удаленно, с земли. В этой связи разделяют автоматические системы, жестко следующие предварительно заданной программе, и автономные системы, обладающие «свободой выбора» из предварительно заданных инструкций при наступлении незапланированной ситуации. Министерство обороны США выделяет 4 уровня автономности при классификации беспилотных систем [4].

Для связи с оператором и передачи данных используется радиоканал с определенной шириной спектра. Разрешенные для использования частоты и мощность передатчиков определяются местными регламентами радиосвязи в соответствии с предписаниями Международного союза электросвязи (WRC), органа ООН. На настоящий момент не существует выделенного участка в спектре радиочастот, предназначенного только для связи с БПЛА.

По типу аэродинамической схемы выделяют БПЛА с неподвижным крылом (самолетного типа) и винтокрылые летательные аппараты.

В первых подъемная сила создается при горизонтальном движении за счет вращения тянущего или толкающего винта в вертикальной плоскости. Такие аппараты взлетают после разбега по взлетной полосе или при помощи катапульты, а садятся либо также на полосу, либо на парашюте. Они развивают более высокие скорости и имеют большую дальность полета, чем винтокрылые БПЛА, что обусловливает их широкое применение для военных целей.

БПЛА второго типа, как правило, поднимаются в воздух несколькими (например, четырьмя или шестью) горизонтальными винтами, за что их часто называют мультикоптерами. Изменение тяги одного или нескольких двигателей, вращающих винты, сообщает аппарату горизонтальную скорость, что позволяет обходиться без применения автомата перекоса. К преимуществам таких аппаратов относится возможность вертикальных взлета и посадки, исключающая необходимость взлетной полосы, меньший уровень шума, а также возможность зависать в воздухе над требуемой точкой.

Встречаются также, хотя и редко, гибридные аппараты, которые могут взлетать и садиться вертикально, как вертолеты, а в полете менять ориентацию винтов и несущих плоскостей на самолетную.

Еще одним важным параметром БПЛА является его вес, непосредственно связанный с возможной дальностью полета и грузоподъемностью, а также определяющий юридический статус летательного аппарата. Один из подходов, например, предлагает считать большими беспилотные летательные аппараты самолетного типа тяжелее 150 кг и мультикоптеры тяжелее 100 кг [5]. Нидерландские транспортные правила разделяют

тяжелые и легкие БПЛА граничной массой в 150 кг независимо от конструкции аппарата. Текущее направление развития беспилотных летательных аппаратов сфокусировано на том, чтобы сделать более легкие и компактные дроны доступными для широкого круга потребителей.

Наконец, беспилотные летательные аппараты классифицируются по виду источника энергии, необходимой для питания двигателей. В тяжелых БПЛА самолетного типа, в том числе военных (MQ-1B Predator, «Орлан-10»), применяют двигатели внутреннего сгорания, питающиеся керосином или другим видом авиационного топлива. Гораздо шире, в особенности на малых БПЛА, распространено питание приводных электродвигателей от сменных перезаряжаемых аккумуляторов (например, литиевых), обеспечивающих время полета порядка получаса–часа. На более крупных аппаратах могут устанавливаться топливные ячейки, в которых энергия химической реакции преобразуется непосредственно в электрическую энергию. Несмотря на хорошую экономичность, недостатком таких ячеек является достаточно большой вес. Кроме того, есть примеры применения солнечных панелей на больших БПЛА самолетного типа, в результате чего увеличилось время беспосадочного полета летательного аппарата.

Перечисленные выше характеристики должны учитываться при выборе модели БПЛА, соответствующей массе нагрузки и требуемой дальности полета, которые зависят от решаемой задачи. Рассмотрим некоторые из видов полезной нагрузки беспилотных летательных аппаратов.

Наиболее распространены в качестве нагрузки камеры видимого диапазона, передающие изображение в различном разрешении на пульт управления БПЛА. Значительное большинство дронов на потребительском рынке продается с установленной на них камерой.

Применение БПЛА для природоохранных целей часто связано со съемками животных в инфракрасном диапазоне [6]. Наилучший контраст изображения при этом достигается в прохладные дни, по утрам и ночью. Плотная растительность может перекрывать тепловое излучение от объекта съемки, а нагретые объекты – причиной ложных срабатываний, однако такие ограничения характерны не только для съемки с БПЛА [7].

Растущая доступность беспилотных летательных аппаратов привела к появлению в ассортименте ряда производителей инфракрасных камер моделей, пригодных для установки на малые БПЛА. Так, FLIR DuoPro R сочетает инфракрасную камеру с камерой видимого диапазона высокого разрешения (4K). Успешность тепловой съемки во многом определяется расстоянием до объекта и разрешением инфракрасной камеры. Приборы с высоким разрешением (640 × 512 пикселей) дают возможность обнаружения животных с большего расстояния, однако и стоят дороже, чем камеры среднего или низкого разрешения (256 и 160 × 120 пикселей соответственно). Фокусное расстояние инфракрасной камеры задается предварительно установленной входной линзой, и, соответственно, линейный размер поля зрения изменяется только с изменением высоты полета носителя. К примеру, установка линзы с фокусным расстоянием 9 мм на камеру FLIR Duo Pro R с разрешением 336 × 256 пикселей дает поле зрения шириной в 35°, в то время как линза с фокусным расстоянием 17 мм обеспечивает 17°.

Дальнейшее развитие технологий БПЛА приведет к уменьшению размеров, веса, стоимости дронов, расширению их доступности для широкого круга потребителей и области их применения. Вероятно повышение автономности беспилотных летательных аппаратов и возможностей их работы в группах-роях.

СПИСОК ЛИТЕРАТУРЫ

1. Colomina I., Molina P. Unmanned aerial systems for photogrammetry and remote sensing: A review // ISPRS Journal of Photogrammetry and Remote Sensing. 2014, V. 92. P. 79–97.
2. Ayamga M., Tekinerdogan B., Kassahun A., Rambaldi G. Developing a policy framework for adoption and management of drones for agriculture in Africa // Technology Analysis & Strategic Management. 2021, V. 33 (8). P. 970-987.
3. Malveaux C., Hall S. G., Price R. Using drones in agriculture: unmanned aerial systems for agricultural remote sensing applications / American Society of Agricultural and Biological Engineers, Quebec Canada, 2014. Montreal. July 13 – July 16 2014. P. 1.
4. USDOD. Unmanned systems integrated roadmap. Washington, DC: US Department of Defence, 2013. http://www.defense.gov/Portals/1/Documents/pubs/DODUSRM-2013.pdf.
5. Clarke R. Understanding the drone epidemic // Computer Law & Security Review. 2014, V. 30 (3). P. 230-246.
6. Scholten C. N., Kamphuis A. J., Vredevoodg K. J., Lee-Strydhorst K. G., Atma J. L., Shea C. B., Lamberg O. N., Proppe D. S. Real-time thermal imagery from an unmanned aerial vehicle can locate ground nests of a grassland songbird at rates similar to traditional methods // Biological Conservation. 2019, V. 233. P. 241-246.
7. Butler D. A., Ballard W. B., Haskell S. P., Wallace M. C. Limitations of thermal infrared imaging for locating neonatal deer in semiarid shrub communities // Wildlife Society Bulletin. 2006, V. 34. P. 1458-1462.

УДК 51.76

ПРИМЕНЕНИЕ ЛОГИКО-СОБЫТИЙНОГО МОДЕЛИРОВАНИЯ ДЛЯ ОПИСАНИЯ КРИТИЧЕСКИХ ФАЗ РАЗВИТИЯ СОЦИОИНФОРМАЦИОННЫХ ПРОЦЕССОВ

Переварюха Андрей Юрьевич
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: madelf@rambler.ru

Аннотация. В работе авторами рассмотрены преимущества метода формирования гибридных вычислительных структур применительно к экстремальным процессам в информационном обществе. Метод строится на применении систем основных и вспомогательных дифференциальных уравнений. Вычислительная модель логико-событийной структуры дополнена набором предикатов, позволивших выделить события смены

режима функционирования в системе информационных потоков. Итоговая модель дискретно-непрерывная анализируется как итерация с несколькими областями притяжения и хаотическим множеством, граничный кризис хаотического репеллера опишет переход в катастрофические режимы для распространения информационных волн в гетерогенной среде.

Ключевые слова: гибридные модели; кризис потоков информации; информационный вброс.

APPLICATION OF LOGIC-EVENT MODELING TO DESCRIBE CRITICAL PHASES OF DEVELOPMENT OF SOCIO-INFORMATION PROCESSES

Perevaryukha Andrey
St. Petersburg Institute for Informatics and Automation of the Russian Academy of Science
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: madelf@pisem.net

Abstract. The authors consider the advantages of the method of forming hybrid computing structures in relation to extreme processes in the information society. The method is based on use of systems of basic and auxiliary differential equations. The computational model of the logical-event structure is supplemented with a set of predicates that made it possible to single out the events of a change in the operating mode in the information flow system. The final discrete-continuous model is analyzed as iteration with several regions of attraction and a chaotic set, the boundary crisis of a chaotic repeller will describe the transition to catastrophic modes for the propagation of information waves in a heterogeneous environment.

Keywords: hybrid models; crisis of information flows; information stuffing.

Новые методы моделирования требуются для описания взрывообразных «эруптивных» фаз развития информационных процессов в современном социуме при замедленной реакции регулирующих организаций. Гибридные вычислительные структуры призваны решать актуальные задачи прогнозирования, качественной и количественной оценки последствий и выработке методов противодействия явлению вторжения целенаправленной деструктивной информации, имеющей тенденцию к неконтролируемому распространению в создавшихся условиях. Смена фаз генезиса и формализация масштабных нестационарных состояний в информационных потоках, к которым относится подавляющее большинство деструктивных информационных вбросов, одновременно одна из актуальных нерешенных проблем для математической социологии как междисциплинарного научного направления. С точки зрения системной социологии постановка задачи формального описания стремительных изменений в информационной динамике у разных общественных групп влияния представляет теоретический интерес из-за необходимой модификации представлений о действующих механизмах, точнее о диапазонах их действия и выключения, в регуляции эффективности передачи волны сообщений в различных состояниях настроения общества.

Процесс распространения волны информационного вброса сравним с агрессивной инвазией. Экодинамика популяций вселенцев зависит от уровня сопротивления биотического окружения. Многие наблюдаемые ситуации при массовых размножениях связаны с явлениями инвазий и адаптаций чужеродных видов перманентной современной проблемой. В некоторых случаях вид-вселенец, представленный изначально малой группой особей, не встречает конкурентного противодействия со стороны автохтонного биологического окружения. Тогда у образующейся популяции происходит максимизация репродуктивного потенциала, который на самом деле является агрегированной и отнюдь не независимой характеристикой. Данная характеристика должна включать запаздывание в регуляции. Инвазия далеко не всегда переходит в стадию вспышки. В некоторых случаях инвазия может оказаться даже полезной для питания ценных потребителей, как в случае с донной фауной Каспийского моря, где проникновение средиземноморских моллюсков повысило продуктивность кормовой биомассы рыб во время падения уровня моря. Вспышки численности свойственны и неизмеримо давно присутствующим в экосистеме видам. В некотором смысле они становятся частью круга последовательных перестроений в растительных сообществах. О цикличности или стохастичности причин таких явлений ведется длительная дискуссия. Можно сделать вывод о действии пороговых состояний численности при сложном межвидовом взаимодействии группы видов, составляющих трехуровневую систему противоборства ос-паразитов и их жертв, других ос или фитофагов.

Основной аспект, выделяемый нами в комплексной проблеме исследования вспышек в том, что, по-видимому, нереально выделить общий путь развития процесса именно с позиций теории метаморфозов фазовых портретов нелинейных динамических систем, аппарата для описания резких изменений. Данные ряда примеров указывают на различия в типах бифуркаций. Наиболее оправданным видится сценарный подход к моделированию ситуаций с некоторым множеством вариантов дальнейшего развития.

В настоящей работе мы предлагаем непрерывную модель бифуркационного запуска сценария специфически осциллирующей вспышки на основе концепции запаздывания в действии регулирующих факторов. Модельный сценарий актуален по имеющимся данным наблюдений для случаев поражения вредителем лесов Канады и позволяет оценивать временную эволюцию характеристик пилообразных колебаний численности.

Традиционными методами математической экологии описать нелинейность завершения и спонтанность выхода из хаотических флуктуаций представлялось невозможным. Был выбран подход в форме непрерывно-

дискретной динамической системы, строившейся на формализации выживаемости поколения. Изменения непрерывной системы в выделенные условиями моменты времени были соотнесены с переходами между тремя стадиями развития онтогенеза псиллид, для каждой из стадий отличаются факторы зависящей от плотности смертности, как и независимой.

Непрерывная часть базовой модели для $N(t)$ описывалась переопределяемой правой частью дифференциального уравнения для убыли численности на трех последовательных временных интервалах с набором условий завершения активности и перехода к расчету смежного поколения [2].

Таким образом, мы получили сложную зависимость для дискретной составляющей траектории, которая демонстрирует спонтанное преодоление порогового равновесия из переходного хаотического режима. Изначально при анализе наблюдений предполагалась вариативность на стадии завершения вспышки, что не было учтено нами в предыдущей статье, но вполне можно отразить в модели просто уменьшив вклад функционала, индуцирующего тут эффект Allee. Для описания завершения вспышки инкапсулирован триггерный функционал. Он редуцирует притягивающую стационарную точку R^*, что резко переведет популяцию в следующих период хаотических флуктуаций. Порог запуска вспышки L не может быть монотонно достижим из любого состояния системы, все же вспышка численности с дефолиацией — это эпизодическое явление, потому несвязные границы областей притяжения аттракторов в нашей модели хорошо описывают данный экологический аспект. Существование порога, отраженного в модели граничным неустойчивым положением равновесия, объясняется сложными взаимоотношениями различных видов паразитических наездников. Полученные модели можно использовать в составе систем уравнений явного межвидового противоборства, они вычислительно значительно более сложны, чем современные модели трофодинамики «хищник-жертва», но обладают качественным разнообразием поведения у дискретных итераций.

Вспышки автохтонных видов менее разнообразны по аспектам прохождения фаз, чем экстремальные варианты развития инвазионного процесса, потому полученные имитационные сценарии не исчерпывают всю возможную динамику. Особенно интересны различия, если посмотреть на хорошо документированные явления в экосистемах через призму математической теории динамических систем. Например, инвазионный вид после стремительной вспышки может проходить критическое состояние «бутылочного горлышка», с сохранением реликтовой популяции либо полным исчезновением из нового ареала. Полученный в уравнении переходный режим можно рассматривать так же для задачи анализа случая специфического развития рецидивирующей инфекции. Интересно дальнейшее расширение уравнений для модельных исследований инвазионных процессов других видов со сложным независимым противодействием. Спровоцировать следующую серию колебаний с уровня информационных потоков в такой модели может стремительные изменения состояния общественных настроений. В дальнейшем развитии модели нами планируется описание осциллирующей пилообразной динамики информационных волн из-за рецидивов активации интереса к деструктивной информации со стороны малых, но активных групп влияния.

Работа выполнена в рамках проекта РФФИ: № 17-07-00125 (в СПИИРАН).

СПИСОК ЛИТЕРАТУРЫ

1. Дубровская В.А. О критериях обоснованности для анализа нелинейных эффектов в моделях эксплуатируемых популяций // Проблемы механики и управления: Нелинейные динамические системы. 2016. № 48. С. 74-83.
2. Переварюха А.Ю. Модель развития спонтанной вспышки численности насекомого с апериодической динамикой // Энтомологическое обозрение. 2015. Т. 94. № 1. С. 203-215.

УДК 528.71, 004.032.22

ОПЕРАТИВНАЯ ОБРАБОТКА БОЛЬШИХ ПОТОКОВ ИНФОРМАЦИИ С ПОМОЩЬЮ НЕЙРОСЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ НА АЭРОФОТОСНИМКАХ ТЮЛЕНЕЙ

Черноок Владимир Ильич[1], Сабиров Марат Авхатович[1], Васильев Александр Николаевич[1], Бузников Анатолий Алексеевич[2], Черноок Илья Владимирович[1], Мелентьев Владимир Владимирович[3]

[1] Автономная некоммерческая организация «Экофактор»
Нейшлотский пер., 11/1 А, Санкт-Петербург, 194044, Россия

[2] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия

[3] Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП)
Большая Морская ул., 67, Санкт-Петербург, 190000, Россия
e-mails: chernook@mail.ru, aabuznikov@mail.ru

Аннотация. С помощью методов из открытой библиотеки алгоритмов компьютерного зрения Open CV и алгоритма на основе сверточной нейронной сети архитектуры U-Net реализована автоматизированная обработка большого объёма фотоснимков, полученных с БПЛА, для обнаружения на отснятых льдах тюленей.

Ключевые слова: искусственные нейронные сети; беспилотные летательные аппараты; аэрофотоснимки; обнаружение; тюлени.

RAPID PROCESSING OF LARGE INFORMATION FLOWS USING ARTIFICIAL NEURAL NETWORKS TO DETECT SEALS IN AERIAL PHOTOGRAPHS

Chernook Vladimir[1], Sabirov Marat[1], Vasilyev Aleksandr[1], Buznikov Anatoliy[2], Chernook Ilya[1], Melentyev Vladimir[3]

[1] Autonomous non-profit organization «Ecofactor»
11/1A Neyshlotskiy Ln, St. Petersburg, 194044, Russia
[2] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
[3] Saint Petersburg State University of Aerospace Instrumentation (SUAI)
67 Bolshaya Morskaya St, St. Petersburg, 190000, Russia
e-mails: chernook@mail.ru, aabuznikov@mail.ru

Abstract. Using methods from the open-source library of computer vision algorithms Open CV and an algorithm based on a U-Net convolutional neural network, automatic processing of large volumes of aerial photographs was implemented, to detect seals for detecting seals on captured ice.

Keywords: artificial neural networks; unmanned aerial vehicles; aerial photographs; detection; seals.

Весной 2018 г. в Белом море выполнена авиасъёмка ледовых залежек гренландских тюленей с трех беспилотных самолетов «Орлан-10» с большой дальностью полётов (около 1000 км). За один полетный день с трех самолетов было получено около 10 тысяч фотоснимков [1]. При этом для планирования следующих маршрутов полетов крайне важно знать результаты уже выполненных полётов – насколько много животных определяется по данным, собранным за последний полет. Поэтому возникает необходимость оперативной обработки полученных материалов.

С помощью методов из открытой библиотеки алгоритмов компьютерного зрения Open CV (https://opencv.org/) и алгоритма на основе сверточной нейронной сети архитектуры U-Net [2], нами реализована автоматизированная обработка большого объёма фотоснимков с целью обнаружения на отснятых льдах тюленей.

Формирование обучающей выборки для U-Net включало этапы предварительной обработки изображений (изменение размера, оценка цветовых характеристик), нарезки оригинальных широкоформатных изображений на небольшие фрагменты 512x512 пикс., 60% из которых содержало хотя бы одно животное и ручной разметки данных – ограничивающими прямоугольниками (bounding box) размечено 1000 фрагментов.

Работа нейронной сети архитектуры U-Net основана на нескольких этапах «свертки» размеров изображения по мере извлечения признаков искомых объектов (т. н. encoder) и последующей «развертке» до размеров, соответствующих оригиналу (decoder), причем на шагах развертки изображение умножается с таковым для соответствующего шага свертки. Подобный алгоритм работы позволяет при помощи одной архитектуры сети решать одновременно задачи сегментации и классификации (взрослый тюлень / детеныш).

По результатам обработки обученной сетью более 1000 оригинальных изображений ошибка обнаружения взрослых тюленей составила 5 – 10%, детенышей (бельков) – около 20%. Это объясняется меньшей видимостью детенышей на оригинальных изображениях.

Разработанный подход позволяет в автоматическом режиме обнаруживать тюленей на фотоснимках, практически не теряет тюленей, однако допускает наличие ложноположительных объектов. Результат работы сети позволяет получить фотоматериалы для «ручного» уточнения учетчиком, сокращая время обработки массивов фотоданных в десятки раз. Разработанная методика позволяет обнаруживать на льдах не только взрослых тюленей, но и белых детёнышей (бельков), причем точность классификации сети может быть повышена как сбором и разметкой дополнительных данных, так и другими методами.

СПИСОК ЛИТЕРАТУРЫ

1. Черноок В. И., Болтнев А. И., Бузников А. А., Васильев А. Н., Михалин В. А, Черноок И. В., Мелентьев В. В. Особенности получения и обработки информации при мультиспектральной авиасъёмке тюленей на льдах с использованием нескольких БПЛА с большой дальностью полётов // Материалы конференции Информационная безопасность регионов России (ИБРР-2019), С-Петербург, 2019, С. 413-415.
2. Ronneberger O., Fischer P., Brox T. U-Net: Convolutional Networks for Biomedical Image Segmentation https://arxiv.org/pdf/1505.04597.pdf

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИОКОМПЬЮТИНГЕ

УДК 004.031.4

АГРЕГАЦИЯ СВЕДЕНИЙ И ОЦЕНКА ПАРАМЕТРОВ ГРУЗОВЫХ МАРШРУТОВ НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ДЕФИЦИТА

Абрамов Максим Викторович[1,2], Есин Максим Сергеевич[2]
[1] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
[2] Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mails: mva@dscs.pro, maksim.esin.2002@gmail.com

Аннотация. В статье рассматривается общая концепция автоматизированных сервисов оценки стоимости перевозок грузов, а также различные механизмы их работы, основные составляющие запросов к таким сервисам, существующие решения и технологии и пути их развития.

Ключевые слова: оценка стоимости перевозок груза; автоматизация поиска оптимального маршрута грузоперевозок; логистика; веб-разработка.

AGGREGATION OF INFORMATION AND ESTIMATION OF CARGO ROUTE PARAMETERS BASED ON MACHINE LEARNING METHODS IN CONDITIONS OF INFORMATION SCARCITY

Abramov Maxim[1,2], Esin Maxim[2]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[2] Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mails: mva@dscs.pro, maksim.esin.2002@gmail.com

Abstract. The article deals with the general concept of automated cargo transportation cost estimation services, various mechanisms of their operation, the main components of requests to such services, existing solutions and technologies and ways of their development.

Keywords: estimation of the cost of cargo transportation; automation of the search for the optimal route of cargo transportation; logistics; web development.

Введение. Перевозки грузов и курьерские доставки пользуются большим спросом, особенно во время пандемии. Грузоперевозками пользуются как обычные люди, например при переезде или доставке важных бумаг, так и крупные компании. При росте числа транспортных компаний конкуренция в сфере перевозок грузов постоянно растет. Грузовые компании стараются повысить лояльность клиентов, с которыми уже работали, и привлечь новых, проводя ребрендинг, увеличивая автопарк, а также повышая уровень доступности клиентов к своим предложениям.

Это стремление выражается в размещении информации о своих перевозчиках на различных агрегаторах и в поисковиках, которые стали популярны на рынке логистики в том числе из-за тренда на объединение [1] независимых компаний.

Агрегаторы доставок грузов, которые берут на себя ответственность за доставку товаров, делегируют реальную работу курьерским службам и логистическим компаниям, которые работают независимо друг от друга. Поисковики доставок подбирают по запросу пользователя лучшие предложения от грузовых компаний, сортируя варианты по стоимости доставки и по срокам доставки.

В этой статье рассмотрен один из важнейших для клиента аспект, а именно расчет стоимости перевозки груза. Предметный интерес в рамках этой статьи представляют как независимые сервисы по расчету стоимости доставки, так и специальные поисковики, собирающие в одном месте лучшие предложения независимых сервисов, а также принципы их работы и данные о грузе, которыми оперируют сервисы при расчете.

Формулировка задачи. В масштабах данной статьи планируется рассмотреть общую концепцию автоматизированных сервисов оценки стоимости доставки, классифицировать данные о доставке, необходимые для расчета стоимости, и сравнить различные подходы к реализации подобных сервисов. На практике полученные наблюдения помогут улучшить уже существующий функционал сайта cargotime.ru.

Концепция сервиса расчета стоимости доставки.

Данные для запроса. Безусловно, нельзя указать все факторы, сказывающиеся на конечной стоимости доставки ввиду возможного наличия форс-мажорных обстоятельств, непредвиденных расходов на топливо и ремонт или гарантийных выплат за утрату или повреждение груза и неустойки за нарушение сроков выполнения доставки.

Среди факторов, влияющих на стоимость доставки можно выделить три группы: факторы, влияющие на тип и размер контейнера, такие как габариты груза, его вес и условия перевозки; факторы влияющие на маршрут, такие как точки отправления и назначения, срочность доставки и обязательные промежуточные пункты; и вторичные факторы, такие как наличие дополнительной страховки и настройка уведомлений о текущем местонахождении груза и статусе доставки.

Отметим основные составляющие перевозки груза [2] с которыми предстоит работать, чтобы вычислить примерную стоимость доставки: среди них габариты груза, его вес и условия хранения, а также начальный и конечный пункт доставки.

Габариты и вес груза напрямую влияют на размер контейнера. В случае, когда груз имеет большие габариты при маленьком весе, размеры контейнера могут быть меньше габаритов груза. Чтобы не возникало ситуаций, когда груз и подходящий к нему по физическому весу контейнер несовместимы, придумали понятие объемного веса, которое учитывает плотность груза. В той части вычислений, где учитываются физические масштабы груза, используют большее из значений физического и объемного веса. Причем разные компании используют разные способы подсчета значения объемного веса, что затрудняет работу агрегаторов по созданию общего стандарта.

Условия хранения влияют на вид контейнера. Классификация грузов по условиям перевозки довольно обширна: одни только опасные грузы (ADR) делятся на 9 классов [3]. Специфические грузы требуют специфических условий, и чем сложнее поддерживать условия, необходимые для груза в пути, тем дороже окажется транспортировка.

Дистанция между пунктом отправления и пунктом назначения, как ни странно, влияет не пропорционально: количество пересеченных границ и проезд по тарифным зонам сказывается иногда даже сильнее, чем пройденный путь. Особенно это заметно при перевозках по России на большие расстояния. У каждой логистической компании свои тарифы на каждую из зон, что дает агрегаторам простор к составлению маршрута, состоящего из нескольких отрезков, выполняемых разными перевозчиками.

Помимо основных данных о грузе и маршруте доставки на стоимость также влияет срочность и тип доставки (например, от двери до постамата), дополнительная страховка груза и настройка уведомлений о местонахождении и статусе заказа, причем последние две опции учитываются при расчете в последнюю очередь.

Принцип работы независимого сервиса. Используя данные о грузе, начальной и конечной точке, типе и срочности доставки, которые предоставляет пользователь, сервис рассчитывает несколько оптимальных маршрутов: самый оптимальный с точки зрения стоимости, срока доставки, обязательного условия посещения некоторых промежуточных пунктов или некоторой совокупности этих факторов.

Автоматизированность процесса важна для высокой скорости обработки данных от пользователя, построения маршрута и согласования конечного маршрута и примерной стоимости с пользователем.

Принцип работы агрегатора сервисов. Поиск лучшего из подходящих предложений на многочисленных сайтах грузовых компаний может оказаться очень продолжительным и энергозатратным. В таком случае, клиент может не найти лучшего среди множества решений, а логистическая компания — потерять потенциального клиента.

Поисковики сервисов доставок собирают информацию от разных логистических компаний. По запросу пользователя данные поисковики должны выдавать список самых лучших предложений на основе свежих данных от перевозчиков. Чаще всего, они работают как доска объявлений: пользователь получает список вариантов перевозки его груза, к каждому из которых прикреплена ссылка на сайт перевозчика или другой контакт.

Агрегаторы работают для пользователя еще проще: они берут ответственность за доставку товара на себя и поручают ее одной из своих партнерских компаний, при этом пользователю не нужно выбирать, какая именно из компаний совершит грузоперевозку.

Перспективы развития сервиса калькулятора доставки на портале Cargotime.ru.

Сервис Cargotime.ru [4] — один из самых известных информационных порталов, посвященных грузоперевозкам и предоставляющий набор инструментов для работы логистов. Кроме модуля, вычисляющего оптимальные варианты перевозки грузов из пункта А в пункт Б разными компаниями, в нем есть калькулятор поездки, рассчитывающий оптимальный маршрут поездки в пределах одного континента с самыми дешевыми заправками на автомобиле. Также добавлена возможность отслеживания посылок и контейнеров с грузами. На сайте размещают свои данные многие крупные российские и иностранные компании перевозчиков и таможенные брокеры.

Почти все более-менее крупные логистические компании, например, как EastLines [5] и FastPoint [6], имеют на своем сайте калькулятор стоимости доставки своими курьерами и перевозчиками. Cargotime по запросу пользователя выдает список таких предложений.

Среди сервисов с похожим, но несколько более скромным функционалом можно выделить Cargo.guru [7], у которого есть похожий калькулятор вариантов стоимости доставки. Также, сервис Ati.su [8] предоставляет возможность найти не только грузовые машины, готовые выполнить заказ, но и грузы, которые можно перевезти.

Главный недостаток калькулятора перевозок Cargotime перед аналогами — отсутствие выбора условий перевозки и типа контейнера. Этот критерий мог бы помочь более качественно сортировать предложения компаний.

Cargotime может стать уникальным сервисом в русскоязычной части интернета, если добавить возможность калькулятора строить сложные маршруты: это особенно актуально в России, где региональные тарифные планы у разных перевозчиков отличаются. Это в несколько раз ускорит процесс генерации сложного маршрута вручную, соответственно будет пользоваться спросом.

Заключение. В статье была описана общая концепция автоматизированных сервисов оценки стоимости доставки, а также реализация такой концепции в рамках сайта Cargotime. С помощью анализа минимального набора данных о грузе, необходимых для построения маршрутов доставки, были выделены основные направления развития проекта с целью стать уникальным сервисом на российском рынке логистики.

СПИСОК ЛИТЕРАТУРЫ

1. Цифровая конкуренция. Статья газеты Коммерсантъ [Электронный ресурс] // Логистика. 11 декабря 2018. URL: https://www.kommersant.ru/doc/3825982 (дата обращения: 06.10.2021).
2. Тарифный калькулятор доставки груза - просто о сложном [Электронный ресурс] URL: https://efsol.ru/articles/tariff-calculator.html (дата обращения: 06.10.2021).
3. Классы опасных веществ [Электронный ресурс] // Статья о соглашении ADR в энциклопедии Wikipedia. Дата обновления: 01.07.2021. URL: https://ru.wikipedia.org/wiki/Европейское_соглашение_о_международной_дорожной_перевозке_опасных_грузов#Классы_опасных_веществ (дата обращения: 06.10.2021).
4. Информационный ресурс Cargotime [Электронный ресурс] URL: https://cargotime.ru/ (дата обращения: 06.10.2021).
5. Электронный калькулятор стоимости доставки сервиса EastLines [Электронный ресурс] URL: https://www.eastlines.ru/raschet-stoimosti/ (дата обращения: 06.10.2021).
6. Электронный калькулятор стоимости доставки сервиса FastPoint [Электронный ресурс] URL: https://www.fastpoint.ru/calc (дата обращения: 06.10.2021).
7. Агрегатор грузовых перевозок Cargo.guru [Электронный ресурс] URL: https://cargo.guru/ (дата обращения: 06.10.2021).
8. Биржа грузоперевозок Ati.su [Электронный ресурс] URL: https://ati.su/ (дата обращения: 06.10.2021).

УДК 004.8

АВТОМАТИЗАЦИЯ ПРОВЕРКИ НЕПРОТИВОРЕЧИВОСТИ ИДЕАЛОВ КОНЪЮНКТОВ С ОЦЕНКАМИ ВЕРОЯТНОСТИ ИСТИННОСТИ

Вяткин Артём Андреевич[1], Тулупьев Александр Львович [2]
[1] Санкт-Петербургский государственный университет
Университетский пр., 28, Старый Петергоф, Санкт-Петербург, 198504, Россия
[2] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mails: vyatkin.artex@gmail.com, alt@dscs.pro

Аннотация. В работе рассматривается проверка непротиворечивости идеалов конъюнктов с оценками вероятности истинности, выступающих в качестве математической модели фрагмента знаний в теории алгебраических байесовских сетей, а также ее реализация.

Ключевые слова: алгебраические байесовские сети; фрагмент знаний; идеал конъюнктов; машинное обучение; вероятностные графические модели.

AUTOMATION OF CONSISTENCY CHECKING OF IDEALS OF CONJUNCTS WITH TRUTH PROBABILITY ESTIMATES

Vyatkin Artyom[1], Tulupyev Alexander[2]
[1] Saint Petersburg State University
28 Universitetskiy Av, Stary Peterhof, St. Petersburg, 198504, Russia
[2] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mails: vyatkin.artex@gmail.com, alt@dscs.pro

Abstract. This work considers the consistency check of ideals of conjuncts with estimates of the probability of truth, acting as a mathematical model of a knowledge pattern in the theory of algebraic Bayesian networks, as well as its implementation.

Keywords: algebraic Bayesian networks; knowledge pattern; ideals of conjuncts; machine learning; probabilistic graphical model.

Введение. Для того, чтобы рассуждать в терминах некоторой предметной области, делать выводы или строить планы на дальнейшую деятельность, часто приходится основываться на знаниях, которые были накоплены в данной области. Упомянутые знания в большинстве случаев содержат в себе неопределенность,

изучение и обработка которой является одним из направлений современной информатики [10]. Такие знания можно рассмотреть, как систему утверждений. Между их элементами или набором элементов существуют связи, которые могут оценить эксперты в данной области. При этом, как правило, высказывания экспертов характеризуют связи между небольшим количеством сущностей из предметной области, поэтому вся совокупность знаний экспертов разбивается на части, фрагменты знаний, образующие вместе базу фрагментов знаний [7].

Одной из моделей, способной описать экспертную систему являются вероятностные графические модели. Вероятностную графическую модель можно представить как базу фрагментов знаний с неопределенностью, если внутри предметной области возможно разбиение на фрагменты знаний [6]. Вероятностные графические модели находят себе применение в различного рода задачах, связанных, например, с распознаванием и отслеживанием людей на видео [3], анализом кредитного риска [2], оценкой того, каково влияние человеческого фактора в морских авариях [4]. Представителем класса вероятностных графических моделей являются алгебраические байесовские сети, которые в будущем предполагается использовать, например, для исследований социоинженерных атак [1, 5]. Одним из представлений фрагментов знаний в данной модели является идеал конъюнктов над некоторым множеством атомарных пропозициональных формул, характеризующих атомарные утверждения, каждому элементу которого приписывается некоторая точечная или интервальная оценка вероятности истинности [7]. При этом подобная оценка может заключать в себе противоречие и для дальнейшей работы с фрагментами знаний их необходимо либо устранять, согласовывая оценки, либо утверждать о невозможности исключения противоречий.

Ввиду развития теории алгебраических байесовских сетей возникает потребность в реализации программ, предоставляющих возможность удобной обработки полученных данных, что позволит ускорить процесс оценки имеющейся информации, упростить построение соответствующих выводов. Так, в этом нуждается задача проверки непротиворечивости фрагментов знаний, являющаяся частной проблемой вышеупомянутой теории. Данная работа нацелена на разрешение этого вопроса.

Идеал конъюнктов представляется как вектор точечных оценок вероятностей соответствующих конъюнктов, и на них, для однозначного сопоставления, введена перенумерация, вопросы которой подробно разобраны в [8-9]. Исходная интервальная оценка представляет собой пару векторов, составленных из констант, и являющихся нижними и верхними границами соответствующих конъюнктов. Проверка непротиворечивости с математической точки зрения зависит от того, как представлена оценка вероятности. В случае точечных оценок применяется покомпонентная проверка неотрицательности произведения определенного вида матрицы, являющейся степенью Кронекера матрицы с двумя строками и столбцами, и самого вектора, представляющего вероятности конъюнктов [7]. Такое условие следует из аксиоматики вероятностной логики, накладывающей ограничения на кванты, построенные над атомарными пропозициональными формулами, и, соответственно, на конъюнкты, так как между векторами с вероятностями квантов и конъюнктов существует матричное преобразование, и один вектор выражается через другой. Проверка непротиворечивости в случае интервальных оценок сводится к задаче линейного программирования, где покомпонентно ищутся экстремальные значения вероятностей [7]. В качестве условий для задачи линейного программирования выступают исходные оценки вероятностей конъюнктов и условие неотрицательности, как для точечных оценок.

На рис. 1 изображены примеры структур фрагментов знаний, конъюнктам которых назначены интервальные оценки вероятности. Следует отметить, что вероятность пустого конъюнкта равна 1, так как такой конъюнкт представляет собой тождественную истину в вероятностной логике. На рис. 1.а назначение интервальных оценок вероятности противоречиво, так как в рамках этих интервальных оценок можно выбрать такие точечные значения для конъюнктов, при которых этот выбор задает противоречивую оценку. Подобное назначение интервальных оценок можно согласовать, и результат согласования для рассматриваемого выше фрагмента знаний представлен на рис. 1.б.

Реализация автоматизации проверки непротиворечивости идеалов конъюнктов была осуществлена на языке программирования Python. Для вычислений использовались такие пакеты, как numpy, предоставляющий работу с матрицами, и cvxopt, позволяющий решать задачи линейного программирования. Для взаимодействия с пользователем было разработано десктопное приложение с использованием пакета PyQt5. Реализованное приложение позволяет легко проверить фрагмент знаний на предмет его непротиворечивости, а также, если допустимо, согласовать границы. Ввод оценок вероятности может происходить как покомпонентно, где пользователю предлагается ввести оценку вероятности для каждого компонента по отдельности, так и в одном поле ввода для верхних и нижних границ.

Заключение. Представленные результаты позволяют в автоматическом режиме обрабатывать данные о фрагментах знаний, представленных в виде идеалов конъюнктов с оценками вероятности истинности. Обработка заключается в проверке непротиворечивости и, если допустимо, согласовании интервальных оценок вероятностей, что дает возможность использовать результаты данной работы при практическом применений теории алгебраических байесовских сетей.

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № 0073-2019-0003, при финансовой поддержке РФФИ проект №20-07-00839; поддержана Санкт-Петербургским государственным университетом, проект № 73555239.

СПИСОК ЛИТЕРАТУРЫ

1. Khlobystova A. O., Abramov M. V., Tulupyev A.L. An approach to estimating of criticality of social engineering attacks traces // Studies in Systems, Decision and Control. 2019. vol. 199. P. 446–456.
2. Masmoudi K., Abid L., Masmoudi A. Credit risk modeling using Bayesian network with a latent variable //Expert Systems with Applications. 2019. Vol. 127. P. 157–166.
3. Yang Y., Xu M., Wu W., Zhang R., Peng Y. 3D multiview basketball players detection and localization based on probabilistic occupancy //2018 Digital Image Computing: Techniques and Applications (DICTA). IEEE, 2018. P. 1–8.
4. Qiao W., Liu Y., Ma X., Liu Y. Human factors analysis for maritime accidents based on a dynamic fuzzy Bayesian network // Risk analysis. 2020. Vol. 40. №. 5. P. 957–980.
5. Корепанова А. А., Абрамов М. В., Тулупьева Т.В. Идентификация аккаунтов пользователей в социальных сетях «Вконтакте» и «Одноклассники» // Семнадцатая Национальная конференция по искусственному интеллекту с международным участием. КИИ–2019. Ульяновск, 21–25 окт. 2019. Т. 2. Ульяновск: УлГТУ, 2019. С. 153–163.
6. Тулупьев А.Л. Алгебраические байесовские сети: логико-вероятностный подход к моделированию баз знаний с неопределенностью. // СПб.: СПИИРАН, 2000. 282 с.
7. Тулупьев А. Л. Алгебраические байесовские сети: локальный логико-вероятностный вывод: Учеб. пособие. // СПб.: ООО Издательство «Анатолия», 2007. 80 с.
8. Тулупьев А. Л. Генерация множества ограничений на распределение оценок вероятности над идеалом цепочки конъююнкций // Вестник молодых ученых. 2004. № 4. Сер. Прикладная математика и механика. 2004. № 1. С. 35-43.
9. Тулупьев А. Л., Никитин Д. А. Экстремальные задачи в апостериорном выводе над идеалами цепочек конъюнкций // Труды СПИИРАН. 2005. Вып. 2, т. 2. СПб.: Наука, 2005. С. 12-15.
10. Тулупьев А. Л., Николенко С. И., Сироткин А. В. Байесовские сети: логико-вероятностный подход. // СПб.: Наука, 2006. 607 с.

УДК 004.853

ОЦЕНКА ДОСТОВЕРНОСТИ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ В КОНТЕКСТЕ ОЦЕНКИ ЛИЧНОСТНЫХ ОСОБЕННОСТЕЙ ПОЛЬЗОВАТЕЛЯ

Корепанова Анастасия Андреевна
Санкт-Петербургский государственный университет
Университетский пр., 28, Старый Петергоф, Санкт-Петербург, 198504, Россия
Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
e-mail: aak@dscs.pro

Аннотация. Данная статья посвящена задаче оценки правдоподобия данных, содержащихся на страницах пользователя в социальной сети. В данной статье предложен обзор проблематики правдивости данных в социальных сетях, предложен дизайн исследования для построения модели оценки истинности данных в профилях пользователей. Результаты данного исследования могут быть полезны в широком спектре задач связанных с анализом социальных сетей, в том числе в задачах, связанных с анализом защищённости пользователей информационных систем от социоинженерных атак.

Ключевые слова: социоинженерные атаки; профиль уязвимостей пользователя; анализ социальных сетей.

EVALUATION OF THE ACCURACY OF INFORMATION ON ONLINE SOCIAL NETWORKS IN THE CONTEXT OF ASSESSMENT OF PERSONAL FEATURES OF THE USER

Korepanova Anastasia
Saint Petersburg State University
28 Universitetskiy Av, Stary Peterhof, St. Petersburg, 198504, Russia
St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
e-mail: aak@dscs.pro

Abstract. This article is devoted to the problem of assessing the likelihood of data contained on a user's pages in a social network. This article provides an overview of the problem of the truthfulness of data in social networks, and proposes a study design to build a model for assessing the truthfulness of data in user profiles. The results of this study can be useful in a wide range of tasks related to the analysis of social networks, including tasks related to the analysis of the security of users of information systems from social engineering attacks.

Keywords: socio-engineering attacks; user vulnerability profile; social network analysis.

Введение. Задачи анализа социальных сетей в последнее время набирают всё большую популярность. Они возникают во множестве областей и контекстов науки и индустрии, например, в сфере информационной безопасности [1], таргетированной рекламы [2, 3], оценке кредитоспособности кредитозаёмщика [4–6] и множества других, связанных, например, с медициной. Анализ социальных сетей имеет два основных вида: это анализ данных одного конкретного пользователя для определения каких-либо его личностных особенностей, или анализ объеждинений и групп пользователей и динамики их взаимодействия или общих особенностей. Также данные из социальных сетей могут быть использованы в такой сфере информационной безопасности, как оценка защищённости пользователей информационных систем от социоинженерных атак [7–11]; информация о из аккаунта пользователя мозволяет предлагать ему релевантную рекламу в задачах маркетинга [2, 3] и т.п. Для оценки общества к какому-то объекту, явлению или событию, используется анализ анализ групп пользователей

[3], в последнее время такой анализ стал особенно популярен в связи с необходимостью оценки влияния коронавирусной пандемии и локдауна на психическое состояние общества [15]. Среди всех сфер анализа социальных сетей хочется выделить область, связанную с оценкой защищённости пользователей информационных систем от социоинженерных атак. Социоинженерные атаки направлены не на технические уязвимости системы, а на психологические и другие уязвимости её пользователей, связанные с их личностными (психическими, культурантропологическими, социодемографическими) особенностями, так что для оценки защищённости системы необходимо уметь оценивать эти особенности, для чего строятся профили уязвимости пользователей. Как один из источников данных для построения профиля уязвимостей пользователя могут вытупать его профили (или аккаунты) в социальных сетях [16-19].

Однако данные из социальных сетей не всегда могут быть в достаточной степени достоверны, так как люди склонны в них лгать [12]. По результатам опроса 2000 человек, который провёл Custard.com [12], 43% опрошенных подтвердили, что приукрашают факты о себе и своей жизни в социальных сетях. Дети могут часто преувеличивать свой возраст: в 2014 году исследователи EU Kids Online провели опрос 442 детей возраста от 8 до 12 лет, который показал, что большую часть времени за компьютером большинство из них проводит в социальной сети «Facebook», хотя регистрация там разрешена с 13 лет [13]. В работе [14] авторы провели опрос 272 взрослых людей, только 32% опрошенных заявили, что они всегда честны в социальных сетях. В работе [14] исследовалась зависимость между личностными чертами тёмной триады (нарциссизм, макиавеллизм, психопатия) и честностью в социальной сети «Instagram». Результаты показали, что нарциссические личности уязвимого типа, а также пользователи с высокими показателями по «шкале макиавеллизма» имеют склонности к тому, чтобы лгать в социальных сетях.

Таким образом, социальные сети могут быть ненадёжным источником информации о пользователях. Чтобы использовать данные, содержащиеся в социальных сетях, необходимо уметь оценивать вероятность истинности информации, содержащейся на странице пользователя, или, иначе говоря, степень доверия к этой информации. В рамках исследования, посвящённого повышению защищённости пользователей информационных систем от социоинженерных атак, для оценки уязвимости пользователей к разным видам СИА, по данным из социальных сетей извлекается информация о личностных (психологических, социодемографических, культуратропологиечских и т.д.) особенностях каждого пользователя, в дальнейшем на основе этой информации строится профиль уязвимостей каждого пользователя к различным социоинженерным атакам. Для повышения надёжности оценок степени выраженности уязвимостей пользователей к СИА планируется провести исследование для выявления степени надёжности различных фактов, которые пользователи публикуют о себе в социальных сетях, а именно о социодемографических культурантропологических и психологиечских особенностях.

Гипотеза исследования состоит в том, что некоторые комбинации значений атрибутов в профиле пользователя могут свидетельствовать о том, что пользователь с какой-то степенью вероятности не является искренним. Примером может быть использование заведомо невозможных локаций в городе проживания: «Средиземье», «Лихолесье» и т.д., статус «замужем» при возрасте меньше 18 лет и т.д.

Предлагаемый дизайн исследования:

– Планируется собрать набор данных, содержащий достоверную информацию о личностных особенностях пользователей и её представление в социальных сетях с помощью анкетирования на различных площадках.

– С помощью методов статистического анализа планируется определить комбинации атрибутов, в которых пользователи наиболее часто указывают ложные данные.

– Построить модель для оценки вероятности истинности данных в профиле. Для этой задачи могут быть использованы вероятностные графические модели: байесовские сети доверия или алгебраические байесовские сети [19, 20, 21].

Заключение. Таким образом, в данной статье предложен обзор проблематики правдивости данных в социальных сетях, предложен дизайн исследования для построения модели оценки истинности данных в профилях пользователей. Результаты данного исследования могут быть полезны в широком спектре задач связанных с анализом социальных сетей, в том числе в задачах, связанных с анализом защищённости пользователей информационных систем от социоинженерных атак.

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № 0073-2019-0003, при финансовой поддержке РФФИ проект №20-07-00839; поддержана Санкт-Петербургским государственным университетом, проект № 73555239.

СПИСОК ЛИТЕРАТУРЫ

1. Camacho D., Panizo-LLedot Á., Bello-Orgaz G., Gonzalez-Pardo A., Cambria E. The four dimensions of social network analysis: An overview of research methods, applications, and software tools // Information Fusion. 2020. Vol. 63. Pp. 88–20. doi: 10.1016/j.inffus.2020.05.009.
2. Yamane D., Yamane P., Ivory S.L. Targeted Advertising: Documenting the emergence of Gun Culture 2.0 in Guns magazine // Palgrave Communications. 2020. № 6 (1). Art. no. 61. doi: 10.1057/s41599-020-0437-0.
3. Hinds J., Williams E.J., Joinson A.N. “It wouldn't happen to me”: Privacy concerns and perspectives following the Cambridge Analytica scandal // International Journal of Human Computer Studies. 2020. Vol. 143. Art. no. 102498. doi: 10.1016/j.ijhcs.2020.102498.
4. Yu X., Yang Q., Wang R., Fang R., Deng M. Data cleaning for personal credit scoring by utilizing social media data: An empirical study // IEEE Intelligent Systems. 2020. Vol. 35 (2). Art. no. 8986628. Pp. 7–15. doi: 10.1109/MIS.2020.2972214.
5. Óskarsdóttir M., Bravo C., Sarraute C., Vanthienen J., Baesens B. The value of big data for credit scoring: Enhancing financial inclusion using mobile phone data and social network analytics // Applied Soft Computing Journal. 2019. Vol. 74. Pp. 26–39. doi: 10.1016/j.asoc.2018.10.004.

6. Guo G., Zhu F., Chen E., Liu Q., Wu L., Guan C. From footprint to evidence: An exploratory study of mining social data for credit scoring // ACM Transactions on the Web. 2016. Vol. 10 (4). Pp. 1–38. doi: 10.1145/2996465.
7. Абрамов М.В. Автоматизация анализа социальных сетей для оценивания защищённости от социоинженерных атак // Автоматизация процессов управления. 2018. № 1 (51). С. 34– 40.
8. Корепанова А.А., Олисеенко В.Д., Абрамов М.В., Тулупьев А.Л. Применение методов машинного обучения в задаче идентификации аккаунтов пользователя в двух социальных сетях // Компьютерные инструменты в образовании. 2019. №3. С. 29–43. doi:10.32603/2071-2340-2019-3-29-43.
9. Багрецов Г.И., Шиндарев Н.А., Абрамов М.В., Тулупьева Т.В. Подходы к автоматизации сбора, структурирования и анализа информации о сотрудниках компании на основе данных социальной сети // Нечеткие системы, мягкие вычисления и интеллектуальные технологии (НСМВИТ–2017). Труды VII Всероссийской научно-практической конференции. 2017. С. 9–16.
10. Khlobystova A., Abramov M., Tulupyev A. An approach to estimating of criticality of social engineering attacks traces // Studies in Systems, Decision and Control. 2019. Vol. 199. Pp. 446– 456. doi: 10.1007/978-3-030-12072-6_36.
11. Suleimanov A., Abramov M., Tulupyev A. Modelling of the social engineering attacks based on social graph of employees communications analysis // Proceedings – 2018 IEEE Industrial Cyber-Physical Systems, ICPS 2018. 2018. Pp. 801–805. doi: 10.1109/ICPHYS.2018.8390809.
12. Custard.co. [Электронный ресурс] URL: https://www.custard.co.uk/over-three-quarters-of-brits-say-their-social-media-page-is-a-lie/ (дата обращения 06.09.2021).
13. The Social Media Invisibles [Электронный ресурс] URL: https://www.theatlantic.com/technology/archive/2016/08/the-social-media-invisibles/497729/ (дата обращения 06.09.2021).
14. M. Drouina, D. Miller., Sh.M.J. Wehleb, E. Hernandeza Why do people lie online? “Because everyone lies on the internet” // Computers in Human Behavior. 2016. P. 134-142.
15. Наместников А.М., Филиппов А.А., Мошкин В.С., Ярушкина Н.Г. Модель социального портрета пользователя социальной сети на основе семантического анализа слабоструктурированного контента профиля // Системный анализ и информационные технологии САИТ–2019. Труды Восьмой международной конференции. 2019. С. 336– 341.
16. Han X., Huang H., Wang L. F-PAD: Private Attribute Disclosure Risk Estimation in Online Social Networks // IEEE Transactions on Dependable and Secure Computing. 2019. Vol. 16. No. 6. Pp. 1054–1069. doi: 10.1109/tdsc.2019.2934096.
17. Li Y., Yan Q., Deng R.H. Privacy leakage analysis in online social networks // Computers and Security. 2015. Vol. 49. Pp. 239–254. doi: 10.1016/j.cose.2014.10.012.
18. Hastie T., Tibshirani R., Friedman J. Random forests //The elements of statistical learning. – Springer, New York, NY, 2009. С. 587–604. doi: 10.1007/978-0-387-84858-7_15.
19. Utkin L., Kovalev M., Meldo A., Coolen F. Imprecise Extensions of Random Forests and Random Survival Forests // Proceedings of the Eleventh International Symposium on Imprecise Probabilities: Theories and Applications, PMLR. 2019. Vol. 103. Pp. 404–413.
20. Тулупьев А.Л. Преобразование ациклических байесовских сетей доверия в алгебраические байесовские сети // Известия высших учебных заведений. Приборостроение. 2009. Т. 52. № 3. С. 21-23.
21. Тулупьев А.Л. Алгебраические байесовские сети: система операций глобального логико-вероятностного вывода // Информационно-измерительные и управляющие системы. 2010. Т. 8. № 11. С. 65-71.

УДК 004

ПОДХОДЫ И МЕТОДЫ К ОЦЕНКЕ ВЫРАЖЕННОСТИ ПСИХОЛОГИЧЕСКИХ ОСОБЕННОСТЕЙ ПОЛЬЗОВАТЕЛЕЙ В СОЦИАЛЬНЫХ СЕТЯХ

Олисеенко Валерий Дмитриевич[1], Тулупьева Татьяна Валентиновна[2,1]

[1] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
[2] Санкт-Петербургский государственный университет
Университетский пр., 28, Старый Петергоф, Санкт-Петербург, 198504, Россия
e-mails: vdo@dscs.pro, tvt@dscs.pro

Аннотация. В работе представлена формализация задачи выявления (оценки) выраженности психологических особенностей пользователей социальных сетей по информации, собранной в их аккаунтах. Представленные результаты могут быть использованы для создания систем, основанных на методах машинного обучения, которые позволят предсказывать оценку выраженности психологических особенностей. Также рассмотрены существующие методы и подходы в данной области.

Ключевые слова: психологические особенности пользователей; социальные сети; социоинженерные атаки.

APPROACHES AND METHODS TO IDENTIFY THE PSYCHOLOGICAL CHARACTERISTICS OF USERS IN ONLINE SOCIAL NETWORKS

Oliseenko Valerii[1], Tulupyeva Tatiana[2,1,3]

[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[2] Saint Petersburg State University
28 Universitetskiy Av, Stary Peterhof, St. Petersburg, 198504, Russia
e-mails: vdo@dscs.pro, tvt@dscs.pro

Abstract. This paper presents a formalization of the task of identifying (evaluating) the expression of psychological traits of social network users, based on the information collected in their accounts. The presented results can be used to create systems based on machine learning methods, which will allow predicting the evaluation of the severity of psychological traits. The existing methods and approaches in this field are also considered.

Keywords: psychological characteristics of users; social networks; information security; social engineering attacks.

Введение. Вопрос оценки выраженности психологических особенностей пользователей социальных сетей затрагивает многие сферы общества. Такие оценки могут быть полезны маркетологам, которые хотят понять, как лучше действовать, чтобы продать товар или сотрудникам отдела кадров, когда они хотят оценить человека перед принятием на работу. Однако самыми опасными интересантами в получении такой оценки являются социальные инженеры. Зная какие психологические особенности присущи пользователю, они могут подстроить социоинженерную атаку таким образом, чтобы максимизировать вероятность успешности её проведения. Например, зная, что человек имеет ярко выраженную эмоциональную нестабильность злоумышленник (социальный инженер) создаст ситуацию, вынуждающую человека принимать множества быстрых и важных решений для того, чтобы он потерял контроль над собой и выполнил нужные злоумышленнику действия.

Оценка выраженности психологических особенностей в классическом своём виде происходит косвенно — через прохождения человеком опросников и тестов. Такие опросники и тесты моделируют представление человека в виде выраженности его черт.

На данный момент существует множество опросников и тестов — Большая пятерка, 16-факторный личностный опросник Кеттела, Миннесотский многоаспектный личностный опросник, NEO PI-R и другие. Однако вопрос выбора оптимальной модели представления психологических особенностей человека является всё ещё открытым. Помимо этого, окончательно не выработаны методы и подходы по косвенной оценки психологических особенностей по информации, не связанной с опросниками и тестами. К такой информации также относиться информация, полученная из социальных сетей, в частности из аккаунтов пользователей. В свою очередь, социальные сети являются огромным источником информации о пользователях.

Для построения системы, которая сможет строить оценку выраженности психологических особенностей по аккаунтам пользователей в социальных сетях необходимо произвести математическую формализацию данной системы. Пусть $x \in X$ — множество характеристик аккаунта пользователя (анкетные данные; количество друзей; посты с текстовой, графическим, музыкальным наполнением; фотографии пользователя; характеристики взаимодействия пользователя (лайки, репосты), список групп и их направленность и т.д.), а Y — множество характеристик результатов психологических тестов (Большая пятерка, 16-факторный личностный опросник Кеттела, Миннесотский многоаспектный личностный опросник, NEO PI-R и т.д.), тогда необходимо построить такую функцию PSY: $X \to Y$, которая бы позволила по характеристикам, извлеченным из аккаунта пользователя строить оценку его психологических особенностей.

В качестве функции PSY могут выступать методы машинного обучения с учителем, которые в соответствии с полученными на вход характеристиками аккаунта пользователя будут вычислять оценку выраженности их психологических особенностей пользователя. Однако для использования таких методов нужно решить две проблемы: преобразования входящего потока данных (входных характеристик) из «количественных» в «качественные» и разметки набора данных. Рассмотрим каждую проблему подробнее. Под преобразования входных характеристик подразумевается некоторая нормировка, которая позволит, применять полученные методы машинного обучения к различным (по количеству данных) аккаунтам. Например, к аккаунтам, у которых варьируется количество постов, фотографий, лайков и т.д. Под разметкой понимается получения численных характеристик оценки выраженности психологических особенностей пользователя. Т.е. прохождения им психологических тестов. Таким образом предполагаемые методы машинного обучения должны обучаться и предсказывать по следующим схемам: Человек->Акквунт->Метод->Модель

Существующие методы и подходы по оценки психологических особенностей можно выделить в несколько групп по типу используемой в них информации: по текстовым постам [1–3]; по изображениям [4]; по музыке [5]; по другой информации [6, 7]. Однако представленные подходы и методы имеют ряд недостатков: низкий охват аудитории, отсутствует автоматизация, учитывают только один тип характеристик аккаунтов и т.д.

Заключение. В представленной статье были рассмотрены вопросы формализация задачи выявления (оценки) выраженности психологических особенностей пользователей социальных сетей по информации, собранной в их аккаунтах. Представленные результаты могут быть использованы для создания систем, основанных на методах машинного обучения, которые позволят предсказывать оценку выраженности психологических особенностей. Также рассмотрены существующие методы и подходы в данной области.

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № 0073-2019-0003, при финансовой поддержке РФФИ проект №20-07-00839; поддержана Санкт-Петербургским государственным университетом, проект № 73555239.

СПИСОК ЛИТЕРАТУРЫ

1. Тулупьева Т.В., Тафинцева А.С., Тулупьев А.Л. Подход к анализу отражения особенностей личности в цифровых следах // Вестн. психотерапии. 2016. № 60 (65). С. 124–137.
2. Татарникова Т.М., Богданов П.Ю. Построение психологического портрета человека с применением технологий обработки естественного языка // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 1. С. 85–91. doi: 10.17586/2226-1494-2021-21-1-85-91
3. Тулупьева Т.В., Суворова А.В., Азаров А.А., Тулупьев А.Л., Бордовская Н.В. Возможности и опыт применения компьютерных инструментов в анализе цифровых следов студентов-пользователей социальной сети // Компьютерные инструменты в образовании. 2017. №5. С. 3–13.
4. Бушмелев Ф.В., Абрамов М.В., Тулупьева Т.В. Адаптированный метод цветовых выборов в применении к изображениям из социальных медиа // Нечеткие системы, мягкие вычисления и интеллектуальные технологии (НСМВИТ-2020). 2020. С. 154-163.
5. Абрамов М.В., Азаров А.А. Выявление психологических особенностей пользователей социальных сетей на основании музыкальных предпочтений. // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM-2017). Санкт-Петербург.

Том 1-2. Т. 1. 2017. С. 130–133.
6. Lima, A.C.E.S., de Castro, L.N.: A multi-label, semi-supervised classification approach applied to personality prediction in social media // Neural Networks. 2014. № 58. P. 122–130. doi: 10.1016/j.neunet.2014.05.020
7. Liu, S.M., Chen, J.-H.: A multi-label classification-based approach for sentiment classification // Expert System Appl. №42(3). P. 1083–1093

УДК 004.8

АЛГЕБРАИЧЕСКИЕ БАЙЕСОВСКИЕ СЕТИ: ОБУЧЕНИЕ СТРУКТУРЫ СЕТИ

Харитонов Никита Алексеевич
Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mail: nak@dscs.pro

Аннотация. Алгебраические байесовские сети относятся к классу вероятностных графических моделей, которые служат для представления неточности и неопределенности знаний. Работа посвящена имплементации PC-алгоритма обучения структуры сети.

Ключевые слова: математическое обучение, вероятностные графические сети, алгебраические байесовские сети, PC-алгоритм, структурное обучение.

ALGEBRAIC BAYESIAN NETWORKS: NETWORK STRUCTURE TRAINING

Kharitonov Nikita
Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mail: nak@dscs.pro

Abstract. Algebraic Bayesian networks are one of the probabilistic graphical models. The last are used for the processing of information with uncertainty. This work is dedicated to the implementation of PC-algorithm of algebraic Bayesian network structure training.

Keywords: machine learning; probabilistic graphical networks; algebraic Bayesian networks; PC-algorithm; structure training.

Алгебраические байесовские сети относятся к классу вероятностных графических моделей, которые служат для представления неточности и неопределенности знаний.

Одной из основных концепций, используемых в рамках работы с алгебраическими байесовскими сетями, является декомпозиция знаний, в связи с чем они представляются в виде набора фрагментов знаний. Каждый фрагмент знаний является малой, но тесно связанной частью информации о предметной области, что выражается в его математическом представлении в виде идеала конъюнктов, дизъюнктов или набора квантов. Каждому элементу фрагмента знаний сопоставляется скалярная или интервальная оценка вероятности истинности. Алгебраическая байесовская сеть представляется в виде набора фрагментов знаний одного типа, при этом описаны процессы преобразования фрагментов знаний из одного типа в другой [1,2].

Алгебраическая байесовская сеть может быть представлена как ненаправленный граф с фрагментами знаний в узлах. Данное представление называется вторичной структурой алгебраической байесовской сети [1,2].

Основными операциями, проводимыми с алгебраическими байесовскими сетями, являются априорный вывод, то есть получение оценок вероятности пропозициональной формулы на основе представленных в сети оценок, апостериорный вывод, являющийся обновлением оценок сети на основе поступившего свидетельства, а также собственно обучение алгебраической байесовской сети. Последнее делится на обучение оценок вероятности истинности и на обучение структуры сети.

В работе описана имплементация PC-алгоритма обучения структуры сети, представленного ранее, на языке python. Изучается время работы алгоритма в зависимости от размера входных данных. Представленные результаты планируется использовать в практических применениях алгебраических байесовских сетей, в частности в рамках изучения защищенности пользователя от социоинженерных атак [4].

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № 0073-2019-0003, при финансовой поддержке РФФИ проект №20-07-00839; поддержана Санкт-Петербургским государственным университетом, проект № 73555239.

СПИСОК ЛИТЕРАТУРЫ

1. Тулупьев А.Л., Николенко С.И., Сироткин А.В. Байесовские сети: логико-вероятностный подход. — СПб.: Наука, 2006. 607 с.
2. Тулупьев А.Л., Сироткин А.В., Николенко С.И. Байесовские сети доверия: логико-вероятностный вывод в ациклических направленных графах. — СПб.: Изд-во С.-Петерб. ун-та, 2009.
3. Харитонов Н.А., Тулупьев А.Л. PC-алгоритм обучения вторичной структуры алгебраической байесовской сети // сборник материалов конференции КИИ-2021 [в печати]
4. Khlobystova A., Abramov M. The models separation of access rights of users to critical documents of information system as factor of reduce impact of successful social engineering attacks // CEUR Workshop Proceedings, 2020, 2782, стр. 264–268.

УДК 004.056

ЧАТ-БОТ ДЛЯ НАВИГАЦИИ АБИТУРИЕНТОВ: ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Хлобыстова Анастасия Олеговна[1,2], Евдокимов Данил Сергеевич[2]
[1] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия
[2] Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия
e-mails: aok@dscs.pro, st084331@student.spbu.ru

Аннотация. В статье рассматриваются возможные методы защиты чат-ботов от различных атак (DoS, флуд и спам-атаки) и их предотвращение на примере разрабатываемого Telegram-бота для абитуриентов СПбГУ, предназначенного для помощи в поиске необходимой информации, связанной с поступлением.

Ключевые слова: чат-боты; спам-атаки; флуд-атаки; DoS-атаки; информационная безопасность.

CHATBOT FOR APPLICANT NAVIGATION: INFORMATION SECURITY ISSUES

Khlobystova Anastasia[1,2], Yevdokimov Danil[2]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[2] Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mails: aok@dscs.pro, st084331@student.spbu.ru

Abstract. The article discusses possible methods of protecting chat bots from various attacks (DoS, flooding and spam attacks) and their prevention using the example of the Telegram bot being developed for SPbU applicants, designed to help in finding the necessary information related to admission.

Keywords: chat bots; spam attacks; flood attacks; DoS attacks; Information Security.

Введение. В настоящее время информационная безопасность играет важную роль при разработке любой информационной системы [1, 2]. При этом каждый год отмечается рост числа кибератак, так в ежегодном отчете компании по информационной безопасности Positive Technologies [3] в 2020 году был зафиксирован рост числа атак на 51% по сравнению с 2019 годом. И как сообщает РБК Россия заняла второе место по числу кибератак в 2017 году [4], что еще раз подчеркивает необходимость разработки способов защиты и предотвращения данного рода преступлений для Российской Федерации. Стоит заметить, что огромную часть всех киберпреступлений составляют DoS-атаки. DoS-атаки — это класс хакерских атак, призванных довести до отказа вычислительную систему либо затруднить ее работу. По данным “Лаборатории Касперского” каждая шестая компания РФ в 2015 г. подвергалась DDoS-атаке [5]. В то же время согласно отчету Qrator Labs [6] интенсивность таких атак только растет, а их процент в социальных сетях остается практически неизменным, поэтому проблема DoS-атак по сей день остается актуальной.

С другой стороны, одной из тенденций современного мира является использование чат-ботов [7]. Согласно прогнозам экспертов, разговорный искусственный интеллект и, в частности, чат-боты станут незаменимым помощником для большинства организаций [8]. Несмотря на то, что в настоящее время чат-боты часто не представляют никакого практического интереса для хакеров [9], нельзя упускать из виду методы их защиты, потому как развитие новых технологий зачастую влечет за собой и новые мошеннические схемы. Обратим свое внимание, например, на Telegram-бота для СПбГУ, который призван помогать поступающим в поиске нужной информации, используя современные технологии машинного обучения и процессинга естественного языка. Такая помощь крайне необходима будущим студентам, так как для многих вузов удобство их сайта для рядового пользователя находится не на первом месте, например, в силу существующих регламентов по наполнению сайта. В связи с этим абитуриенты часто обращаются прямо в приемную комиссию, из-за чего скорость поиска необходимых знаний значительно замедляется, что в разы усложняет процесс поступления. Поэтому в самый ответственный момент — май, время подготовки документов к подаче в университеты, такой цифровой помощник не имеет права на перебои в работе и ошибки, которые могут случиться из-за недобросовестных пользователей решивших устроить атаку на бота, с целью выведения его из строя или замедления обработки запросов.

Защитные механизмы. Самым простым способом атаки является обычный спам. Хакер с помощью множества ботов отправляет запросы с разных аккаунтов, тем самым перегружая вычислительный мощности приложения. Мониторинг и анализ трафика одни из ключевых инструментов борьбы с вредоносным софтом. Данный механизм можно реализовать, например, с помощью вычисления временной разницы между запросами пользователя. Высокая частота запросов может сигнализировать о том, что запросы поступают не от человека, а от вредоносной программы, следовательно подключенный к ней аккаунт социальной сети необходимо внести в “чёрный список” и не реагировать на поступающие запросы. Рассредоточение и создание резервных источников вычислительной мощности может помочь в случае успешной DoS-атаки для продолжения работы даже при выведении из строя некоторых элементов. Из-за ошибок в логике работы программы появляется риск

возникновения уязвимостей, которые могут быть использованы для увеличения нагрузки на систему, вывода ее из строя или для получения доступа к конфиденциальным данным. Регулярные тестирования и борьба с уязвимостями могут снизить эффективность или вовсе предотвратить ряд различных кибератак. Один из самых эффективных способов защиты — это наращивание ресурсов. Чем больше потенциальная мощность — тем больше средств понадобится хакеру для нанесения вреда боту, соответственно это может предотвратить многие маломощные атаки без дополнительного вмешательства. Для некоторых ботов также может быть актуальной проблема перегрузки баз данных. Telegram-бот для СПбГУ, например, хранит параметр “язык общения с пользователем”. То есть кибератака может быть нацелена на выведения из строя с помощью переполнения базы данных бота. Данная уязвимость частично решается автоматической чисткой или архивацией данных о пользователях, которые давно не посылали запросы. Но данный подход не подойдет для новых обращений к боту, поэтому стоит комбинировать данный метод с наращиваем ресурсов памяти. Еще один немаловажный фактор — это использование методов социальной инженерии вместе с атакой или для последующей DoS-атаки. С помощью различных методов социоинженерии можно заставить человека ослабить защиту бота в каком-то аспекте, после чего нанести кибер удар. Или же вовсе бот сможет стать огромным источником информации для разного рода мошенников. Обманув человека, можно выманить у него данные необходимые для доступа к боту, украсть всю накопленную информацию или незаметно собирать новую. Как актуальный пример использования социоинженерии в синтезе с хакерскими атаками, можно привести недавно обнаруженную уязвимость некоторых банковских чат-ботов, которая позволяет получить персональные данные о пользователях, сообщает ТАСС с ссылкой на газету “Известие” [10]. В публикации не сказано какие именно уязвимости были использованы хакерами, но точно известно, что полученные данные: номер и срок действия карт, баланс счета и мобильный телефон клиента — стали отличным ресурсом для применения методов социальной инженерии интернет-мошенниками. В данном случае могут помочь как классические методы — повышение осведомленности персонала и населения о методах социоинженерии, так и комплексные подходы, направленные на выявление и устранение уязвимостей к социоинженерным атакам во всей информационной системе [11, 12].

Заключение. Таким образом, перечисленные методы и способы информационной защиты могут быть эффективно и просто использованы для создания устойчивых и безопасных чат-ботов. Но стоит заметить, что они не ограничиваются названными в этой статье, и вопросы изучения такого рода атак достойны внимания и дальнейшего изучения.

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № 0073-2019-0003, поддержана Санкт-Петербургским государственным университетом, проект № 75254082 и РФФИ (грант № 20-07-00839).

СПИСОК ЛИТЕРАТУРЫ

1. Carcary M., Doherty E., Conway G. A Capability Approach to Managing Organisational Information Security //ECCWS 2019 18th European Conference on Cyber Warfare and Security. – Academic Conferences and publishing limited, 2019. – Pp. 97−105.
2. Tun H., Lupin S., Thike A.M., Oo K.K. Analysis of Information Systems in the Context of their Security //International Conference on Cyber Warfare and Security. – Academic Conferences International Limited, 2018. – Pp. 561−569.
3. Актуальные киберугрозы: итоги 2020 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/#id2 (дата обращения: 06.10.2021).
4. Россия стала второй после США по количеству кибератак [Электронный ресурс]. URL:
5. https://www.rbc.ru/technology_and_media/13/06/2017/593a9a749a794766d6b11c54 (дата обращения: 07.10.2021).
6. 2015: каждая шестая компания в России подверглась DDoS-атакам [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/2015-kazhdaya-shestaya-kompaniya-v-rossii-podverglas-ddos-atakam/15027/ (дата обращения: 06.10.2021).
7. Отчет о проблемах и доступности интернета в 2018-2019 годах [Электронный ресурс]. URL: https://blog.qrator.net/ru/annual-report-18-ru_34/ (дата обращения: 06.10.2021).
8. Будущее чат-ботов: 10 исследований и прогнозы экспертов [Электронный ресурс]. URL: https://www.carrotquest.io/chatbot/future-of-chatbots/ (дата обращения: 07.10.2021).
9. Какое будущее ожидает чат-боты. Перспективы и предсказания [Электронный ресурс]. URL: https://apix-drive.com/ru/blog/marketing/chat-bots-future (дата обращения: 07.10.2021).
10. H. Halpin. The philosophy of Anonymous, 2013, P. 28.
11. Эксперты обнаружили уязвимость для атак мошенников в банковских чат-ботах [Электронный ресурс]. URL: https://tass.ru/ekonomika/12267947 (дата обращения: 07.10.2021).
12. Azarov A., Abramov M., Tulupyev A., Tulupyeva T. Models and algorithms for the information system’s users’ protection level probabilistic estimation //Proceedings of the First International Scientific Conference “Intelligent Information Technologies for Industry”(IITI’16). – Springer, Cham, 2016. – Pp. 39−46.
13. Фролова М.С., Корепанова А.А., Абрамов М.В. Оценка степени открытости пользователя социальной сети с применением экспертной модели на основе байесовской сети доверия // Сборник докладов XXIV Международной конференции по мягким вычислениям и измерениям (SCM-2021). М. СПб: СПбГЭТУ «ЛЭТИ». – 2021. – Т.1. – С. 69−73.

УДК 004.89

TELEGRAM -БОТ ДЛЯ ПОМОЩИ АБИТУРИЕНТАМ СПБГУ В НАВИГАЦИИ И ВЫБОРЕ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ УНИВЕРСИТЕТА

Хлобыстова Анастасия Олеговна[1,2], Чекалёв Артём Алексеевич[1], Тулупьева Татьяна Валентиновна[1,2]

[1] Санкт-Петербургский федеральный исследовательский центр Российской академии наук (СПб ФИЦ РАН)
14-я линия, В.О., 39, Санкт-Петербург, 199178, Россия

[2] Санкт-Петербургский государственный университет
Университетская наб., 7-9, Санкт-Петербург, 199034, Россия

e-mails: aok@dscs.pro, st087200@student.spbu.ru, tvt@dscs.pro

Аннотация. В статье представлены возможные решения для молодых людей, собирающихся поступать в высшее учебное заведение, но еще не выбравших конкретную образовательную программу. Также указаны уже существующие аналоги.

Ключевые слова: профориентация; Телеграм-бот; социальная сеть; тест.

A TELEGRAM-BOT FOR HELPING SPBU APPLICANTS WITH NAVIGATION AND CHOOSING THE UNIVERSITY'S EDUCATIONAL PROGRAMS

Khlobystova Anastasiia [1,2], Chekalev Artyom [1], Tulupyeva Tatiana [1,2]
[1] St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS)
39 14th line, Vasilievsky Island, St. Petersburg, 199178, Russia
[2] Saint Petersburg State University
7-9 Universitetskaya Emb, St. Petersburg, 199034, Russia
e-mails: aok@dscs.pro, st087200@student.spbu.ru, tvt@dscs.pro

Abstract. The article presents possible solutions for young people who are going to enter a higher education, but have not chosen a specific educational program yet. Existing analogues are also indicated.

Keywords: vocational guidance; Telegram bot; social network; test.

Введение. Одним из наиболее важных этапов в жизни каждого человека является выбор будущей профессии и, как следствие, определение направления подготовки (специальности). Опираясь на статистику последних лет [1, 2], с каждым годом в Санкт-Петербургский Государственный Университет поступает все больше выпускников: за 2020 год количество зачисленных абитуриентов достигло отметки в 9148 студентов, в 2021 году — более 10000. При этом, у абитуриентов часто возникает вопрос — какую из образовательных программ можно выбрать? Проблема, возникающая у будущих студентов, достаточно распространена — далеко не каждый может самостоятельно и осознанно выбрать направление подготовки, которое будет опираться и на интересы, и на знания абитуриента.

В современном мире для молодых людей важную роль в их жизнедеятельности играют социальные сети [3]. Благодаря ним появляется больше возможностей к взаимодействию между сверстниками, обмену информацией в развлекательных и образовательных целях. Одним из примеров социальных медиа является Telegram. Он сочетает в себе простой в использовании интерфейс, широкий набор функций и обмен информацией, находящийся под надежной защитой. Благодаря таким качествам Telegram очень популярен среди подростков. При этом, Telegram известен не только как мессенджер, но и как удобный информационный ресурс. Например, в данной социальной сети популярны боты и специальные программы-аккаунты, которые позволяют пользователю совершать как прикладные, так и рутинные действия.

В связи со всем вышеперечисленным актуальным является разработка и развитие проекта, который бы с одной стороны способствовал улучшению процесса выбора абитуриентом направления подготовки среди реализуемых в Санкт-Петербургском государственном университете, а с другой стороны оставался удобным и понятным для использования. Учитывая популярность социальной сети Telegram, было принято решение создать Telegram-бота, который осуществляет профориентационное тестирование пользователя, и в результате предлагает список наиболее подходящих для рассмотрения образовательных программ. При этом связь результатов теста и основной образовательной программы высшего образования может быть произведена на основе перечня применяемых профессиональных стандартов, указанных в общей характеристике образовательной программы. Следующим шагом исследования станет связь профориентационного тестирования и данных, которые могут быть получены из открытых источников — социальных сетей Вконтакте и Instagram. При этом предполагается произвести сбор данных, которые бы содержали с одной стороны информацию об результатах теста по профориентации, а с другой различные характеристики контента (текстового, графического, аудио или видео), размещаемого пользователем в своём профиле в социальной сети. После чего при помощи методов анализа данных и машинного обучения идентифицировать ключевые маркеры, метрики и предикторы контента, которые могли бы охарактеризовать склонность пользователя к той или иной профессии. Впоследствии это позволит по ссылке абитуриента на его профиль в социальных сетях выдавать ему информацию о наиболее подходящем для него направлении обучения. Кроме того, в дальнейшем могут быть применены уже существующие наработки по сопоставлению двух аккаунтов в разных социальных сетях [4] с целью сбора большего числа данных о пользователе, а также различные методы по восстановлению данных [5].

Обзор существующих решений. Первым шагом к реализации данного проекта является существующих аналогов. Данный обзор представлен в Таблице 1.

Обзор существующих Telegram-ботов для помощи абитуриентам ВУЗов:

– @studyinspb_bot (Предназначен для абитуриентов Санкт-Петербургских ВУЗов.): Бот позволяет пользователю найти образовательные программы Санкт-Петербургских университетов. Благодаря нему можно узнать количество бюджетных мест, балл прошлых лет, наличие общежития и многую другую полезную информацию;

– @deifmobot (Предназначен для студентов университета ИТМО): Бот отправляет в личные сообщения пользователю изменения в онлайн–платформе Центра дистанционного обучения. Есть возможность узнать о новых оценках и о баллах, начисленных за выполнение задач. Бот работает на базе университета ИТМО;

– @SPbPUbot (Предназначен для абитуриентов университета СПбПУ): Бот предоставляет информацию о поступлении в Санкт Петербургский Политехнический Университет. Можно узнать большое количество необходимой информации: какие нужны документы для поступления, проходные баллы прошлых лет, направления подготовки и т.д.

Помимо ботов, конечно, существуют и другие подходы для помощи абитуриентам в вопросе выбора специальностей. Например, на официальном сайте Высшей Школы Экономики выложен тест [6], способный помочь пользователю в выборе направления подготовки. В начале теста необходимо указать, собираетесь ли Вы поступать на бакалавриат или же в магистратуру, после чего задается 10 тематических вопросов. Затем сайт сканирует ответы и выводит ту область, в которой может быть заинтересован пользователь, а также предлагает специальность, информацию о которой можно также узнать, перейдя по ссылке.

Не менее значимым примером может послужить тест от Московского Государственного Технического Университета [7]. Сначала пользователю даётся список из 45 пар профессий, в каждой из которых ему предлагается выбрать одну. Важно, что необходимо среди всех пар выбрать ровно одну профессию, наиболее предпочтительную для пользователя, иначе переход к следующему вопросу теста не предстоит возможным. После того, как абитуриент отметил все варианты, ему предлагается поделиться адресом своей электронной почты, на которую придет результат профориентации. В письме будет подведена статистика ответов будущего студента: сколько баллов он набрал в каждой из 6 категорий. Затем пользователю можно прочитать о каждой категории, проанализировать результаты и выбрать направление подготовки, которые также прилагаются в письме.

При этом стоит отметить, что любой такой тест может хранить в себе и скрытую уязвимость. Так, например, злоумышленники-социоинженеры зачастую создают сайты-двойники для заполучения персональных данных, которые в дальнейшем используют для получения материальной выгоды [8, 9]. В свою очередь создание Telegram-бота способствовало бы снижению возникновения риска компрометации персональных данных абитуриентов.

Заключение. Таким образом, в статье была описана актуальная в настоящее время задача по разработке Telegram-бота, способствующего улучшению процесса ориентации абитуриента в существующих образовательных программах СПбГУ, а также предложена идея по подбору наиболее подходящего для него направления обучения на основе данных, извлекаемых из социальных сетей.

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН № 0073-2019-0003, поддержана Санкт-Петербургским государственным университетом, проект № 75254082 и РФФИ (грант № 20-07-00839).

СПИСОК ЛИТЕРАТУРЫ

1. Рекордный средний балл и небывалый конкурс: СПбГУ подвел итоги приемной кампании —2020 // СПбГУ [Электронный ресурс]. — URL: https://abiturient.spbu.ru/2553-rekordnyj-srednij-ball-i-nebyvalyj-konkurs-spbgu-podvel-itogi-priemnoj-kampanii-2020.html (Дата обращения: 25.09.2021)
2. Рекордное количество заявлений и первенство по иностранцам: СПбГУ подвел итоги приемной кампании — 2021 // СПбГУ [Электронный ресурс]. — URL: https://spbu.ru/news-events/novosti/rekordnoe-kolichestvo-zayavleniy-i-pervenstvo-po-inostrancam-spbgu-podvel-itogi (Дата обращения: 25.09.2021)
3. Доля пользователей интернета в России среди молодежи приблизилась к 100% // РБК [Электронный ресурс]. — URL https://www.rbc.ru/technology_and_media/12/01/2021/5ffde01e9a79478eb5230426 (Дата обращения: 25.09.2021)
4. Корепанова А.А., Олисеенко В.Д., Абрамов М.В., Тулупьев А.Л. Применение методов машинного обучения в задаче идентификации аккаунтов пользователя в двух социальных сетях //Компьютерные инструменты в образовании. — 2019. — №. 3. — С. 29−43
5. Корепанова А.А., Абрамов М.В. Применение случайного леса в выборе метода восстановления возраста пользователя социальной сети //Искусственный интеллект и принятие решений. — 2021. — №. 2. — С. 66−77.
6. Профориентационный тест // ВШЭ [Электронный ресурс]. — URL: https://admissions.hse.ru/test (Дата обращения: 25.09.2021)
7. Профориентационный тест // МГТУ [Электронный ресурс]. — URL: https://mgutm.ru/abiturient/abitur-2021/prof-test/ (дата обращения: 25.09.2021)
8. Сайты-двойники: как защититься от мошенников в интернете // ТАСС [Электронный ресурс]. — URL: https://tass.ru/press/12513 (Дата обращения: 26.09.2021)
9. Двойник Тинькова зазывает на сайт-фейк. Как не стать жертвой фишинга // РБК [Электронный ресурс]. — URL: https://quote.rbc.ru/news/article/6082f2149a79472a41c5ed2d (Дата обращения: 26.09.2021).

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

УДК 004.056

ОСОБЕННОСТИ АУТЕНТИФИКАЦИИ В СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ С АРХИТЕКТУРОЙ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ

Александрова Елена Борисовна, Облогина Анастасия Юрьевна
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: aleksandrova_eb@spbstu.ru, oblogina.ayu@edu.spbstu.ru

Аннотация. Рассматриваются особенности сетей Интернета вещей с архитектурой граничных вычислений, особое внимание уделено методам аутентификации для различных моделей взаимодействия участников сети.

Ключевые слова: интернет вещей; аутентификация; граничные вычисления; низкоресурсные устройства.

AUTHENTICATION FEATURES IN IOT NETWORK WITH THE EDGE COMPUTING ARCHITECTURE

Aleksandrova Elena, Oblogina Anastasiya
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mails: aleksandrova_eb@spbstu.ru, oblogina.ayu@edu.spbstu.ru

Abstract. The features of IoT networks with the Edge Computing architecture are considered, focused on authentication methods in various communication models between resource-constrained devices.

Keywords: internet of Things; authentication; Edge Computing; resource-constrained devices.

В настоящее время технологии Интернета вещей стали неотъемлемой частью повседневной жизни. Все чаще встречаются системы «Умный дом» и «Умный город», интеллектуальные устройства помогают качественно и быстро выполнять задачи в области медицины, спорта, транспорта. С таким стремительным выходом информационных технологий в реальную жизнь возникает вопрос о кибербезопасности подобных систем. Она имеет особую значимость, так как может иметь не только информационное, но и физическое воздействие.

Развитие Интернета вещей и стандарта передачи данных 5G, разработанного с целью поддержки интеллектуальных систем, привело к возникновению архитектуры граничных вычислений. Граничные вычисления – это принцип построения иерархической инфраструктуры, при котором вычислительные ресурсы частично или полностью перемещаются к границе сети. Популярность такой архитектуры растет и, несмотря на ее молодость и отсутствие зрелых решений в некоторых вопросах, она используется даже в крупных IT-компаниях [1]. Это обусловлено преимуществами, которые дают граничные вычисления сетям Интернета вещей. Идея смещения ресурсов к границе появилась в связи с ограничениями на взаимодействие с облачными серверами. Системы интеллектуальных устройств являются системами реального времени, выдвигая жесткие требования к скорости реакции на запрос. Сервера облачной инфраструктуры не могут обеспечить такой быстрый ответ по следующим причинам. Первая обусловлена географической удаленностью серверов. Учитывая значительное расстояние до физического расположения сервера, может потребоваться скорость передачи данных больше, чем скорость света, что невозможно. Вторая причина заключается в увеличении количества передаваемых и обрабатываемых данных, чем характеризуются сети Интернета вещей. Объем информации от множества устройств стал настолько велик, что облачных ресурсов становится недостаточно. Таким образом, оба ограничения приводят к необходимости децентрализованной обработки данных в логической и физической близости к самим устройствам.

Архитектура граничных вычислений предполагает, что между устройствами Интернета вещей и облачным сервером будет находиться граничный сервер. Причем он должен быть расположен максимально близко к устройству. В отличие от архитектуры туманных вычислений, где сервер выполняет только предварительную обработку данных до того, как они попадут в облако, граничные сервера являются самостоятельными, то есть способны выполнять запросы от устройств без обращения к облаку [2].

Такое решение предоставляет очень важное преимущество для сетей, узлами которых являются низкоресурсные устройства. Архитектура позволяет делегировать часть задач с устройства на граничный сервер.

Особенно это актуально в вопросах безопасности, так как протоколы, обеспечивающие защиту, часто требуют высоких энергозатрат или большого объема памяти.

Чтобы это преимущество было применимым на практике, необходимо создать новые или адаптировать существующие механизмы безопасности, которые будут учитывать неравномерное распределение вычислительной нагрузки на различных участников сети [3].

Одним из основных методов обеспечения безопасности в вычислительных системах является аутентификация. В рамках сетей Интернета вещей следует обращать особое внимание на этот механизм защиты, так как нарушение проверки подлинности одного или нескольких участников сети может привести к нарушению не только конфиденциальности, но также целостности и доступности системы, что может повлечь негативные киберфизические последствия..

В силу того, что архитектура граничных вычислений отличается от традиционной облачной инфраструктуры, протоколы аутентификации должны решать дополнительные задачи. В первую очередь, следует учесть распределение нагрузки, делегируя максимальное количество задач от устройств граничному серверу.

Также следует учитывать, что граничный сервер не должен иметь такой же уровень доверия, как и облачный. Архитектура граничных вычислений предполагает распределенную систему из большого количества серверов. Следовательно, невозможно обеспечить каждому достаточную физическую защиту, как делают с облаками. Несмотря на то, что граничный сервер располагает достаточными ресурсами, чтобы защититься от различного рода атак, в том числе и по побочным каналам, необходимо принять во внимание возможность подмены и, следовательно, проводить проверку подлинности сервера.

В настоящее время предложено несколько протоколов аутентификации, которые преимущественно отличаются своими концептуальными моделями. Авторы публикаций [4, 5] в качестве главной цели своих протоколов ставят задачу аутентификации устройства на граничном сервере. Такой подход способен защитить сеть Интернета вещей от недостоверных данных или от нелегитимных команд, однако не позволит выполнять проверку подлинности сервера, а также проводить проверку доступа управляющих устройств к исполнительным. Авторы работы [5] предлагают специальный протокол для сетей VANET, учитывающий высокую скорость перемещения участников.

В работе [6] предлагается проводить аутентификацию устройства на облачном сервере через граничный. Такой механизм тоже может стать необходимым в рамках архитектуры, однако использоваться он будет гораздо реже, чем модель взаимодействия между устройствами.

Авторы публикации [7] предлагают PHY-аутентификацию на основе данных о состоянии канала связи. Устройствам не требуется проходить аутентификацию как таковую, их подлинность доказывают характеристики соединения. Для проверки устройства на граничном сервере реализована нейронная сеть с глубоким обучением, способная отличить злоумышленников от легитимных пользователей. Однако в чистом виде это решение неприменимо вычислительных системах, так как ошибки нейронной сети могут привести к проблемам с доступностью. Тем не менее сама идея является перспективной для сетей с низкоресурсными устройствами.

Очень актуальной является проблема взаимной аутентификации управляющего и исполняемого устройств, которые обмениваются данными через граничный сервер. Управляющее устройство отправляет команды на выполнение исполняемому и получает данные от него. В качестве управляющей стороны чаще выступает мобильное устройство, которое не всегда способно поддерживать все разнообразие протоколов взаимодействия с устройствами. Поэтому весь обмен данными целесообразно осуществлять именно через граничный сервер.

Такая модель взаимодействия является очень популярной в сетях Интернета вещей. Однако до сих пор не существовало механизма аутентификации, который смог бы проверить подлинность участников и граничного сервера, а также предотвратить доступ легитимных управляющих устройств к чужим устройствам.

Для решения этой проблемы был разработан протокол аутентификации, удовлетворяющий вышеперечисленным требованиям [8]. Он обеспечивает стойкость к различным атакам и приемлемую скорость выполнения для сетей Интернета вещей. Разработка позволяет выполнять проверку подлинности управляющего устройства на исполняемом через граничный сервер. Важное отличие от многих существующих решений заключается в проверке самого сервера на основе протокола цифровой подписи и характеристик соединения.

Данный протокол учитывает особенности архитектуры граничных вычислений, а именно неравномерное распределение нагрузки на участников сети и возможность подмены граничного сервера. Более того, решение не требует передачи и хранения данных, связанных непосредственно с сервером, что делает протокол применимым в сетях Интернета вещей, участники которых, такие как дроны, беспилотные автомобили и т.п., характеризуются быстрым перемещением и сменой сети

Таким образом, применение разработанного протокола аутентификации делает возможным безопасное взаимодействие устройств в рамках технологий Интернета вещей.

СПИСОК ЛИТЕРАТУРЫ

1. Edge computing for IoT. A guide on how edge computing complements the cloud in IoT [Электронный ресурс]. – 2020. – URL: https://bosch.io/resources/white-paper/iot-edge-computing (дата обращения 10.04.2021).
2. Cloud, Fog and Edge Computing – What's the Difference? [Электронный ресурс]. – 4.14.2017. – URL: https://www.winsystems.com/cloud-fog-and-edge-computing-whats-the-difference/ (дата обращения 15.06.2021).
3. Sha K., Yang T. A.,Wei W., Davari S. A survey of edge computing based designs for IoT security //Digital Communications and Networks. – 2019. – V.6. – №.2. – P.195-202.

4. Nakkar M., AlTawy R., Youssef A. Lightweight Broadcast Authentication Protocol for Edge-Based Applications //IEEE Internet Of Things Journal – 2020. – V.7. – №.12. – P.11766-11777
5. Yang A., Weng J., Yang K., Huang C., Shen X. Delegating Authentication to Edge: A Decentralized Authentication Architecture for Vehicular Networks // IEEE Transactions On Intelligent Transportation Systems – 2020. – P.1-15.
6. Shahidinejad A., Ghobaei-Arani M., Souri A., Shojafar M., Kumari S. Light-Edge: A Lightweight Authentication Protocol for IoT Devices in an Edge-Cloud Environment //IEEE Consumer Electronics Magazine – 2021
7. Liao R. F. et al. Security enhancement for mobile edge computing through physical layer authentication //IEEE Access. – 2019. – Т. 7. – С. 116390-116401.
8. Александрова Е.Б., Облогина А.Ю., Шкоркина. Е.Н. Аутентификация управляющих устройств в сети Интернета вещей с архитектурой граничных вычислений //Проблемы информационной безопасности. Компьютерные системы. – 2021. – № 2. – С. 82-88.

УДК 004

ВНЕДРЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ЖИЗНЕДЕЯТЕЛЬНОСТЬ ОБЩЕСТВА И НЕОБХОДИМОСТЬ СОЗДАНИЯ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ПРИНЯТИЯ УПРАВЛЕНЧЕСКОГО РЕШЕНИЯ

Бурлов Вячеслав Георгиевич[1], Грачев Михаил Иванович[2], Капицын Сергей Юрьевич[3], Абрамов Валерий Михайлович[4]

[1] Государственный университет морского и речного флота имени адмирала С.О. Макарова
Двинская ул., 5/7, Санкт-Петербург, 198035, Россия
[2] Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
[3] Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
[4] Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mails: burlovvg@mail.ru, mig2500@mail.ru, wolf.76@bk.ru, val.abramov@mail.ru

Аннотация. Рассматриваются процессы все большего внедрения информационных технологий в жизнедеятельность человека и общества, что приводит к усложнениям системы управления и необходимости создания математической модели управления позволяющей добиться необходимого уровня эффективности принятия управленческих решений.

Ключевые слова: математическая модель; управление; цифровизация общества; информационные системы и технологии; безопасность системы.

INTRODUCTION OF INFORMATION TECHNOLOGIES INTO THE LIFE OF SOCIETY AND THE NEED TO CREATE A MATHEMATICAL MODEL OF MANAGERIAL DECISION-MAKING

Burlov Vyacheslav[1], Grachev Mikhail[2], Kapitsyn Sergey[3], Abramov Valery[4]

[1] Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya St, St. Petersburg, 198035, Russia
[2] St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
[3] Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
[4] Russian State Hydrometeorological University
79 Voronezhskya St, St. Petersburg, 192007, Russia
e-mails: burlovvg@mail.ru, mig2500@mail.ru, wolf.76@bk.ru, val.abramov@mail.ru

Abstract. The processes of increasing introduction of information technologies into the life of a person and society are considered, which leads to complications of the management system and the need to create a mathematical management model that allows achieving the necessary level of efficiency of managerial decision-making.

Keywords: mathematical model; management; digitalization of society; information systems and technologies; system security.

Все большее внедрение информационных технологий в жизнедеятельность общества приводит к автоматизации процессов производства и управления во всех сферах деятельности человека и общества в том числе и в социальных и экономических системах (СЭС), например, в таких как образование.

Эволюция развития машин провела к возможности проведения операций, которые превышают возможности человека как в мирное, так и в военное время. Так появление интернета и информационных технологий ознаменовало новую эру в развитии человечества. Интернет, предоставляющий людям новые способы общения по всему миру через компьютерные сети, открыл колоссальные возможности по управлению и взаимодействию между людьми.

Количество подключенных к Интернету устройств в повседневной жизни мы стали называть «умными устройствами» уже превышает численность населения планеты. Многие из этих устройств позволяют производить управление автомобилями, самолетами, приборами, интеллектуальными электрическими сетями,

плотинами, промышленными системами и даже многонациональными инфраструктурами, такими как трубопроводы, транспорт и торговля, развитое программное обеспечение позволяет проводить дистанционное обучение курсантов и слушателей. Эта тенденция к распределенным системам «умных устройств», подключенных к Интернету, в последнее время ускорилась с появлением Интернета вещей в качестве его основы. Целью Интернета вещей является подключение любого устройства к другому в любое время по любому протоколу из любой точки мира.

Автоматизация умного дома является ярким примером интеллектуальной среды, построенной на различных типах кибер-физических систем.

Современное развитие технологий неизменно упрощают нашу жизнь. Мы уже не можем себе представить, как обходиться без смартфона или компьютера. С помощью техники мы оплачиваем счета, не выходя из дома, покупаем одежду и еду, и это всего лишь малая часть.

А теперь представьте, что все устройства, которыми вы пользуетесь будут подключены к Интернету. Не только уже ставшие привычными нам смартфоны и компьютеры, но и остальная техника: колонки, жалюзи, кухонная плита, дверные замки, окна, лампочки. И все эти устройства обмениваются информацией между собой, передают ее вам и выполняет ваши команды по средствам нажатием одной кнопки. Нельзя не упомянуть тот факт, что можно управлять приборами в доме с помощью мобильного телефона, даже будучи далеко от дома.

Развитие данных технологий несомненно представляет собой удобство, но не менее важным критерием при их использовании остается их безопасность, так как при проведении кибер атаки, можно стать заложником ситуации. В этом случае у человека управляющего системой должна быть модель управленческого решения, позволяющего достигать цель управления в необходимые временные рамки.

Таким образом, для противодействия возникающим угрозам в системе управления желательно располагать математической модель управленческого решения, позволяющая противодействовать возникающим угрозам в системе и достигать поставленной цели управления с заданным уровнем эффективности принятия решения.

СПИСОК ЛИТЕРАТУРЫ

1. Бурлов В.Г., Грачев М.И. Разработка математической модели управленческого решения руководителя высшего учебного заведения, учитывающей возможности Web-технологий//Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 212-216.
2. Бурлов В.Г., Грачев М.И. Модель управления транспортными системами, учитывающей возможности инноваций. Технико-технологические проблемы сервиса. 2017. № 4 (42). С. 34–38.
3. Бурлов В.Г., Грачев М.И., Примакин А.И. Внедрение информационных технологий в процесс обучения как необходимость. В сборнике: Региональная информатика "РИ-2018" материалы конференции. 2018. С. 360-361.
4. Бурлов В.Г., Грачев М.И. Разработка математической модели управленческого решения руководителя высшего учебного заведения, учитывающей возможности Web-технологий//Региональная информатика и информационная безопасность. Сборник трудов. Санкт-Петербургское общество информатики, вычислительной техники, систем связи и управления. 2016. С. 212-216.
5. Бурлов В.Г., Грачев М.И. Модель управленческого решения как перспективное направление в обеспечении информационной безопасности. В сборнике: Информационная безопасность: вчера, сегодня, завтра. Сборник статей по материалам III Международной научно-практической конференции. Москва, 2020. С. 153-157.
6. Burlov V.G., Grachev M.I. Model of transport systems management, taking into account the possibilities of innovation. Technical and technological problems of service. 2017, vol. 42. no. 4, pp. 34-38. (in Russian) DOI: 10.1016/j.trpro.2017.01.023
7. Имитационная модель управления образовательной организацией высшего образования / М. И. Грачев, В. Г. Бурлов, О. Е. Чудаков, А. И. Примакин // XXI век: итоги прошлого и проблемы настоящего плюс. – 2021. – Т. 10. – № 1(53). – С. 57-62. – DOI 10.46548/21vek-2021-1053-0010.
8. Бурлов, В. Г. Оценивание эффективности принятия управленческих решений в социально-экономических системах на примере учебного заведения высшего образования / В. Г. Бурлов, М. И. Грачев // T-Comm: Телекоммуникации и транспорт. – 2020. – Т. 14. – № 2. – С. 32-38. – DOI 10.36724/2072-8735-2020-14-2-32-38.
9. Модель управления в социальных и экономических системах с учетом воздействия на информационные процессы в обществе / В. Г. Бурлов, М. И. Грачев, М. Н. Васильев, С. Ю. Капицын // T-Comm: Телекоммуникации и транспорт. – 2020. – Т. 14. – № 5. – С. 46-55. – DOI 10.36724/2072-8735-2020-14-5-46-55.
10. Бурлов, В. Г. Аналитическо-динамическая модель управленческого решения в социально-экономических системах на примере руководителя учебного заведения высшего образования / В. Г. Бурлов, М. И. Грачев // T-Comm: Телекоммуникации и транспорт. – 2019. – Т. 13. – № 10. – С. 27-34. – DOI 10.24411/2072-8735-2018-10314.
11. Беженцев, А. А. Внедрение новых информационных технологий в образовательный процесс на основе использования учебных полигонов мониторинговый центр и ситуационный центр / А. А. Беженцев, В. Г. Бурлов, М. И. Грачев // T-Comm: Телекоммуникации и транспорт. – 2020. – Т. 14. – № 7. – С. 36-41. – DOI 10.36724/2072-8735-2020-14-7-36-41.

УДК 004.056

ПРОБЛЕМЫ БЕЗОПАСНОСТИ СЕТЕЙ НА ОСНОВЕ НАМЕРЕНИЙ

Лаврова Дарья Сергеевна, Попова Елена Александровна
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: ep@ibks.spbstu.ru, lavrova_ds@spbstu.ru

Аннотация. В работе рассмотрены назначение и основные характеристики сетей на основе намерений, выделены основные отличия сетей на основе намерений от традиционного подхода к построению сетевых архитектур, а также сформулированы основные преимущества использования сетей на основе намерения. Также был проведен анализ актуальных исследований в области обеспечения безопасности таких сетей, выделены

основные проблемы безопасности, возникающие при переходе к построению сетевых инфраструктур к парадигме сетей на основе намерений.

Ключевые слова: сети на основе намерений; сетевая инфраструктура; информационная безопасность.

SECURITY ISSUES OF INTENT-BASED NETWORKS

Lavrova Daria, Popova Elena
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mails: ep@ibks.spbstu.ru, lavrova_ds@spbstu.ru

Abstract. The paper considers the purpose and main characteristics of intent-based networks, highlights the main differences between intent-based networks and the traditional approach to building network architectures, and formulates the main advantages of using intent-based networks. An analysis of current research in the field of ensuring the security of such networks was also carried out, the main security problems arising in the transition to the construction of network infrastructures to the paradigm of networks based on intentions were highlighted.

Keywords: intent-based networks; network infrastructure; information security.

Сети на основе намерений являются новой концепцией построения сетевых архитектур, предназначенная для настройки IT-инфраструктуры с учетом назначения бизнес-процессов и участия сетевого администратора в настройки инфраструктуры [1]. Концепция сетей на основе намерений подразумевает, что при указании администратором намерения сеть реализует его самостоятельно за счет использования интегрированных средств автоматизации и методов искусственного интеллекта. По словам экспертов Cisco, концепция сети на основе намерения предполагает использование встроенных функций безопасности и интеграцию с решениями сетевой безопасности. Однако недостаточная изученность данных сетей приводит к возникновению следующих проблем информационной безопасности [2]:

1. Проблема согласования политик. Эта проблема касается как согласования бизнес-политик и политик безопасности, так и бизнес-политик в рамках одной сложной крупномасштабной сети, в которой функционирует сразу несколько контроллеров.
2. Проблема некорректной трансляции намерений в политики. Сочетание высокоуровневых намерений с конкретными техническими изменениями в конфигурации сети требует использования точной и недвусмысленной модели трансляции.
3. Проблема уязвимости к DoS-атакам единой точки отказа – контроллера IBN, что влечет потерю контроля над работой всей сети и невыполнение критически важных бизнес-процессов.
4. Проблема несанкционированного воздействия на контроллер, в частности, на реализуемую им стратегию, что может привести к невыполнению ряда бизнес-задач или к их некорректному выполнению.
5. Проблемы безопасности, характерные для технологии искусственного интеллекта (ИИ). К спектру возможных воздействий нарушителя на ИИ относятся, например, манипуляция входными данными (как обучающими, так и тестовыми), ошибки в реализации логики работы механизма принятия решения средством ИИ.

Проблема обеспечения киберустойчивости сетей на основе намерения может быть отчасти решена применением методов саморегуляции и их реализацией в рамках стратегии IBN-контроллера.

Таким образом, сетевая концепция IBN может обеспечить более гибкое функционирование сетевых технологий при условии заранее определенного комплекса методов и сценариев устранения определенных проблем безопасности.

Исследование выполнено в рамках стипендии Президента РФ молодым ученым и аспирантам СП-1932.2019.5.

СПИСОК ЛИТЕРАТУРЫ

1. Сеть на основе намерения. Устранение разрыва между бизнесом и IT [Электронный ресурс]. – URL: https://www.cisco.com/c/dam/global/ru_ru/solutions/ enterprise-networks/c11-740210-00_ibn_wp_v2a.pdf
2. Jain R. The State of Intent-Based Networks [Электронный ресурс]. – URL: https://www.cse.wustl.edu/~jain/cse570-19/ftp/intent/index.html

УДК 004.056

ЗАЩИТА ОТ СЕТЕВЫХ АТАК НА КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ НА ОСНОВЕ НЕЙРОЭВОЛЮЦИОННЫХ АЛГОРИТМОВ

Фатин Александр Денисович, Павленко Евгений Юрьевич
Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
e-mails: sasha-fatin@mail.ru, pavlenko@ibks.spbstu.ru

Аннотация. Авторами предложен подход к обеспечению безопасности киберфизических систем, направленный на сохранение способности системы к корректному функционированию в условиях кибератак. В основе подхода лежат принципы молекулярно-генетической системы управления и саморегуляции живой ткани.

Ключевые слова: киберфизическая система; молекулярно-генетическая система управления; саморегуляция; многомерные временные ряды; IoT; нейроэволюционные алгоритмы; NEAT; информационная безопасность.

PROTECTION AGAINST NETWORK ATTACKS ON CYBERPHYSICAL SYSTEMS BASED ON NEUROEVOLUTIONARY ALGORITHMS

Fatin Alexander, Pavlenko Evgeny
Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
e-mails: sasha-fatin@mail.ru, pavlenko@ibks.spbstu.ru

Abstract. The authors propose an approach to ensuring the security of cyber-physical systems, aimed at preserving the system's ability to function correctly in conditions of cyber-attacks. The approach is based on the principles of the molecular genetic system of control and self-regulation of living tissue.

Keywords: cyber-physical system; molecular genetic control system; self-regulation; multidimensional time series; IoT; neuroevolution; NEAT; information security.

В работе рассматривается метод выявления аномального поведения в работе киберфизических систем (КФС) с помощью предсказания и анализа многомерных временных рядов средствами нейроэволюционных алгоритмов.

Использовался набор данных [1], включающий в себя состояния, передаваемые данные и конечных получателей данных каждого из анализируемых устройств сети. Размерность многомерного временного ряда составила 28 (для каждого из 7 устройств и 4 конечных базисов каждого устройства).

Анализируемый период работы системы включает 4 периода функционирования по 48 часов (1 период в нормальном состоянии и 3 периода, в течение которых дискретно проводились атаки разных типов на систему).

Изначально составлялся классический многомерный временной ряд, где каждое значение временного ряда было представлено вектором обработанных и нормированных данных.

Рассматриваемая нейросеть строилась и обучалась по алгоритму гиперкуба с использованием библиотеки NEAT-Python языка Python, где роль реконфигуратора сети выполнялась генетической составляющей алгоритма.

Для расчета ошибки между предсказанным состоянием системы и реальным выполнялся следующий ряд действий: вычисление разницы между предсказанным и реальным значением многомерного временного ряда, характеризующего общее состояние системы; выявление аномального поведения на основе условия превышения значения ошибки предсказанного и реального состояния более чем на фиксированную величину, где под фиксированной величиной понимается пороговое значение проявления аномального поведения в системе.

Пороговая величина ошибки определялась эмпирически и составила в данном случае 0,4. При данном значении доля обнаруженных аномалий составила 93%. Ошибка первого рода составила 0,12, второго – 0,01.

Таким образом, использование механизма NEAT-гиперкуба на основе нейроэволюционного процесса продемонстрировало возможность эффективного детектирования аномального поведения в КФС. Данный подход не уступает в эффективности классическим подходам, основанным на статистических инструментах [2] и механизмах машинного обучения [3]. Данные результаты обусловлены возможностью перестроения сэндвич-структуры нейроэволюционной сети в процессе стагнации поиска решения и возможностью оптимизации процесса поиска генетической составляющей NEAT-алгоритма путём регулирования механизмов скрещивания.

Дальнейшим направлением развития является создание модели потока данных КФС на основе гиперкуба с возможностью самовосстановления по адаптивному графу.

Исследование выполнено в рамках стипендии Президента РФ молодым ученым и аспирантам СП-1689.2019.5.

СПИСОК ЛИТЕРАТУРЫ

1. TON_IOT DATASETS. – URL: https://ieee-dataport.org/documents/toniot-datasets (дата обращения: 12.01.2021).
2. Tulone D., Madden S. PAQ: Time series forecasting for approximate query answering in sensor networks / D. Tulone, S. Madden // Wireless Sensor Networks: Third European Workshop, EWSN 2006, Zurich, Switzerland, 2006. – pp. 21-37.
3. Detecting Spacecraft Anomalies Using LSTMs and Nonparametric Dynamic Thresholding / K. Hundman, V. Constantinou, Ch. Laporte, I. Colwell, T. Soderstrom //KDD '18: Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. – 2018. – pp. 387–395.

УДК 004.056

ПОДХОД К СРАВНЕНИЮ ПАТТЕРНОВ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ НА ОСНОВЕ АНАЛИЗА РАСПРЕДЕЛЕНИЯ МНОГОМЕРНЫХ ДАННЫХ В ПРОСТРАНСТВЕ

Шулепов Антон Андреевич[1,2],Новикова Евгения Сергеевна[1]
[1] Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
[2] НИЦ Радиотехники
Матроса Железняка ул., 57, Санкт-Петербург, Россия, 197343
e-mails: ao-shyleo@yandex.ru, novikova.evgenia123@gmail.com

Аннотация. Методы визуализации, основанные на методах проецирования многомерных данных, часто применяются для исследования разнородных данных с нескольких датчиков системы. Их можно использовать для создания графических паттернов как нормальных, так и ненормальных состояний функционирования системы. Однако необходимо определить показатели и критерии для оценки состояния системы для обнаружения типичных закономерностей и выбросов.

Ключевые слова: обнаружение аномалий; поведение объекта; многомерная проекция данных; триангуляция Делоне; анализ состояния системы.

AN APPROACH TO COMPARING PATTERNS OF SYSTEM FUNCTIONING BASED ON ANALYSIS OFDISTRIBUTION OF MULTI-DIMENSIONAL DATA IN SPACE

Shulepov Anton[1,2], Novikova Evgenia[2]
[1] Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
[2] Research & Engineering Centre of Radiotechnics (“NIC Radiotechniki”)
57 Matrosa Zheleznyaka St, St. Petersburg, 197343, Russia
e-mails: ao-shyleo@yandex.ru, novikova.evgenia123@gmail.com

Abstract. Visualization techniques based on multidimensional data projection techniques are often used to explore heterogeneous data from multiple sensors in a system. They can be used to create graphical patterns of both normal and abnormal states of a system's functioning. However, it is necessary to define indicators and criteria for assessing the state of the system in order to detect typical patterns and outliers**.**

Keywords: anomaly detection; object behavior; multidimensional data projection; Delaunay triangulation; system state analysis.

Визуализация данных облегчает анализ и оценку аномалий с использованием различных интерактивных визуальных моделей и интуитивного представления предметной области, что обеспечивает дополнительные доказательства для подтверждения или опровержения гипотез, выдвинутых аналитиком [1]. Однако эффективность основанных на визуализации методов обнаружения паттернов и аномалий зависит от выбранных визуальных моделей и методов автоматического обнаружения аномалий. Если многомерная точка представляет собой состояние сложного объекта, характеризуемого множеством атрибутов в некоторый момент времени, тогда группа точек может рассматриваться как точки, описывающие некоторые типичные состояния объекта, в то время как выбросы могут уведомлять о некоторых отклонениях в поведении объекта [2, 3]. Эта идея может быть использована при построении моделей визуализации для мониторинга сложного объекта, поскольку они, с одной стороны, позволяют уменьшить начальный размер пространства данных, таким образом уменьшая когнитивную нагрузку, а с другой стороны, поддерживают обнаружение закономерностей и аномалий в поведении объекта.

В работе исследуется триангуляция Делоне для сравнения распределения точек, полученных с помощью методов уменьшения размерности. В качестве метода снижения размерности применяется метод главных компонент PCA. Эксперименты показали, что использование триангуляции Делоне как метрики сравнения распределения данных на плоскости позволяет дифференцировать между «нормальным» и «аномальным» распределением точек, которые были получены для нормального и аномального функционирования системы. Выбранная метрика может быть дополнительно применена для измерения эффективности методов измерения данных при обнаружении паттернов и аномалий в функционировании системы.

Одним из возможных подходов к оценке распределения точек на плоскости с последующим сравнением с другими распределениями является триангуляция Делоне [4]. Триангуляция Делоне — это особый вид триангуляции, обладающий следующими важными свойствами:

– триангуляция Делоне уникальна, если никакие четыре точки не лежат на одной окружности;

– никакие точки не лежат внутри описанной окружности любого треугольника;

– каждый треугольник образован тремя ближайшими точками, и каждый отрезок прямой не пересекается;

– триангуляция Делоне максимизирует минимальный угол всех построенных треугольников среди всех возможных триангуляций, что позволяет получить менее «тонкие» треугольники среди всех возможных триангуляций. Таким образом, можно построить треугольники, площадь которых имеет минимальный разброс.

Такой способ разделения пространства на плоские фигуры, одна из которых - внешняя бесконечность, а остальные - треугольники, не оптимален с точки зрения минимальной суммы всех ребер. Однако построение оптимальной триангуляции может оказаться слишком ресурсоемким процессом.

В работе авторы исследуют триангуляцию Делоне к множеству точек, созданных с помощью метода проекции многомерных данных PCA. Поскольку основной целью исследования является способность оценить состояние сложного объекта, исходный набор точек был разделен на подмножества, соответствующие некоторым равным периодам времени, например день, месяц или год. Это предположение, с одной стороны, не позволяет точно идентифицировать аномалии в течение определенного периода времени, но позволяет быстро определить, насколько отличается модель поведения системы в течение определенного периода времени относительно других, а также дает возможность создать автоматический поиск аномалий и аннотирования данных на основе полученных оценок.

Метод PCA и последующая триангуляция Делоне полученных точек формирует характерный визуальный паттерн для каждого исследуемого интервала времени. Разница в полученных триангуляциях, а также в средней и общей площади треугольников очевидна. Это различие позволяет предположить, что поведение системы в эти периоды сильно различается. Исходные данные не размечены, и нельзя однозначно ответить на вопрос, аномальное ли это состояние системы или нет.

Авторы предположили, что площадь между точками, расположенных последовательно может быть применена как мера изменений в поведении системы, и ее визуализация может быть использована более точного контроля и анализа состояния системы на выбранном интервале времени. Мы назвали этот подход «Последовательная триангуляция». Таким образом, алгоритм предварительной триангуляции описывается следующим образом:

- применить PCA для отображения оригинальных данных в двумерное пространство;
- выбрать размер скользящего окна для выбора последовательности точек, включая текущую;
- применить триангуляцию Делоне над выбранным набором точек (если количество точек больше 2);
- вычислить оценки изменения состояния системы как общей площади обнаруженных треугольников или как расстояния между точками, если в выбранном множестве только 2 точки;
- построить график полученных оценок, на котором по оси Y - оценки состояний системы в текущей точке, по оси X - время точки.

Чтобы оценить применимость триангуляции Делоне для оценки распределения точек, мы использовали набор данных, предоставленный в рамках VASTChallenge 2016. Он описывает функционирование системы HVAC. Здание разделено на зоны, состояния которых определяются 10 параметрами. Хотя набор данных не размечен, он был тщательно проанализирован, было сформировано множество дней с нормальным поведением системы, а также выделено несколько дней с аномальным функционированием системы.

При выполнении экспериментов сначала было выполнено снижение размерности всего набора данных, затем исходный набор данных был разделен на подмножества равного размера, соответствующие одному дню. Для каждого подмножества точек была вычислена общая площадь всех треугольников, полученных триангуляцией Делоне. Полученные графики выявили значительные выбросы в данных для двух дней, которым соответствовало аномальное состояние системы, а применение методики последовательной триангуляции для одного из дней с аномальной активностью позволило выявить конкретные интервалы времени с выбросами в данных. Можно предположить, что именно на этих временных интервалах произошло сильное отклонение поведения системы от нормального, и именно на них следует заострить свое внимание при последующем более тщательном анализе причин, вызвавших это отклонение.

В основе представленного подхода к сравнению распределения многомерных точек лежит методика снижения размерности и триангуляция Делоне. Эксперименты показали, что этот метод позволяет получить численную оценку распределения точек, что дает возможность без тщательного анализа множества атрибутов выявить аномальное поведение системы.

СПИСОК ЛИТЕРАТУРЫ

1. Leite, R. A., Gschwandtner, T., Miksch, S., Gstrein, E., &Kuntner, J. (2018). Visual analytics for event detection: Focusing on fraud. Visual Informatics, 2018. 2(4), 198-212.
2. Bruneau P., Pinheiro B., Broeksema B., Otjacques B. Cluster Sculptor, an interactive visual clustering system, Neurocomputing, 2015. Vol 150, Part B, , pp. 627-644.
3. Novikova E, Kotenko I., Fedotov E. Interactive Multi-view Visualization for Fraud Detection in Mobile Money Transfer Services. IJMCMC, 2014
4. de Berg M., van Kreveld M., Overmars M., Schwarzkopf O.C. Delaunay Triangulations. In: Computational Geometry. 2020. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-04245-8_9.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГЕОИНФОРМАЦИОННЫХ СИСТЕМ

УДК 004.75:004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ УСТРОЙСТВ ЦОС ДЛЯ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ УСТРОЙСТВ РАДИОЛОКАЦИОННОЙ СТАНЦИИ ГЕОИНФОРМАЦИОННОЙ СИСТЕМЫ

Афанасьев Дмитрий Сергеевич, Виноградов Алексей Борисович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: Dmitr-afanas@yandex.ru, abvinogradov@etu.ru

Аннотация. В системе управления комплексом радиолокационных станций, оснащенных устройствами цифровой обработки сигналов, рассмотрена обработка переотраженного зондирующего сигнала в действующей радиолокационной станции контроля воздушного пространства геоинформационной системы. При одновременном функционировании различных подсистем геоинформационной системы в реальном времени требуется их синхронизация. Синхронизация производится одновременно на многих уровнях по методам синхронизации на различных уровнях и между различными устройствами программируемой логической интегральной схемы. Проверка работоспособности методов синхронизации производится по модели работы радиолокационной станции на основе цифровой антенной решетки.

Ключевые слова: информационная безопасность объектов связи; геоинформационная система; радиолокационная станция; цифровая обработка сигналов; протокол связи.

INFORMATION SECURITY OF THE RADAR STATION FOR INFORMATION INTERACTION OF DEVICES OF THE RADAR STATION OF THE GEO-INFORMATION SYSTEM

Afanasiyev Dmitriy, Vinogradov Aleksey
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: Dmitr-afanas@yandex.ru, abvinogradov@etu.ru

Abstract. In the system of controlling the range of radar stations equipped with digital signal processing devices, the processing of a transitioned probing signal in the active radar station controlling the airspace of the geo-information system is considered. With the simultaneous operation of various subsystems of the geographic information system in real time, their synchronization is required. Synchronization is performed simultaneously at many levels by synchronization methods at various levels and between different devices of a programmable logical integrated circuit. Checking the performance of synchronization methods is performed according to the mode of operation of the radar station based on a digital antenna array.

Keywords: information security of communication facilities; geoinformation systems; radar; digital signal processing; communication Protocol.

Устройства цифровой обработки сигналов радиолокационной станции геоинформационной системы поддерживают информационную безопасность компонентов систем связи для передачи и обработки информации [1], позволяют строить модели защиты сигналов от помех, проверять работоспособность и эффективность средств авторизации, выявлять возможные источники и технические каналы утечки информации, перехвата информации. В задачи системы защиты каналов связи и устройств обработки информации входит защищенность информации, информационных потоков и каналов их передачи [2, 3]. Меры защиты объекта и его информационного ресурса зависят от степени соответствия описания объекта и его ресурса. При одновременном функционировании различных подсистем в реальном времени – а каждая подсистема состоит из многих управляемых элементов – требуется их синхронизация. При этом синхронизация производится одновременно на многих уровнях. Были рассмотрены методы синхронизации на различных уровнях и между различными устройствами программируемой логической интегральной схемы (ПЛИС). Проверка работоспособности рассмотренных методов синхронизации проведена на модель работы системы.

Для оценки работоспособности устройств взаимодействия радиолокационной станции геоинформационной системы были

Сформулированы критерии оценки эффективности работы системы и основные мешающие функционированию системы факторы; апробирована модель работы системы с учетом основных мешающих

факторов; предложены методы синхронизации на радиочастотном уровне; апробированы методы синхронизации внутри программируемой логической интегральной схемы; апробированы методы синхронизации между устройствами с ПЛИС; предложены методы синхронизации между ПЛИС и процессорным модулем операционной системы (ОС); апробированы методы синхронизации между процессорными модулями и операционной системой.

СПИСОК ЛИТЕРАТУРЫ

1. Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации. М.: Техносфера. – 2005. 592 с. (+ решетки)
2. Шеннон К. Работы по теории информации и кибернетике. М.: Изд-во Иностранной литературы, 1963. - 830 с.
3. Габидулин Э.М, Пилипчук Н.И. Лекции по теории информации. Изд-во МФТИ, 2007. - 214 с.

УДК 004.7

ПРОБЛЕМЫ ИНТЕРНЕТ-ПИРАТСТВА В ПИРИНГОВЫХ СЕТЯХ

Балицкий Георгий Викторович
Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mail: zbalitskits@mail.ru

Аннотация. Рассматривается общие принципы работы протоколов пиринговых сетей. Обсуждаются проблемы интернет-пиратства в пиринговых файлообменных сетях и способы из разрешения.

Ключевые слова: пиринговые сети; протоколы torrent; интернет-пиратство.

INTERNET PIRACY PROBLEMS IN PERING NETWORKS

Balitsky Georgy
Russian State Hydrometeorological University
79 Voronezhskya St, St. Petersburg, 192007, Russia
e-mail: zbalitskits@mail.ru

Abstract. The general principles of peer-to-peer protocols operation are considered. Discussed the problems of Internet piracy in peer-to-peer file-sharing networks and methods of resolution.

Keywords: peer-to-peer networks; torrent protocols; internet piracy.

Сегодня в основном словосочетание “скачать из интернета” подразумевает использование Torrent клиента, где практически беспрепятственно можно добыть нужные программы, файлы, игры, программное обеспечение и т.д. Но пользователь, скачивая нелицензионный контент, подвергает себя и свой компьютер угрозам. Рассмотрим этот протокол и какие последствия несет его использование пользователю [1].

Torrent – это пиринговые файлообменные сети, т. е. основанные на технологии peer-to-peer (P2P), – это компьютерные сети, в которых все участники, могут выступать и в качестве клиента, и в качестве сервера одновременно. Работает эта технология следующим образом. Пользователь устанавливает на компьютер специальную программу (клиент) для работы с конкретной P2P сетью, и после этого может как сделать доступным свой файл в сети, поместив его в специальную директорию, так и отправить запрос на поиск нужного ему файла. Если нашлось несколько источников, то файл будет скачиваться частями одновременно со всех. С другой стороны, доступный файл пользователя, равно как и уже скаченные части искомого им файла, могут в этот момент служить одним из источников для другого пользователя. За счет такого подхода и достигается высокая пропускная способность пиринговый сетей. Существуют различные P2P протоколы и основанные на них сети, такие как, например, eDonkey, Dirrect Connect, Gnutella, BitTorrent [2].

Большие одноранговые (пиринговые) сети намного устойчивее многоранговых (клиент-серверных), а также скорость обмена файлами в P2P-сетях на порядок выше, чем в традиционных.

В то же время основными проблемами для многих пользователей пиринговых сетей является необходимость постоянно держать свой компьютер, подключенным к Интернету, трафик значительно возрастет – причем как входящий, так и исходящий.

Передача в torrent осуществляется не последовательно, а параллельно – каждому пользователю, подключенному к раздаче, отправляется один сегмент. Затем они обмениваются ими между собой.

На сервере (торрент-трекере) хранятся не сами файлы, а лишь информация, полученная от подключенных к обмену клиентов, список самих клиентов и некоторые другие данные. Для креативных индустрий (производство музыки, книг, фильмов и др.), а также для индустрии программного обеспечения это означает серьезную потерю доходов, отсутствие стимула для творчества, необходимость дополнительных вложений в средства борьбы с пиратством [3].

Несмотря на то, что пиратство в интернете в России все еще имеет огромные масштабы, данные исследовательских компаний свидетельствуют о его падении. Причиной этому стал целый ряд мер, предпринимаемых в последние годы правительством нашей страны, а также разработка новых технологичных

способов борьбы с незаконным распространением контента, эффективных и простых в применении, уже дающих заметные результаты.

Традиционно виды незаконного использования контента определяют в зависимости от того, какие объекты интеллектуальной собственности используются без разрешения правообладателя и каким образом было нарушено исключительное право. В первом случае выделяют следующие виды интернет-пиратства:

- литературное пиратство;
- видеопиратство;
- аудиопиратство;
- пиратство компьютерных игр;
- пиратство программного обеспечения.

Во втором можно говорить:

- о нелегальной загрузке произведения на электронный ресурс вне зависимости от того, кто имеет доступ к этому ресурсу и с какой целью это было сделано;
- пересылке произведения с помощью любых средств (по электронной почте, мессенджер, социальную сеть и т.п.);
- открытии доступа третьим лицам к ресурсу, который содержит легальные копии произведения;
- полном нелицензионном использовании произведения;
- использовании легальной копии произведения, но с нарушением условий лицензии (такое происходит, например, когда организация использует программное обеспечение для большего количества рабочих мест, чем это предусмотрено лицензионным договором);
- использовании легальной копии основного продукта с нелицензионными дополнениями к нему.

Первые три вида относятся больше к интернет-пиратам, вторые - к конечным пользователям. Между ними есть принципиальная разница, не имеющая значения с точки зрения закона, но очень важная с моральной: конечные пользователи не всегда нарушают авторское право намеренно. Иногда это может происходить просто по незнанию законодательства, иногда - из-за невнимательности при ознакомлении с условиями лицензии.

И за рубежом, и в Российской Федерации применяются не только технические средства защиты, но и иные способы, заключающиеся в том числе:

- в информировании граждан о достоинствах использования легальных копий произведения и недостатках пиратских, а также о их правах и обязанностях в сфере интеллектуальной собственности;
- воспитании культуры уважения к чужому интеллектуальному труду и творчеству;
- создании ресурсов, предлагающих конечным пользователям максимально большой выбор произведений музыки, литературы, кино и др., которые он мог бы приобрести с минимальными затратами и без лишних действий;
- выявлении производителей и распространителей нелегального контента и привлечении их к ответственности. Так, в России в 2019 году впервые владелец крупного пиратского онлайн-кинотеатра был привлечен не к административной, как это было принято раньше, а к уголовной ответственности.

Что касается технических средств защиты, их существует огромное количество. Многие страны мира успешно противостоят нелегальному использованию контента с помощью:

- систем поиска нелегального контента по цифровым отпечаткам. Например, в России успешно применяют систему n’RIS Antipiracy, которая осуществляет поиск по большинству электронных ресурсов и даже способна в автоматическом режиме направлять администрации таких ресурсов досудебные претензии;
- блокировки файлообменных сайтов и других ресурсов, на которых обнаруживается нелегальный бесплатный контент.

Совершенствуется и законодательство по интеллектуальным правам: ответственность за пиратство в интернете несут не только лица, непосредственно занимающиеся незаконным распространением контента, но и другие стороны - конечные пользователи и владельцы электронных ресурсов, провайдеры, поисковые системы и др.

СПИСОК ЛИТЕРАТУРЫ

1. Что такое и как работает торрент трекер? URL: https://voron-xak.ru/progi/kak-rabotaet-torrent-treker.html (дата обращения: 09.05.2021)
2. https://ru.wikipedia.org/wiki/%CE%9CTorrent
3. Татарникова Т.М. Технологии защиты авторского права на цифровой контент // Геополитика и безопасность. 2017, № 1 (37). С. 66-72.

УДК 004.75

МЕТОДИКА ДЕТЕКТИРОВАНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ УСТРОЙСТВ УМНОГО ДОМА

Богданов Павел Юрьевич
Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП)
Большая Морская ул., 67, Санкт-Петербург, 190000, Россия
e-mail: 45bogdanov@gmail.com

Аннотация. Приведена методика процесса детектирования аномального поведения сенсорного устройства. Методика основана на сравнении паттернов поведения сенсорного устройства на приеме и передаче данных и сравнении паттернов с реальным поведением сенсорного устройства.

Ключевые слова: интернет вещей; детектирование атаки; паттерн поведения.

METHOD FOR DETECTING ANOMALOUS BEHAVIOR OF SMART HOME DEVICES

Bogdanov Pavel
Saint Petersburg State University of Aerospace Instrumentation (SUAI)
67 Bolshaya Morskaya St, St. Petersburg, 190000, Russia
e-mail: 45bogdanov@gmail.com

Abstract. The technique of the process of detecting anomalous behavior of the sensor device is presented. The technique is based on comparing the patterns of behavior of the sensor device in receiving and transmitting data and comparing the patterns with the real behavior of the sensor device.

Keywords: internet of things; attack detection; pattern of behavior.

Суть интернета вещей заключается в возможности взаимодействия с реальным, физическим миром. Сенсорные устройства (СУ) измеряют характеристики окружающего мира. На основе этих данных управляющая программа устройства принимает решение о запуске того или иного управляющего воздействия. Атака на сенсоры, манипуляция с поступающими в программу данными, подмена данных, выводимых на пульт оператора, воздействие непосредственно на исполнительные механизмы – успешные атаки на любые звенья этой цепочки могут привести к захвату контроля над системой интернета вещей.

Таким образом, при проектировании систем интернета вещей особое внимание уделяется обеспечению безопасности данных, в основном передаваемых по беспроводным каналам [1, 2].

В докладе предлагается методика процесса детектирования аномального поведения сенсорного устройства. Методика основана на сравнении паттернов поведения сенсорного устройства на приеме и передаче данных и сравнении паттернов с реальным поведением сенсорного устройства. Методика включает следующие шаги [3, 4]:

Подготовка исходных данных:

– получение паттерна поведения умного устройства;

– запись паттерна поведения умного устройства для активного режима работы на прием и передачу пакетов данных для хранения в базу эталонных данных системы обнаружения атак;

– выбор порогового значение для принятия решения о наличии атакующего воздействия при превышении порогового значения, назовем $d_{доп}$.

При передаче данных от СУ на сервер:

– на сервере фиксируется временной ряд передаваемых пакетов данных в течении временного периода, например 4800 с;

– подсчитать количество временных тактов с нулевых уровнем объема переданных данных, в байтах за период;

– подсчитать относительные частоты временных тактов с нулевых уровнем объема, в байтах за период;

– построить плотность распределения относительных частот на периоде, назовем p';

– сервер обращается к базе эталонных данных и по идентификатору устройства находит паттерн p его поведения;

– сервер выполняет потактовое сравнение p и p', разницу назовем d;

– сравнить d и $d_{доп}$. Если $d \geq d_{доп}$, то генерируется оповещение об аномальном поведении. Если $d < d_{доп}$, то регистрируется, при необходимости, состояние штатной работы.

При приеме данных от сервера на СУ выполняются те же действия, что и при передаче от СУ на сервер (пп. 2.1 – 2.7) с разницей в том, что СУ обращается к своей локальной памяти за паттерном p взаимодействия сервера с СУ.

СПИСОК ЛИТЕРАТУРЫ

1. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаужение вторжений в компьютерные сети. Сетевые аномалии. – М.: Горячая линия - Телеком, 2013. 220 с.
2. Jyothsna V., Prasad V.V.R. A Review of Anomaly Based Intrusion Detection Systems // International Journal of Computer Applications. 2011. Vol. 28, no. 7. P. 26–35
3. Wattenberg F.S., Perez J.I.A, Higuera P.C., Fernandez M.M., Dimitradis I.A. Anomaly detection of network traffic based on statistical inference and a-stable modeling // IEEE Transaction on Dependable and Secure Computing. 2011. Vol. 8, no. 4. P. 494-509.
4. Татарникова Т.М. Статистические методы исследования сетевого трафика // Информационно-управляющие системы. 2018. № 5 (96). С. 35-43.

УДК 004.772

ПРОГРАММНЫЕ РЕШЕНИЯ ПОИСКА НЕИСПРАВНОСТЕЙ В СЕТЯХ

Деркач Денис Иванович
Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mail: dovus@rshu.ru

Аннотация. В статье рассматриваются основные программные решения по поиску, анализу и выявления неисправностей, возникающих внутри сети.

Ключевые слова: уязвимость; информация; безопасность; утилита; перехват.

NETWORK TROUBLESHOOTING SOFTWARE

Derkach Denis
Russian State Hydrometeorological University
79 Voronezhskya St, St. Petersburg, 192007, Russia
e-mail: dovus@rshu.ru

Abstract. The article discusses the main software solutions for the search, analysis and detection of faults occurring within the network.

Keywords: vulnerability; information; security; utility; hardware; interception.

В данной работе проводится анализ исследований и публикаций в данной тематике и формирование общих проблем. Даны общие рекомендации по их устранению.

Проблемы защиты информации в сфере жизни человека является центральной и только усиливается с распространением их использования как в быту, так и внутри компаний. Поскольку данная система является местом повышенной опасности в связи с сложным технологическим устройством, и распространенностью, в обществе требуется создание крупной системы культуры безопасности, включая также и защиту информации [1-3].

Первым инструментом для выявления проблем внутри сети являются внутренние утилиты, такие как ping, tracert, netstat и другие. С помощью ping производится проверка целостности и качества соединений по протоколу TCP/IP. Она заключается в том, что оператор вводя команду на отправку 4 пакетов на сервер некоторого сайта. По каждому пакету выводится информация о времени отправки и максимальный период времени, за который данный пакет должен был просуществовать. Также в командной строке выводится основная статистика по проделанной работе – это то, сколько было отправлено пакетов, сколько было получено, сколько было потеряно и время приема-передачи. Также с помощью утилиты может быть получен ip адрес сервера. С помощью утилиты Tracert или Traceroute еможно определить маршрут, по которому происходит передача пакета до нужного сервера. В основном, Tracert может проводить операции по протоколам UDP, TCP, ICMP и GRE. В виде таблицы выводится сколько узлов было пройдено и какой ip адрес у каждого узла. Для каждого из них оценивается время обработки пакета. Основная задача утилиты Netstat – это выведение состояния различных структур данных, связанных с сетью, в виде таблицы маршрутизации TCP-соединений, сетевую статистику и число интерфейсов.

Программа WireShark является относительно новым инструментом сетевой диагностики с открытым исходным кодом и бесплатным распространением. Wireshark – это мощный сетевой анализатор, который может использоваться для анализа трафика, проходящего через сетевой интерфейс компьютера. Основные возможности программы:

- Захват пакетов в реальном времени из проводного или любого другого типа сетевых интерфейсов, а также чтение из файла;
- Поддерживаются такие интерфейсы захвата: Ethernet, IEEE 802.11, PPP и локальные виртуальные интерфейсы;
- Пакеты можно отсеивать по множеству параметров с помощью фильтров;
- Все известные протоколы подсвечиваются в списке разными цветами, например TCP, HTTP, FTP, DNS, ICMP и так далее;
- Поддержка захвата трафика VoIP-звонков;
- Поддерживается расшифровка HTTPS-трафика при наличии сертификата;
- Расшифровка WEP-, WPA-трафика беспроводных сетей при наличии ключа и handshake;
- Отображение статистики нагрузки на сеть;
- Просмотр содержимого пакетов для всех сетевых уровней;
- Отображение времени отправки и получения пакетов.

SolarWinds Network Bandwidth Analyze – данное решение является программным пакетом из двух продуктов: Network Performance Monitor (базовое решение) и NetFlow Traffic Analyzer (модульное расширение). Network Performance Monitor осуществляет мониторинг производительности сети. Пользователь имеет возможность контролировать общую работоспособность сети: опираясь на огромное количество статистических данных, таких как скорость и надежность передачи данных и пакетов, что позволяет быстро идентифицировать неисправности в работе сети. Интеллектуальные возможности программы по выявлению потенциальных проблем и широкие возможности по визуальному представлению результатов в виде таблиц и графиков с четкими предупреждениями о возможных проблемах, еще больше облегчат эту работу. Модульное расширение NetFlow Traffic Analyzer больше сконцентрировано на анализе самого трафика. В то время, как функциональность базового программного решения Network Performance Monitor больше предназначена для получения общего представления о производительности сети, в NetFlow Traffic Analyzer фокус внимания направлен на более детальный анализ процессов, происходящих в сети. В частности, эта часть программного пакета позволит проанализировать перегрузки или аномальные скачки полосы пропускания и предоставит

статистику, отсортированную по пользователям, протоколам или приложениям. Даная программа доступна только для среды Windows.

Программы для анализа сетевого трафика являются важным инструментарием при возникновении сетевых проблем разных видов – будь то производительность, сброшенные соединения или проблемы с сетевыми резервными копиями. Практически все, что связано с передачей и получением данных в сети, может быть быстро идентифицировано и исправлено благодаря сведениям, полученным с помощью программного обеспечения из вышеприведенного списка.

СПИСОК ЛИТЕРАТУРЫ

1. Веревкин С.А., Татарникова Т.М., Краева Е.В., Мартын И.А. Тестирование защищенности беспроводных сетей. В сборнике: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ. Сборник статей научно-практической конференции студентов, аспирантов и молодых ученых. Российский государственный гидрометеорологический университет, Институт информационных систем и геотехнологий. Санкт-Петербург, 2021. С. 29-33
2. Веревкин С.А., Татарникова Т.М., Краева Е.В., Мартын И.А. разработка виртуального маршрутизатора. В сборнике: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ. Сборник статей научно-практической конференции студентов, аспирантов и молодых ученых. Российский государственный гидрометеорологический университет, Институт информационных систем и геотехнологий. Санкт-Петербург, 2021. С. 74-77.
3. Татарникова Т.М. Методы исследования сетевого трафика. В книге: Перспективные направления развития отечественных информационных технологий. материалы V межрегиональной научно-практической конференции. Севастопольский государственный университет; Санкт-Петербургский институт информатики и автоматизации РАН. Севастополь, 2019. С. 227-230.

УДК 004.75

МОДЕЛЬ ОБСЛУЖИВАНИЯ СЕТЕВОГО ТРАФИКА, ИМЕЮЩЕГО ПАЧЕЧНЫЙ ХАРАКТЕР

Кутузов Олег Иванович, Татарникова Татьяна Михайловна
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: tm-tatarn@yandex.ru

Аннотация. Приведена методика расчета вероятности потерь в конечном буфере. Изложены основные шаги методики сбора и обработки выборочных данных при построении модели для оценивания потерь в буфере конечной емкости методом экстремальных статистик.

Ключевые слова: сетевой трафик; обслуживание трафика; вероятность потери; конечный буфер; теория экстремальных порядковых статистик.

MODEL OF SERVING NETWORK TRAFFIC WITH A BACKUP CHARACTER

Kutuzov Oleg, Tatarnikova Tatiana
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: tm-tatarn@yandex.ru

Abstract. The method for calculating the probability of losses in the final buffer is presented. The main steps of the methodology for collecting and processing sample data when constructing a model for estimating losses in a buffer of finite capacity by the method of extreme statistics are presented.

Keywords: network traffic; traffic maintenance; probability of loss; final buffer; theory of extreme order statistics.

Самоподобный трафик моделируется распределениями вероятностей с тяжелыми хвостами. Одним из таких распределений, отражающим пачечный характер сетевого трафика является распределение Вейбулла [1].

Распределение Вейбулла W относится к классу экспоненциальных распределений, но «хвост» у распределения Вейбулла тяжелее «хвоста» экспоненциального распределения.

«Тяжелый хвост» у распределения Вейбулла означает, что этом распределении значительные (большие) значения случайной величины встречаются с большей вероятностью (чаще), чем, те же значения в классическом экспоненциальном распределении.

Задачу оценки емкости буферного накопителя сетевого узла при вейбулловском трафике предлагается решить с применением метода экстремальных порядковых статистик (Extreme Value Theory, EVT).

Математическими моделями сетевых узлов в основном системы массового обслуживания – СМО). В общем случае узел инфокоммуникационной рассматриваем как СМО класса G|G|1|m при стационарном режиме функционирования. Это класс одноканальных СМО с рекуррентным потоком заявок, определяемым произвольной функцией распределения длительности интервалов между ними (интервалов поступления), с рекуррентным временем обслуживания, определяемым произвольной функцией распределения, с числом мест в очереди (размером буфера) $m \leq \infty$. Рассматриваем стационарный режим функционирования такой СМО.

Задача проектирования буферов для СМО типа G|G|1|m сформулирована как нахождение зависимости вероятности потери заявки от размера буфера, что позволит для любой заданной допустимой вероятности потерь определять соответствующий наименьший допустимый размер буфера.

Изложены основные шаги методики сбора и обработки выборочных данных при построении модели для оценивания потерь в буфере конечной емкости методом EVT [2].

Метод EVT был разработан для аппроксимации экстремальных статистик распределений экспоненциального класса [3]. Однако, случай для тяжелых хвостов распределений представляет особый интерес, поскольку распределения Вейбулла занимают промежуточное место между распределениями с экспоненциальным убыванием хвостов (показательное распределение, гамма-распределение) и «тяжелохвостыми» распределениями со степенным убыванием хвостов типа Ципфа-Парето [4]. Это существенное замечание расширяет возможности распределения Вейбулла для описания реального сетевого трафика.

СПИСОК ЛИТЕРАТУРЫ

1. Arfeen M.A., Pawlikowski K., McNickle N., Willig A. The role of the Weibull Distribution in Internet traffic modeling // 25th International Teletraffic Congress (ITC), Shanghai, 2013. P. 1–8. DOI: 10. 1109/ITC.2013.6662948
2. Галамбош Я. Асимптотическая теория экстремальных порядковых статистик. – М.: Наука, 1984. 303 с.
3. Tanenbaum A., Wetherall D. Computer Networks. 5th ed. – Prentice Hall, 2010. 960 p.
4. Zadorozhnyi, V.N. Simulation modeling of fractal queues, in Dynamics of Systems, Mechanisms and Machines (Dynamics), 2014. P. 1-4. DOI: 10.1109 / Dynamics.2014.7005703.
5. Tatarnikova T., Kutuzov O. Evalution and comparison of classical and fractal queuing systems // In 15th International Symposium on Problems of Redundancy in Information and Control Systems, REDUNDANCY 2016. P. 155-157. DOI: 10.1109 / RED.2016.7779352

УДК 004.62

ЦЕНТРАЛИЗОВАННАЯ И РАСПРЕДЕЛЕННАЯ ОБРАБОТКА ИНФОРМАЦИИ ПРИ ПРОЕКТИРОВАНИИ УСЛОВИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГЕОИНФОРМАЦИОННОЙ СИСТЕМЫ

Нечитайленко Роман Александрович, Богданов Тимур Рушанович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: rnet2005@gmail.com, Bbfox.bbfox@gmail.com

Аннотация. Рассмотрение условий информационной безопасности геоинформационной распределенной системы рассматривается как обязательная обеспечивающая составляющая проектирования при централизованной и распределенной обработки информационного ресурса системы. Выделены факторы безопасности как информационного ресурса, так и элементов структуры геоинформационной системы. Проверка безопасности разрабатываемых средств поддержки информационного обеспечения распределенной системы обработки информации осуществляется на выбираемых и создаваемых прототипах распределенной системы. Распределенная система представляется как информационно-аналитическая система поиска, обработки и анализа данных, сопровождаемая сервисным и интерфейсным обслуживанием по установленной коммуникативной форме.

Ключевые слова: распределенная система обработки информации; информационное обеспечение; геоинформационная система; информационная безопасность системы.

CENTRALIZED AND DISTRIBUTED INFORMATION PROCESSING IN THE DESIGN OF INFORMATION SECURITY CONDITIONS OF GEOGRAPHIC INFORMATION SYSTEM

Nechitailenko Roman, Bogdanov Tymur
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: Novopashin.vladimir@gmail.com , rnet2005@gmail.com

Abstract. Consideration of information security conditions of geoinformation distributed system is considered as a mandatory supporting component of the design for centralized and distributed processing of information resource of the system. Highlighted the security factors of both information resource and elements of the geographic information system structure. Verification of safety of developed means of information support of distributed information processing system is carried out on the selected and created prototypes of the distributed system. The distributed system is represented as an information-analytical system of data search, processing and analysis, accompanied by service and interface maintenance according to the established communicative form.

Keywords: distributed information processing system; information support; geoinformation systems; information security of systems.

Информационная безопасность геоинформационной системы при централизованной и распределенной обработке информации в значительной степени зависит от взвешенного распределения информационной нагрузки по всей конфигурации распределенной системы. С точки зрения факторов безопасности как информационного ресурса, так и элементов структуры геоинформационной системы, следует отнести факторы аутентификации пользователей и соблюдения политики безопасности объектов системы. Безопасность ресурса и

структуры включаются в условия политики безопасности объектов системы и сопровождают все сопутствующие характеристики открытых распределенных систем, специфичные для применяемой функциональной структуры:

– входящие в состав распределенной структуры системы подсистемы должны легко взаимодействовать между собой;

– подсистемы распределенной системы должны быть сопрягаемы с четко определенными интерфейсами;

– программно-аппаратное обеспечение распределенной системы должно обеспечивать переносимость установленных приложений;

– открытый характер системы должен быть достигнут с помощью объявленных языков программирования, аппаратных платформ, программного обеспечения, распределенной системы.

Функционально распределенная система обработки информации должна выступать как информационно-аналитическая система для поиска, обработки и анализа данных [1, 2], с обслуживанием установленной коммуникативной формой и сопровождением сервисными и интерфейсным услугами [3]. Проверка безопасности разрабатываемых средств поддержки информационного обеспечения распределенной системы обработки информации осуществляется на выбираемых/создаваемых прототипах распределенной системы. Прототип распределенной системы должен отвечать набору базовых понятий, сформулированным требованиям и принимаемым для оценки особенностям распределенной системы. В качестве основных контролируемых требований выделены: открытость системы, безопасность, надежность, прозрачность (доступа, параллелизма доступа, репликации) [4]. Требования надежности и прозрачности обеспечиваются с учетом неотъемлемых качеств распределенной системы - её открытости и безопасности.

Основным показателем надежности целостной структуры распределенной системы обработки информации, для выбранного прототипа, является отказоустойчивость, с Принципом Отказоустойчивости как возможность продолжения действий, заданных программой функционирования, после возникновения и выявления неисправностей.

Принцип Прозрачности структуры системы, в конкретном случае, заключается в восприятии системы пользователями как однородный целостного объекта, но не как набора объектов структуры, которые организуют взаимодействие между собой. Прозрачность местоположения территориально распределенной системы заключается в отсутствии необходимости пользователю знать, где территориально расположены необходимые ему ресурсы. Файлы ресурса могут перемещаться на различные узлы и элементы распределенной структуры системы. Качества безопасности и прозрачности необходимо обеспечить в едином файловом пространстве, независимо от расположения на физически разных серверах изначально или по условиям реконструкции в рамках политики безопасности распределенной системы.

Прозрачность доступа заключается обеспечивает сокрытие различий доступа и предоставления данных категориям пользователей системы. Прозрачность параллелизма доступа - условия функционирования, при которых различные пользователи распределенной системы должны иметь возможность параллельного доступа к общим данным, при этом обеспечивается параллельное совместное использование ресурсов системы, и одновременно обеспечивается сокрытие факта совместного использования ресурса. Прозрачность репликации организована в целях обеспечения сохранности данных и соблюдения комплексной защиты информационного ресурса системы. В сложных распределенных файловых системах репликация данных обеспечивает организацию данных, при которой пользователю не должно быть известно, что репликация данных существует и для сокрытия данного фактора, у данных или ресурсов, объявлены одинаковые имена.

Безопасность данных и всей структуры распределенной системы, на уровнях отдельных узлов распределенной системы, оговаривается обеспечением совокупности основных факторов безопасности:

– обеспечение аутентификации и конфиденциальности данных и ресурсов;

– обеспечение аутентификации и конфиденциальности доступа к ресурсам для ранжированного множества пользователей;

– обеспечение целостности ресурсов и данных,

– введением политики безопасности и аутентификации пользователей.

Условия информационной безопасности геоинформационной системы обеспечиваются для централизованной и распределенной обработки информации при согласовании требований проектирования и управления распределенной системой. Аспекты информационной безопасности рассматриваются при установлении регламента:

– режимов конфигурирования архитектуры распределенной системы,

– режимов администрирования системы,

– специальных вопросов организации данных:

– восстановления данных в случае возникновения ошибок,

– ограниченности масштабируемости (проблема увеличения количество узлов системы,

– ограниченности возможностей сервера,

– ограниченности сетей передачи данных,

– ограниченности алгоритмов обработки данных,

– переносимости программного обеспечения,

– адаптации сервисных приложений для всех объектов конфигурирации архитектуры системы;

– обработки данных с использованием сервисных приложений распределенной системы:

– рассылки данных на распределенные узлы системы,
– сбора данных из распределенных узлов,
– агрегирования данных в общее пространство данных распределенной системы.

Учет требований проектирования и управления для распределенной системы централизованной и распределенной обработки информации позволил: согласовать локальные параметрические и алгоритмические требования обработки данных в узлах распределенной системы с требованиями, влияющими на общими свойствами распределенной системы; провести анализ свойств данных централизованной и локальной обработки распределенной системы; сформулировать категории распределенных систем для классификации по количеству элементов в системе, по уровню организации распределенных систем, по типу предоставляемых ресурсов, для последующего качественного сравнения вариантов распределения информационной нагрузки распределенной системы обработки информации.

СПИСОК ЛИТЕРАТУРЫ

1. Ван Стеен М., Танненбаум Э. Распределенные системы. Принципы и парадигмы. СПб: Питер, 2003, 877 с.
2. Tanenbaum A., Van Steen M. Distributed systems. Pearson Prentice Hall, 2007. - 803 p.
3. Шокин Ю.И. и др. Распределенная информационно-аналитическая система для поиска, обработки и анализа пространственных данных // Вычислительные технологии. 2007. Т. 12. №. 3. С. 108-115.
4. Карабутов Н.Н. Идентификация систем. Структурный и информационный анализ. Часть 1. - М.: Изд-во Альтаир - МГАВТ, 2005. - 79 с.

УДК 004.056

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ВЕБ-САЙТОВ

Онучин Виталий Сергеевич
Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mail: vitaliyonuchin@gmail.com

Аннотация. Рассматривается безопасность веб-сайтов, основные термины, связанные с безопасностью сайтов, а также аспекты безопасности и способы обеспечить безопасность веб-сайтам.

Ключевые слова: интернет; веб-сайт; аутентификация; безопасность; вирусы.

ENSURING THE SECURITY OF WEBSITES

Onuchin Vitaly
Russian State Hydrometeorological University
79 Voronezhskya St, St. Petersburg, 192007, Russia
e-mail: vitaliyonuchin@gmail.com

Abstract. It discusses the security of websites, the main terms related to the security of websites, as well as security aspects and ways to ensure the security of websites.

Keywords: internet; website; authentication; security; viruses.

Все понимают веб-безопасность по-разному. Для некоторых людей это возможность просматривать веб-сайт, зная, что никто не следит за ним. Для других это способность безопасно проводить финансовые операции. Для кого-то это хранение личных (конфиденциальных) данных на веб-сайте, без последующей передачи третьим лицам. Есть ряд причин, по которым требуется защита при подключении к Интернету или к любой внешней сети [1].

В докладе подробно рассматриваются средства обеспечения безопасности веб-сайтов, такие как:

Брандмауэр (или файерволл) – это системная утилита (сетевой экран) для контроля и фильтрации входящего/исходящего трафика [2]. Он может быть как для отдельного компьютера, так и для локальной сети. Основные функции брандмауэра: защита системы от внешних атак, таки как сканирование портов, подбор паролей, DDoS-атаки, контроль приложений (позволяет настроить доступ в сеть для каждого отдельного приложения), зональная защита – обеспечение различных уровней доступа в рамках локальной сети, протоколирование и предупреждение о возникающих угрозах.

Аутентификация – это процесс подтверждения, что этот человек именно тот, за кого себя выдает [3]. Например, при авторизации на веб-сайте пользователь вводит свои данные, а также задает пароль для своего аккаунта – в этом случае пароль является средством аутентификации. Потому что при повторном использовании веб-сайта пользователь вводит свой пароль и если пароль имеется в базе данных сайта, то аутентификация считается успешной, и пользователь получит доступ к сайту. Подобная проверка может быть как односторонней, так и взаимной – все зависит от способа защиты и политики безопасности сервиса. Повышенная сложность устройств безопасности, например, строгая аутентификация с помощью биометрических сканеров предлагает множество решений проблемы обеспечения доступа к системе только авторизованным пользователям [4].

Вирусы – это программы, которые способны уничтожать файлы компьютерных данных, программные файлы, а иногда даже компьютерное оборудование. Поэтому необходимы антивирусные сканеры. Они, как правило, атакуют слабые места в операционных системах или методах работы. Вирусы могут легко переноситься

из одной системы в другую, что затрудняет их контроль. По мнению различных экспертов, вирусы представляют собой гораздо большую проблему, чем хакеры, поэтому крайне важно обеспечить защиту контента от вирусов.

Рассмотрены аспекты безопасности веб-сайта. Существует две категории: безопасность системы – гарантия того, что другие люди не могут модифицировать сайт и информационная безопасность – обеспечение безопасности любой информации, например, собственных данных покупателя в интернет-магазине. Безопасность системы включает безопасность программного обеспечения, поскольку программное обеспечение может иметь ошибки и уязвимости, через которые можно пробраться в систему без пароля. К информационной безопасности относится хранение данных на веб-сайтах, таких как персональные и собственные данные пользователя.

Обеспечение безопасности включает наличие надежного сервера или виртуального хостинга с подключением SSL-сертификата. Веб-сайты ежедневно подвергаются риску из-за устаревшего и небезопасного программного обеспечения, поэтому важно обновлять сайт, как только появляется новый плагин или новая версия системы управления сайтом (СУС). После выбора СУС необходимо изменить настройки по умолчанию. Изменения помогают предотвратить большое количество атак. Настройки СУС могут включать в себя настройку комментариев элементов управления, видимости пользователей и разрешений, права доступа к файлам [5].

Нарушение безопасности является потенциально опасной угрозой для веб-сайта. Безопасность следует рассматривать как непрерывный процесс, требующий постоянного анализа, который не ограничивается только проверками. По результатам сканирования ресурс необходимо дорабатывать, закрывать дыры, а некоторые вопросы решать на стороне сервера.

СПИСОК ЛИТЕРАТУРЫ

1. Матяш Е.Д., Никонов В.В., Иванова И.А. Обеспечение безопасности веб-сайта //Евразийский союз ученых, 2016, №3(24). С.49-52
2. Лесько С.А. Модели и методы защиты веб-ресурсов: систематический обзор // Cloud of Science. Том 7, 2020, №3. С. 577-609
3. Татарникова Т.М., Веревкин С.А., Краева Е.В. Методика защиты от HID-атак // Проблемы информационной безопасности. Компьютерные системы. 2021, № 2 (46). С. 104-108.
4. Тимочкина Т.В., Татарникова Т.М., Пойманова Е.Д. Применение нейронных сетей для обнаружения сетевых атак//Известия высших учебных заведений. Приборостроение. Том 64, 2021, № 5. С. 357-363.
5. Краева Е.В., Веревкин С.А., Татарникова Т.М. Сокрытие файлов с помощью S-TOOLS // В сборнике: Информационные технологии в образовании. Сборник статей научно-практической конференции студентов, аспирантов и молодых ученых. Российский государственный гидрометеорологический университет, Институт информационных систем и геотехнологий. Санкт-Петербург, 2021. С. 83-87.

УДК 004.78

СЕТЕВОЙ ЭТИКЕТ

Опря Кристина Сергеевна
Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mail: oprya.kristina@bk.ru

Аннотация. В статье описываются основные правила общения в интернете, в интернет-сообществах и в интернет-сети в общем. Исследуются ошибки в общение и коммуникации с людьми, приводящие к последствиям.

Ключевые слова: этикет; правила общения; троллинг; холивары.

NETIQUETTE

Opria Kristina
Russian State Hydrometeorological University
79 Voronezhskya St, St. Petersburg, 192007, Russia
e-mail: oprya.kristina@bk.ru

Abstract. The article talks about basic rules of communication on the Internet, in Internet communities and in the Internet network in general are described. Errors in communication and communication with people, leading to consequences, are investigated.

Keywords: etiquette; communication rules; trolling; holivars.

Как в любой социальной среде, в сети интернет так же нужно соблюдать определённые правила для этичного общения всех пользователей. Однако, поскольку люди имеют разные представления об общении и о нормах поведения, то приходится ограничивать возможности пользователей в интернет-сообществах для предотвращения разных споров, оскорблений, бесконечных непримиримых споров.

Этикет является одним из ярко выраженных феноменов культуры, который затрагивает огромное количество чувств и эмоций человека, обогащает само человеческое общение [1]. Сетевой этикет, так же называемый нетикетом (или сетикетом) – это система правил, созданная людьми для общения друг с другом. Его рекомендуется соблюдать как новичкам, так и опытным пользователям. Однозначно сказать, что такое нетикет невозможно, но чаще всего это правила хорошего тона, общепринятые среди людей. Соблюдение правил хорошего тона повышает авторитет собеседника и привлекает внимание.

Исследовав разные источники с правилами поведения в интернете, можно вывести самые популярные. К ним относится отказ от: использования ненормативной лексики, ведения дискуссии на отвлечённые темы в неположенных для этого местах, обмана и воровства в любом виде и оскорбления людей.

Существует несколько базовых правил сетевого интернета. Это, во-первых, понятная подача информации – собеседники во время переписки не наблюдают друг за другом, поэтому для предотвращения нежелательного конфликта и недопонимания, стоит тщательно относится к написанию содержимого сообщения. Во-вторых, нужно «осмотреться» перед вступлением в дискуссию. Попав в новую область, нужно проанализировать, как общаются другие пользователи сети. В-третьих, нужно сохранять достоинство. Сетевой этикет подразумевает уважение к собеседнику. Если в реальной жизни оно проявляется манерой общения, то в сети это грамматика, лаконичность и оформление текста. И в-четвёртых, нужно отказаться от злоупотребления возможностями. Возможности системных администраторов достаточно обширны, но даже им нельзя читать частные переписки.

К сетевому этикету так же относятся особые правила ведения рабочей переписки [2, 3].

1. Следует писать четкую и понятную тему отправляемого сообщения. Даже если ваш собеседник отличается от вас возрастом, нужно обращаться к нему на «вы», и писать всеми известные, соответствующие нормам хорошего тона, клише. Так у вас будет больше шансов на быстрый и содержательный ответ.

2. Нужно включать блок подписи. В основном, подпись должна включать в себя ваше полное имя, должность, название компании и вашу контактную информацию, включая ваш телефонный номер. Вы также можете добавить туда немного рекламы для себя, но не переусердствуйте с какими-либо высказываниями или иллюстрациями».

3. Следует помнить, что все люди из разных культур говорят и пишут по-разному. Из-за культурных различий недопонимания могут возникнуть достаточно просто, особенно когда мы не можем наблюдать язык тела человека. Следует подгонять свои сообщения под культурную платформу получателя, насколько хорошо вы его знаете.

4. Из-за того, что мало чего в сети остается конфиденциальным, то следует писать соответственно. Посторонние люди могут увидеть письма, которые вы отправляете, поэтому следует не писать того, что может навредить вам или другим людям.

5. Использование профессионального почтового адреса поможет вашему будущему работодателю заметить вас быстрее. Если вы уже работаете на какую-то фирму, то стоит использовать корпоративный почтовый адрес. Если пишите письмо со своей личной почты, то в её названии должны содержаться ваше имя и фамилия. При правильном ведение рабочей переписки вы снижаете риски возникновения недопониманий и конфликтов около вас.

Развитие социальных сетей и интернет-коммуникаций способствует возникновению новых явлений. В современной интернет-терминологии довольно часто используются такие понятия, как «тролль» и «троллинг». Истоки троллинга в социальных сетях укоренены в самой социальной реальности, хотя в реальной практике человеческих отношений социальный троллинг менее популярен, поскольку сдерживается действующим законодательством. Задача тролля состоит в том, чтобы превратить спокойный тренд в ярый спор, конфликт, в который ввяжется как можно большее количество читателей, а изначальная тема разговора будет забыта напрочь. Одним из важных источников появления троллинга является «сетевая анонимность», которая в полной мере даёт человеку возможность высказываться так, как ему хочется, не соблюдая нормы приличия. Были проведены исследования, в которых выяснилось, что анонимность отбивает у человека чувство ответственности и даёт возможность чувствовать себя свободной. Из-за этого в интернет-сообществах могут возникать разного рода конфликты. Самые популярные из них, это холивары и флеймы. Термин «холивар» произошёл от английского holy war – священная война. По данным энциклопедии Britannica, так называют войны, которые ведутся в религиозных целях. В интернет-пространстве термины «холивар» и «религиозные войны» получили новое значение. Они используются для обозначения особых споров. Холивар можно узнать по таким характеристикам, как

1) продолжительность- разного рода «войны», проходящие долгое время под статьями, на форумах и в социальных сетях, имеют свойства то затихать, то снова возобновляться.

2)Категоричность - оппоненты принимают только свою позицию и не меняют её, даже если противник конструктивно и аргументированно доказывают свою правоту.

3) Эмоциональность - участники холиваров часто переключаются с предметами дискуссии на оценку личности оппонента и на оскорбления.

«Священные» войны в интернете иногда называют терминами «флейминг» или «флейм». Они произошли от английского *flame* – огонь – «спор ради спора», обмен сообщениями в местах многопользовательского сетевого общения, например, интернет-форумы, чаты, социальные сети, форумы и др., представляющий собой словесную войну, нередко уже не имеющую отношения к первоначальной причине спора. Сообщения флейма могут содержать личные оскорбления и зачастую направлены на дальнейшее разжигание ссоры. Иногда применяется в контексте троллинга, но чаще флейм вспыхивает просто из-за обиды на виртуального собеседника.

В целом, если сравнивать холивары с флеймамы, то отличия существуют. По данным TechTerms [4], флеймингом обозначают публикацию оскорбительных сообщений в адрес собеседников. То есть холивар может проходить без флейминга, если участники не оскорбляют друг друга, а просто спорят. Приводя примеры холиваров в мире технологий и программирования, можно выделить основные:

1) Спор Эндрю Таненбаума и Линуса Торвальдса. Это классический пример профессионального спора, который перерос в холивар или даже флейм. Таненбаум и Торвальдс начали спор из-за архитектуры ядра операционных систем. Первый утверждал, что лучше использовать микроядра, второй выступал за монолитное ядро. Участники спора много раз возвращались к публичному обсуждению архитектуры ядра, но каждый остался при своём мнении.

2) Объектно-ориентированное программирования против функционального программирования, известная как война парадигм. Ещё один пример вечного спора. Холивары вокруг этого вопроса разгораются с завидной регулярностью на разных площадках. Хороший пример – перевод статьи Роберта Мартина «Функциональное программирование vs Объектно-ориентированное программирование» на Хабре. Автор оригинала утверждает, что споры сторонников функционального и объектно-ориентированного подхода не имеют смысла, так как эти парадигмы отлично уживаются. Более 100 комментариев под переводом показывают, что у людей есть на этот счёт разные мнения.

3) Chrome vs FireFox vs Opera vs, ..., известная как война браузеров. В этом споре активно участвуют как простые пользователи, так и профессиональные разработчики. Если для первых дело скорее в привычках, удобстве и личных предпочтениях, то вторые приводят серьёзные аргументы в пользу любимых интернет-обозревателей. Спор сторонников Opera и FireFox начался на форуме GameDev.ru в 2006 году и продолжился в 2020 году.

Таким образом, для сохранения репутации в сети интернет и для удобного пользования серверами, стоит без пренебрежения относится к базовым правилам сетевого этикета. При их соблюдении не возникнет проблем при коммуникации с другими пользователями. В случае если пользователь попал в агрессивную среду, то стоит отказаться от своих эмоций и проигнорировать агрессивное общение.

СПИСОК ЛИТЕРАТУРЫ

1. Choukimath, Puttaraj. Role of Etiquette and Manners in Communication // Seminar on Communication Skills for Digital Age Libraries (Ed: Sangaraj Hosamani), Shree Swamy Narayan Guru College of Commerce, Chembur, Mumbai, 2006, pp.15-29.
2. Акулич М.М. Троллинг в социальных сетях: возникновение и развитие. // Вестник РУДН, 2012, №3. С. 30-36.
3. Синельникова Л.Н. Дискурс троллинга – коммуникация без табу. //Дискурс Пи. – Екатеринбург, 2016, №24/25. С.270-278.
4. Компьютерный словарю. URL: https://techterms.com/ (дата обращения: 10.06.2021)

УДК 004.056.5

ЗАЩИТА DNS-СЕРВЕРОВ ОТ АТАК

Стандровский Иван Андреевич
Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mail: istandrovskiy@gmail.com

Аннотация. В статье рассматривается система доменных имен и организация ее работы посредством функций DNS-сервера. Обсуждается проблема зашиты DNS-сервера от атак, в частности схемы настройки, такие как технология uRPF, функции IP Source Guard и утилиты dns-validator.

Ключевые слова: система доменных имен; DNS-сервер; атака; схема настройки DNS-сервера.

PROTECTING DNS SERVERS AGAINST ATTACKS

Standrovskiy Ivan
Russian State Hydrometeorological University
79 Voronezhskya St, St. Petersburg, 192007, Russia
e-mail: istandrovskiy@gmail.com

Abstract. The article discusses the domain name system and the organization of its work through the functions of a DNS server. The issue of protecting the DNS server from attacks is discussed, in particular configuration schemes such as uRPF technology, IP Source Guard functions, and dns-validator utilities.

Keywords: Domain Name System; DNS server; attack; DNS server configuration scheme.

Любой сайт в интернете фактически находится на каком-либо устройстве. Отдельный компьютер, подключенный к интернету, имеет индивидуальный номер, который называется IP-адресом. Он представляет собой набор из четырех чисел от 0 до 255. Благодаря этому адресу можно узнать, откуда загружается страница нужного ресурса. IP-адрес устройства можно сравнить с номером мобильного телефона, а DNS – с телефонной книгой. Если говорить конкретнее, DNS – система доменных имен, которая обеспечивает связь между наименованием сайта и его цифровым адресом. Иными словами, пользователь набирает доменное имя ресурса в адресной строке браузера, а DNS конвертирует его в IP-адрес и передает вашему устройству. После чего компьютер, находящийся по этому адресу, обрабатывает запрос и присылает информацию для открытия необходимой страницы сайта [1]. Структуру DNS можно сравнить с логическим деревом. Система содержит распределенную базу доменных имен – пространство, которое организовано по принципу иерархии. На верхнем уровне располагается корневой домен, к которому примыкают домены первого уровня. К каждому из них

присоединяются домены второго уровня и так далее. Система доменных имен действует посредством DNS-сервера, который нужен для выполнения двух основных функций:

хранения данных о соответствии имени домена конкретному IP-адресу,

кэширования ресурсных записей прочих DNS-серверов.

Если пользователь собирается посетить сайт, находящийся в другой стране, то регулярная передача запросов к первичному серверу занимает много времени и приводит к медленной загрузке страниц. Чтобы избежать подобных неудобств, DNS-сервер, находящийся рядом с вашим устройством, кэширует данные о запрашиваемых ранее IP-адресах и выдает их при следующем обращении.

Источниками хранения ресурсных записей являются исходные DNS-серверы, содержащие начальные связи между доменами и сетевыми адресами узлов.

Как правило, рекомендуют задействовать два сервера: первичный и вторичный. Это гарантирует получение доступа к вашему домену, потому как, если будет недоступен один сервер, ответит другой.

Рассмотрим поэтапно функционирование приложений, предназначенных для ответа на DNS-запросы:

Браузер получает запрос от пользователя и направляет его DNS-серверу сети, который ищет совпадение доменного имени и сетевого адреса. Если ответ обнаружен, то страница сайта загружается сразу. В противном случае запрос будет отправлен серверу более высокого уровня или корневому.

Корневой сервер направляет запрос серверу первого уровня, который в свою очередь передает его серверу второго уровня. Это движение продолжается до тех пор, пока не будет найдено совпадение имени и IP-адреса.

Браузер получает ответ на свой запрос, направляет его к хостингу, и страница открывается.

Также возможна обратная процедура – поиск имени домена в DNS-сервере, соответствующего запрашиваемому IP-адресу. К примеру, это происходит в случае работы с сервером электронной почты.

Фундаментом для обработки запросов о доменных именах являются корневые серверы, отвечающие за корневую DNS-зону. Ими руководят разные операторы, которые обеспечивают бесперебойное функционирование серверов. Первые корневые серверы появились в Северной Америке, но с течением времени они стали появляться в других странах мира. На сегодня существует 123 корневых сервера, которые располагаются в разных точках мира (в зависимости от интенсивности пользования всемирной паутиной).

Одному домену могут подходить несколько сетевых адресов, например, интернет-сайт и почтовый сервер. Более того, каждое доменное имя содержит один или несколько поддоменов.

Все соответствия домена и его IP-адресов хранятся в файле на DNS-сервере, содержимое которого называется DNS-зона. Чтобы внести информацию в систему DNS, необходимо прописать ресурсные записи.

Различают несколько ключевых типов ресурсных записей, информация о которых хранится на DNS-сервере:

A – адрес веб-ресурса, который соответствует введенному имени домена.

MX – адрес почтового сервера.

CNAME – указание привязки аналога к собственному доменному имени. Чаще всего используется для прикрепления поддомена. Например, можно привязать веб-адрес www.site.ru к фактическому сайту для домена site.ru.

NS – адрес DNS-сервера, отвечающего за содержание прочих ресурсных записей.

TXT – любая текстовая информация о домене.

SPF – данные с указанием списка серверов, которым позволено отправлять письма от имени указанного домена.

SOA – исходная запись зоны, в которой указаны сведения о сервере, содержащем образцовую информацию о доменном имени.

Опасность воздействия злоумышленников на DNS приобрела глобальные масштабы. Ранее уже были ситуации атак на серверы такого формата, которые приводили к многочисленным сбоям в работе всемирной паутины, в особенности известных социальных сетей.

Наиболее опасными считают нападения на корневые серверы, хранящие данные об IP-адресах. Например, в историю вошла произошедшая в октябре 2002 года DDoS-атака на 10 из 13 серверов верхнего уровня.

Протокол DNS получает результаты по запросам с помощью протокола пользовательских датаграмм UDP. UDP использует модель передачи данных без соединений для обеспечения безопасности и целостности информации. Таким образом, большинство атак производятся на этот протокол с помощью подделки IP-адресов.

Существует несколько схем, настройка которых позволит защитить DNS-сервер от атак злоумышленников [2-4]:

Использование технологии uRPF (Unicast Reverse Path Forwarding). Суть состоит в том, чтобы определить возможность принятия пакета с конкретным адресом отправителя на указанном устройстве для передачи данных. Пакет проходит проверку и принимается в том случае, когда сетевой интерфейс, с которого он получен, предназначен для обмена информацией с адресатом данного пакета. В обратной ситуации пакет будет отброшен. Этот способ помогает выявить и частично отобрать фальшивый трафик, но не гарантирует надежную защиту от фальсификации. uRPF полагает, что данные отправляются на определенный адрес через неизменный интерфейс. Ситуация усложняется, если появляется несколько провайдеров.

Применение функции IP Source Guard. В ее основе лежит технология uRPF и проверка DHCP-пакетов. IP Source Guard отслеживает DHCP-трафик в интернете и выясняет, какие IP-адреса получили сетевые устройства.

Это позволяет выявить поддельный трафик на некоторых портах установки. После этого данные собираются и записываются в общую таблицу итогов проверки DHCP-пакетов. В дальнейшем IP Source Guard обращается к этой таблице, чтобы осуществить проверку пакетов, полученных коммутатором. Если IP-адрес пакета не совпадает с адресом источника, то пакет откладывается.

Использование утилиты dns-validator. Эта программа контролирует передачу всех пакетов DNS, соотносит запрос с ответом и в случае расхождения названий отправляет уведомление пользователю.

СПИСОК ЛИТЕРАТУРЫ

1. Что такое DNS? [Электронный ресурс]. URL: https://1cloud.ru/blog/chto-takoe-dns (Дата обращения: 17.06.2021).
2. Татарникова Т.М., Веревкин С.А., Краева Е.В. Методика защиты от HID-атак // Проблемы информационной безопасности. Компьютерные системы. 2021, № 2 (46). С. 104-108.
3. Тимочкина Т.В., Татарникова Т.М., Пойманова Е.Д. Применение нейронных сетей для обнаружения сетевых атак//Известия высших учебных заведений. Приборостроение. Том 64, 2021, № 5. С. 357-363.
4. Краева Е.В., Веревкин С.А., Татарникова Т.М. Сокрытие файлов с помощью S-TOOLS // В сборнике: Информационные технологии в образовании. Сборник статей научно-практической конференции студентов, аспирантов и молодых ученых. Российский государственный гидрометеорологический университет, Институт информационных систем и геотехнологий. Санкт-Петербург, 2021. С. 83-87.

УДК 004.89

ОБЗОР ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РЕАЛИЗАЦИИ НЕЙРОННЫХ СЕТЕЙ

Тимочкина Татьяна Владимировна
Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mail: timo4kina.tanya@yandex.ru

Аннотация. Рассматривается наиболее известное свободно распространяемое программное обеспечение с открытым исходным кодом, применяемое для реализации различных видов нейронных сетей.

Ключевые слова: искусственные нейронные сети; программное обеспечение; библиотека нейронных сетей.

OVERVIEW OF SOFTWARE FOR IMPLEMENTING NEURAL NETWORKS

Timochkina Tatiana
Russian State Hydrometeorological University
79 Voronezhskya St, St. Petersburg, 192007, Russia
e-mail: timo4kina.tanya@yandex.ru

Abstract. Considered the most famous opensource software open source used for the implementation of various types of neural networks.

Keywords: artificial neural networks; software; library of neural networks.

Современные нейронные сети могут играть в компьютерные игры, писать музыку, рисовать и многое другое. На рынке программного обеспечения множество программных пакетов, которые реализуют нейронные сети. Кратко рассмотрим некоторые наиболее известные [1-4]:

Amygdala - программное обеспечение с открытым исходным кодом для моделирования всплесков нейронных сетей, написанное на C++. Использует биологически точные модели для создания сетей, способных хорошо работать в режиме реального времени, также большое внимание уделяется поддержке многократной распределенной обработке. В настоящее время реализована в виде библиотеки C++, подходящей для использования программистами, также предусмотрены дополнительные интерфейсы к языкам программирования, отличным от C++, для расширения доступности и полезности Amygdala.

Annie - библиотека искусственных нейронных сетей для C++ (Windows и Linux) с открытым исходным кодом. Поддерживает обучение, сохранение и выполнение многослойных персептронов, радиальных базисных функций, сетей Хопфилда и обычных рекуррентных сетей. Наряду с библиотекой включены некоторые примеры приложений и бинарные утилиты, помогающие создать обучающие наборы, обучить сеть, визуализировать и т.д. Взаимодействует с инструментами Nela Network от Matlab, который позволяет создавать и обучать сети Matlab, а затем экспортировать их в формат, понятный библиотеке Annie.

ECANSE - среда разработки программного обеспечения для применения технологий мягких вычислений, таких как нейронные сети, нечеткая логика и генетические алгоритмы. Используется для разработки, моделирования и тестирования приложений мониторинга среды и телекоммуникаций как мощный и гибкий инструмент. На этапе обучения система обучается с использованием исторической информации, полученной за прошедший период. На этапе тестирования необходимые данные обрабатываются в зависимости от текущих измеренных данных.

FANN - бесплатная библиотека нейронных сетей с открытым исходным кодом, которая реализует многослойные нейронные сети на C с поддержкой полносвязных и слабосвязанных сетей. Поддерживается кроссплатформенное выполнение как с фиксированной, так и с плавающей точкой, включает в себя структуру для удобной обработки наборов обучающих данных. Библиотека проста в использовании, универсальна, хорошо

документирована, доступны привязки к более чем 20 языкам программирования, доступно несколько графических пользовательских интерфейсов. для новичков имеется легко читаемая вводная статья и справочное руководство, сопровождаемое примерами и рекомендациями по использованию.

Genesis - платформа для моделирования сложных нейронных систем. Система нейронной симуляции была разработана для создания биологически реалистичных симуляций на различных уровнях, от субклеточных компонентов и биохимических реакций, до сложных моделей одиночных нейронов, симуляции больших сетей и моделей системного уровня. Использует язык моделирования высокого уровня для создания нейронов и их сетей. Команды могут быть введены в интерактивном режиме в командную строку, с помощью сценариев моделирования или через графический интерфейс. Язык сценариев и модули достаточно мощны, поэтому для определения сложной симуляции требуется всего несколько строк сценария.

Joone - (Java Object Oriented Neural Engine) - свободно распространяемый нейросетевой фреймворк на Java для создания, обучения и тестирования ИНС. Это мощная среда, которая подойдет как для новичков, так и для профессиональных пользователей. Joone состоит из центрального движка, который является точкой опоры для разработанных приложений. Нейронные сети Joone могут быть построены на локальном компьютере, обучены в распределенной среде и работать на любом устройстве. Основная идея заключается в том, чтобы создать основу для продвижения приложений на основе искусственного интеллекта. Каждый может написать модули для реализации новых алгоритмов или архитектур, начиная с простых компонентов, распространяемых в ядре.

LibF2N2 - нейросетевая библиотека с открытым исходным кодом, содержит современные классы нейронных сетей с прямой связью, которые реализованы на нескольких языках и способны сохранять и загружать веса нейронных сетей в один и тот же формат файла. Реализует сети прямого распространения на C++ и PHP. Для быстрого обучения сети используют библиотеку F2N2, которая мгновенно инициализирует работающую нейронную сеть и имеет в своем распоряжении данные, необходимые для обучения. После этого скомпилированная программа сохраняет весовые коэффициенты обученной сети в текстовый файл, которые после можно использовать для создания нейронной сети идентичной структуры.

Neural Network Leaves Recognition - java-приложение на основе нейронной сети для распознавания изображений листьев в соответствии с ранее обученной сетью обратного распространения.

Neural Network Toolbox for MATLAB - среда для исследований нейронных сетей в MATLAB. Обеспечивает основу для проектирования и реализации глубоких нейронных сетей с помощью алгоритмов, предварительно обученных моделей и приложений. Дает возможность использовать сверточные нейронные сети и сети с кратковременной памятью для классификации и регрессии изображений, временных рядов и текстовых данных. Приложения и графики помогают визуализировать активации, редактировать и анализировать сетевые архитектуры, а также отслеживать ход обучения.

Simbrain - бесплатный инструмент для построения, запуска и анализа нейронных сетей с открытым исходным кодом, компьютерное моделирование схем мозга. Simbrain стремится быть максимально визуальным и простым в использовании, его особенности включают интегрированные «мировые компоненты» и способность представлять пространство состояний сети. Данный инструмент написан на Java и работает на основных операционных системах.

Анализ функциональных возможностей различных программных средств показал, что все они имеют схожие возможности, наглядный и простой в освоении интерфейс и открытый исходный код. Одни обладают большим количеством инструментов и высокой стоимостью, другие ограничены в выборе функций, позволяющих реализовать сети определенных структур. Под разные задачи может выбираться разное ПО, но основные требования будут схожи. Работа с нейронными сетями требует большого количества вычислительных ресурсов, именно поэтому большое число компаний работает над совершенствованием нейросетевых алгоритмов и созданием принципиально новых аппаратных комплексов.

СПИСОК ЛИТЕРАТУРЫ

1. Применение нейросетевых технологий: Разработка программного обеспечения. [Электронный ресурс]. URL: https://habr.com/ru/post/413095/ (дата обращения: 25.05.2021)
2. Тимочкина Т.В., Татарникова Т.М., Пойманова Е.Д. Применение нейронных сетей для обнаружения сетевых атак// Известия высших учебных заведений. Приборостроение. Том 64, 2021, № 5. С. 357-363.
3. Deep Learning Toolbox. [Электронный ресурс]. URL: https://www.mathworks.com/products/deep-learning.html (дата обращения: 25.05.2021)
4. Татарникова Т.М., Бимбетов Ф., Богданов П.Ю. Выявление аномалий сетевого трафика методом глубокого обучения // Известия СПбГЭТУ ЛЭТИ. 2021, № 4. С. 36-41.

УДК 004.7

ИСПОЛЬЗОВАНИЕ БРАНДМАУЭРОВ ДЛЯ ЗАЩИТЫ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ

Хижнякова Ксения Александровна
Российский государственный гидрометеорологический университет
Воронежская ул., 79, Санкт-Петербург, 192007, Россия
e-mail: ksenia.khizhnyakova@mail.ru

Аннотация. Рассматриваются плюсы и минусы использования брандмауэров для защиты данных пользователей и сравнение брандмауэров с другими способами защиты цифровых данных.

Ключевые слова: брандмауэр; фаерволл; защита данных организаций; цифровые данные; средства защиты; повышение безопасности данных.

USING FIREWALLS FOR PROTECTION OF PERSON'S DATA

Khizhnyakova Ksenia
Russian State Hydrometeorological University
79 Voronezhskya St, St. Petersburg, 192007, Russia
e-mail: ksenia.khizhnyakova@mail.ru

Abstract. The pros and cons of using firewalls to protect persons' data and comparison of firewalls with other ways to protect digital data are discussed.

Keywords: firewall; data protection of organizations; digital data; security tools; improving data security.

Брандмауэр можно назвать защитным экраном между глобальным интернетом и локальной компьютерной сетью. Он проверяет и отфильтровывает все данные, которые через него поступают (имена, IP-адреса, приложения, другие характеристики входящего трафика). В результате фильтрации брандмауэр может или заблокировать, или пропустить данные [1].

В общем брандмауэр выполняет решает следующие задачи [2]:

– предотвращение любого несанкционированного доступа к компьютеру и сетям, которые подключены к сети;

– отслеживание взаимодействия компьютера с другими компьютерами в сети;

– предупреждение о попытках подключения других компьютеров или локальных программ к другим компьютерам.

Стоит перечислить и некоторые недостатки данного способа защиты:

– брандмауэры не могут запретить авторизованному пользователю передать, уничтожить, модифицировать какую-либо информацию;

– разрозненность систем (нет единого центра управления, который отвечал бы и за брандмауэры, и за антивирусы, и за другие способы защиты);

– крупные локальные сети требуют дорогих аппаратных решений.

Так как система брандмауэра довольно сложная, существует много разнообразных способов классифицировать брандмауэры, и одним из них является распределение с точки зрения уровней. По этому способу существует три уровня: пакетный, соединения, прикладной. Работа на пакетном уровне заключается, соответственно, в фильтрации пакетов. Работа шлюза на уровне соединения заключается в том, что пользовательский процесс соединяется с фаерволлом, который самостоятельно устанавливает соединение с внешней сетью. Прикладной уровень – самый верхний, фактически брандмауэры такого уровня представляют собой отдельные подсистеме.

Разбивка на уровни является условной, то есть существуют фаерволлы, которые могут работать на нескольких уровнях одновременно. Можно сказать, что практически все современные брандмауэры функционируют сразу на нескольких уровнях, так как стремятся расширить функциональность и максимально использовать преимущества работы по той или иной схеме.

Новые файрволы часто называют «**следующим поколением», то есть они объе**диняют все старые подходы с углубленным анализом отфильтрованного контента, а также сравнивают контент с базой данных, чтобы выявить потенциально опасный трафик. Такая технология получила название Stateful Inspection, а брандмауэры, работающие по смешанной схеме, называются Stateful Inspection Firewall. Ещё современные брандмауэры часто имеют встроенные дополнительные системы безопасности, например, виртуальные частные сети (VPN), системы предотвращения и обнаружения вторжений (IPS / IDS), управление идентификацией, управление приложениями и веб-фильтрация [3].

На рынке представлены разные файерволлы, в докладе рассматриваются 4 варианта для Windows со сравнением их возможностей и настроек:

– Comodo Firewall
– Avast! Internet Security
– TinyWall
– PrivateFirewall

Основным показателем сравнения брандмауэров выбрана вероятность предотвращение рисков, а не на ликвидацию их последствий.

СПИСОК ЛИТЕРАТУРЫ

1. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. – М: Книжный мир, 2009.
2. Веревкин С.А., Татарникова Т.М., Краева Е.В., Мартын И.А. Тестирование защищенности беспроводных сетей. В сборнике: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ. Сборник статей научно-практической конференции студентов, аспирантов и молодых ученых. Российский государственный гидрометеорологический университет, Институт информационных систем и геотехнологий. Санкт-Петербург, 2021. С. 29-33
3. Веревкин С.А., Татарникова Т.М., Краева Е.В., Мартын И.А. разработка виртуального маршрутизатора. В сборнике: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАНИИ. Сборник статей научно-практической конференции студентов, аспирантов и молодых ученых. Российский государственный гидрометеорологический университет, Институт информационных систем и геотехнологий. Санкт-Петербург, 2021. С. 74-77.

ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УДК 378.1

ТЕХНОЛОГИЯ ОБУЧЕНИЯ ПРОЕКТИРОВАНИЮ ИНФОРМАЦИОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ КОНЦЕПЦИИ UML

Дубенецкий Владислав Алексеевич, Кузнецов Александр Григорьевич, Цехановский Владислав Владимирович

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mails: chr12@yandex.ru,dubvl@list.ru,vvcehanovsky@mail.ru

Аннотация. Рассматривается технология обучения проектированию безопасных информационных систем на основе модельного подхода к разработке с использованием case-средства поддерживающего концепцию на основе языка моделирования UML.

Ключевые слова: безопасные информационные системы; технология проектирования; case-средство; UML.

THE TECHNOLOGY OF TEACHING DESIGN OF INFORMATION SYSTEMS USING THE CONCEPT OF UML

Dubenetsky Vladislav, Kuznetsov Alexander, Tsekhanovsky Vladislav

Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mails: chr12@yandex.ru, dubvl@list.ru, vvcehanovsky@mail.ru

Abstract. The article considers the technology of training in the design of information systems based on a model approach to development using case-a tool that supports the concept based on the UML modeling language.

Keywords: secure information systems; design technology; case-tool; UML.

Проектирование безопасной информационной системы (БИС) сложный многофакторный процесс, который предполагает построение ряда абстрактных моделей, описывающих различные ее аспекты [1, 2].

В настоящее время в области проектирования БИС с успехом применяется концепция моделирования на основе унифицированного языка моделирования UML.

Унифицированный язык моделирования (Unified Modeling Language, UML) является графическим языком для визуализации, специфицирования, конструирования и документирования ИС, включая проектирование программного обеспечения и физическую модель базы данных.

Для использования UML удобно использовать CASE-средства (Computer-Aided Software Engineering) — это набор инструментов и методов программной инженерии для проектирования программного обеспечения, который помогает обеспечить высокое качество программ, отсутствие ошибок и простоту в обслуживании программных продуктов. Существует достаточно много CASE-инструментов моделирования и проектирования ИС, например StarUml [3].

С помощью UML можно детально описать БИС, начиная с разработки концептуальной модели с ее бизнес-функциями и процессами, а также описать особенности реализации системы. Используя такой подход, можно разрабатывать «сложные» БИС быстро и качественно, по сравнению с традиционным.

UML имеет свою нотацию – принятые обозначения. Нотация обеспечивает семантику языка, является способом унификации обозначений визуального моделирования, обеспечивает всестороннее представление системы, которое сравнительно легко и свободно воспринимается студентом. Моделирование с помощью UML осуществляется поэтапным построением ряда моделей, каждая из которых отражает какую-то часть или сторону безопасной информационной системы.

Основные модели UML:

- вариантов использования (use case);
- классов (class);
- кооперации (collaboration);
- последовательности (sequence);
- состояний (statechart);

- деятельности (activity);
- компонентов (component);
- развертывания (deployment).

Разработки и построения этих локальных моделей достаточно для полного построения модели БИС [1].

СПИСОК ЛИТЕРАТУРЫ

1. Дубенецкий В.А., Кузнецов А.Г., Цехановский В.В. Технология создания корпоративных информационно-управляющих систем на основе моделей, допускающих исполнение. СПб.:Изд-во СПбГЭТУ «ЛЭТИ», 2019. ISBN 978-5-7629-2511-2 158 с.
2. Водяхо А.И., Выговский Л.С., Дубенецкий В.А., Цехановский В.В. Архитектурные решения информационных систем: учебник для СПО / Санкт-Петербург: Лань, 2021. - 356 с. ISBN 978-5-8114-7554-4. 2-е изд. стер. Печатное издание.
3. StarUML. The Open Source UML/MDA Platform. Versoon 5.0.2.1570.Руководство пользователя . Перевод Д. В. Летуновского, 2007, 207 с.

УДК 378.14

МЕЖДИСЦИПЛИНАРНЫЕ ОСОБЕННОСТИ ОРГАНИЗАЦИИ НЕПРЕРЫВНОГО ОБРАЗОВАНИЯ В ОБЛАСТИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ И КОГНИТИВНОЙ БЕЗОПАСНОСТИ

Жигадло Валентин Эдуардович[1], Одинокая Мария Александровна[2], Жигадло Надежда Владимировна[3]
[1] ЗАО «Институт телекоммуникаций»
Кантемировская ул., 5, Санкт-Петербург, 194100, Россия
[2] Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
[3] Гимназия №652
Тореза пр., 41, Санкт-Петербург, 194223, Россия
e-mails: zve@mail.ru, World.Maria@hotmail.com

Аннотация. В докладе рассматривается междисциплинарный характер методологии организации непрерывного образовательного процесса при изучении вопросов информационно-психологической и когнитивной безопасности в школе и ВУЗе. Особое внимание уделяется вопросам воспитания детей в духе традиционных русских ценностей и патриотизма, повышения цифровой грамотности и реализации методов цифровой гигиены, как в среде педагогического состава образовательной организации, так и в среде обучаемых.

Ключевые слова: цифровые технологии; информационные технологии; информационная безопасность; защита информации; защита от информации; цифровая гигиена.

INTERDISCIPLINARY FEATURES OF THE ORGANIZATION OF CONTINUING EDUCATION IN THE FIELD OF INFORMATION, PSYCHOLOGICAL AND COGNITIVE SECURITY

Zhigadlo Valentin[1], Odinokaya Maria[2], Zhigadlo Nadezhda[3]
[1] JSC "Institute of Telecommunications"
5 Kantemirovskaya St, St. Petersburg, 194100, Russia
[2] Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
[3] Gymnasium № 652
41 Torez Av, St. Petersburg, 194223, Russia
e-mails: zve@mail.ru, World.Maria@hotmail.com

Abstract. The theses of the report consider the interdisciplinary nature of the methodology of the organization of the continuous educational process in the study of information, psychological and cognitive security at school and university. Special attention is paid to the issues of raising children in the spirit of traditional Russian values and patriotism, improving digital literacy and implementing digital hygiene methods, both among the teaching staff of the university and among students.

Keywords: digital technologies; information technologies; information security; information protection; information protection; digital hygiene.

В настоящее время, в условиях усиливающегося противоборства в информационной сфере, ведения против нашей страны информационных и ментальных войн [1], существенно возрастает роль и значение информационной безопасности, в части защиты подрастающего поколения и, в первую очередь, молодежи от деструктивного информационного воздействия.

Как определено в Стратегии национальной безопасности Российской Федерации [2] - «…Целью обеспечения информационной безопасности является укрепление суверенитета Российской Федерации в информационном пространстве».

В докладе подробно рассматриваются вопросы неоднозначности (двойственного характера) воздействия информации на человека и социальную среду в целом – конструктивного и деструктивного и, соответственно, возникающих новых задач защиты от деструктивного, разрушительного воздействия информации на учеников начальной и средней школы, на студентов ВУЗов.

Подробно анализируются механизмы разрушительного воздействия информации на молодое поколение, анализируются известные способы защиты от информации и формулируются основные направления научных исследований в области защиты от информации.

Сформулированы цели, задачи и методы информационно-психологической и когнитивной безопасности, направленные на формирование устойчивого иммунитета к существующим и вновь возникающим угрозам деструктивного информационного воздействия на население страны и, как следствие, обеспечение государственного суверенитета в информационном пространстве страны.

Одной из ключевых задач информационно-психологической и когнитивной безопасности и обеспечения суверенитета страны в информационном пространстве выделяется задача подготовки кадров в области информационно-психологической и когнитивной безопасности и повышения общего образовательного уровня населения в области информационной безопасности.

В докладе рассматриваются вопросы деструктивного воздействия информации на человека и социальную среду в целом и, соответственно, новая задача образования - организация непрерывной подготовки в области информационно-психологической безопасности (ИПКБ) [3], начиная с младших классов начальной школы и заканчивая пост вузовской подготовкой.

Анализ структуры деструктивного информационного воздействия на молодое поколения и особенностей процесса подготовки в школе и в ВУЗе показал необходимость использования междисциплинарного подхода при реализации процесса подготовки по вопросам информационной безопасности, а, в ряде случаев, и существенного пересмотра структуры дисциплин и содержания образовательных программ.

Отмечается, что процесс подготовки в области информационно-психологической безопасности включает две взаимоувязанные составные части – изучение источников и угроз в области ИПКБ, обучение методам и средствам защиты от деструктивного информационного воздействия, включая вопросы цифровой (информационной) гигиены, и развитие у молодого поколения таких внутренних морально-нравственных и ценностных потенциалов, которые позволили бы выработать у них устойчивый иммунитет к любому деструктивному информационному воздействию.

Показано, что если первая составляющая подготовки может быть реализована в рамках отдельной дисциплины по ИПКБ (как в начальной и средней школе, так и в ВУЗе), то вторая составляющая в целом носит междисциплинарный характер, затрагивает практически все гуманитарные и общеобразовательные дисциплины (история, в первую очередь, история Отечества, литература, биология, география, литература, изобразительное искусство, музыка) и требует глубокого пересмотра большинства учебных программ, с целью их переориентации на пропаганду традиционных национальных истинно русских культурных ценностей, воспитание молодого поколения детей в духе традиционных русских ценностей и патриотизма.

Показано, что при этом потребуется не только пересмотр образовательных программ, но и существенное изменение содержания многих дисциплин, а, в итоге, пересмотр и внесение изменений в учебные планы подготовки, пересмотр и разработка новой методологии преподавания всего спектра общеобразовательных дисциплин.

В докладе подробно анализируется существующая методология преподавания предметов в начальной, средней школе, ВУЗе, рассматриваются особенности изучения предметной области информационно-психологической безопасности, ее междисциплинарные особенности.

Проводится анализ структуры дисциплин образовательных программ начальной школы, в частности, по соотношению объема материала и выделяемых учебных часов, для примера, по предметам «История древнего мира» и «Окружающий мир» (его одного раздела –«Мое Отечество»).

Обосновывается вывод, в целях обеспечения принципа системности, при изучении ИПКБ о возможном изменении как содержания ряда дисциплин (история, география), так и ввода новых дисциплин, ориентированных на изучение национальной истории (истории России и древней Руси), культуры, обычаев, традиций начиная с древней истории.

Особое внимание обращается на насущную необходимость нормативного возвращения в учебный процесс функции воспитания во всех его аспектах, направленную на воспитание детей (начиная с младших классов) в духе традиционных русских ценностей и патриотизма, повышения уровня культуры, цифровой грамотности и реализации методов цифровой гигиены, как в среде педагогического состава образовательной организации, так и в среде обучаемых.

СПИСОК ЛИТЕРАТУРЫ

1. Ильницкий, А.М., Безопасность страны как фундамент развития. М.: «Арсенал Отечества», № 1 (51), 2021.
2. Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400.
3. Юсупов, Р.М., Жигадло. В.Э. О проблемах защиты от разрушительного воздействия информации. // Перспективные направления развития отечественных информационных технологий. Материалы конференции, Ч. 1., Севастополь, 22-26 сентября 2020 г. / Севастопольский государственный университет, науч. ред. Б.В. Соколов. – Севастополь: 2020. – С.35-37.

УДК 378.14

МЕТОДОЛОГИЯ НЕПРЕРЫВНОГО ОБРАЗОВАНИЯ В ОБЛАСТИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ И КОГНИТИВНОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ИНФОРМАЦИОННЫХ И МЕНТАЛЬНЫХ ВОЙН

Жигадло Валентин Эдуардович[1], Одинокая Мария Александровна[2], Жигадло Надежда Владимировна[3], Елисеева Елена Николаевна[3]

[1] ЗАО «Институт телекоммуникаций»
Кантемировская ул., 5, Санкт-Петербург, 194100, Россия
[2] Санкт-Петербургский политехнический университет Петра Великого
Политехническая ул., 29, Санкт-Петербург, 195251, Россия
[3] Гимназия №652
Тореза пр., 41, Санкт-Петербург, 194223, Россия
e-mails: zve@mail.ru, World.Maria@hotmail.com

Аннотация. В тезисах доклада рассматривается методология организации непрерывного образовательного процесса при изучении вопросов информационно-психологической и когнитивной безопасности. Особое внимание уделяется вопросам воспитания детей в духе традиционных русских ценностей и патриотизма, повышения цифровой грамотности, а также реализации методов цифровой гигиены, как в среде педагогического состава ВУЗа, так и в среде студентов.

Ключевые слова: цифровые технологии; информационные технологии; информационная безопасность; защита информации; защита от информации; цифровая гигиена.

METHODOLOGY OF THE ORGANIZATION OF EDUCATION IN THE FIELD OF INFORMATION, PSYCHOLOGICAL AND COGNITIVE SECURITY IN THE CONDITIONS OF INFORMATION AND MENTAL WARS

Zhigadlo Valentin[1], Odinokaya Maria[2], Zhigadlo Nadezhda[3], Eliseeva Elena[3]

[1] JSC "Institute of Telecommunications"
5 Kantemirovskaya St, St. Petersburg, 194100, Russia
[2] Peter the Great St. Petersburg Polytechnic University
29 Polytechnicheskaya St, St. Petersburg, 195251, Russia
[3] Gymnasium № 652
41 Torez Av, St. Petersburg, 194223, Russia
e-mails: zve@mail.ru, World.Maria@hotmail.com

Abstract. The theses of the report consider the interdisciplinary nature of the methodology of the organization of the continuous In the theses of the report, the methodology of organizing a continuous educational process in the study of information, psychological and cognitive security issues is considered. Special attention is paid to the issues of raising children in the spirit of traditional Russian values and patriotism, improving digital literacy, as well as implementing digital hygiene methods, both among the teaching staff of the university and among students.

Keywords: digital technologies; information technologies; information security; information protection; information protection; digital hygiene.

В настоящее время все больше усиливается противоборство в информационной сфере. Против нашей страны развернуты широко масштабные информационная война в крайне агрессивной форме ее проявления – когнитивной (ментальной) войны, направленной на деструкцию (изменение) мироощущения, миропонимания и целостного мировоззрения жителей [1]. Под воздействием когнитивных операций осуществляется манипуляция сознанием и навязывание ложных убеждений. Результатом когнитивных операций является инверсия убеждений, мировоззрения и идеологических ориентиров. Если в классических войнах целью является уничтожение живой силы противника, а в современных кибервойнах - уничтожение инфраструктуры противника, то целью новой когнитивной (ментальной) войны является манипуляция сознанием, уничтожение самосознания, изменение ментальной (цивилизационной) основы общества, разрушение мировоззрения. И если живую силу и инфраструктуру можно восстановить, то «ход эволюции сознания повернуть вспять невозможно, тем более что последствия этой "ментальной" войны проявляются не сразу, а только как минимум через поколение, когда сделать уже что-либо будет просто невозможно" [1]. В этих условиях существенно возрастает роль и значение информационной безопасности, в частности, задач защиты всего населения и, в первую очередь, молодежи от деструктивного информационного воздействия. Данным вопросам особое внимание уделено так же в Стратегии национальной безопасности Российской Федерации [2], где информационной безопасности посвящен целый раздел и определено, что целью обеспечения информационной безопасности является укрепление суверенитета Российской Федерации в информационном пространстве.

В докладе подробно рассматриваются вопросы неоднозначности (двойственного характера) воздействия информации на человека и социальную среду в целом – конструктивного и деструктивного и, соответственно, возникающих новых задач защиты от деструктивного, разрушительного воздействия информации на учеников начальной и средней школы, на студентов ВУЗов. Подробно анализируются механизмы разрушительного

воздействия информации на молодое поколение, анализируются известные способы защиты от информации и формулируются основные направления научных исследований в области защиты от информации.

Сформулированы цели, задачи и методы информационно-психологической и когнитивной безопасности (ИПКБ) [3], направленные на формирование устойчивого иммунитета к существующим и вновь возникающим угрозам деструктивного информационного воздействия на население страны и, как следствие, обеспечение государственного суверенитета в информационном пространстве страны.

Одной из ключевых задач информационно-психологической и когнитивной безопасности и обеспечения суверенитета страны в информационном пространстве выделяется задача подготовки кадров в области информационно-психологической и когнитивной безопасности и повышения общего образовательного уровня населения в области информационной безопасности.

Особое внимание уделено методологии образования в области информационно-психологической и когнитивной безопасности и, в частности, междисциплинарному характеру организации непрерывного образовательного процесса при изучении вопросов информационно-психологической и когнитивной безопасности, начиная с младших классов начальной школы и заканчивая пост вузовской подготовкой. Особое внимание уделяется вопросам воспитания детей в духе традиционных русских ценностей и патриотизма, повышения цифровой грамотности и реализации методов цифровой гигиены, как в среде педагогического состава образовательных учреждений, так и в среде обучаемых.

В результате анализа структуры дисциплин, изучаемых в начальной, средней и высшей школе, новых современных угроз информационной безопасности и деструктивного характера воздействия информации на человека и социальную среду в целом, делается вывод о необходимости существенного пересмотра методологии подготовки специалистов в области информационной безопасности, а так же формулируется новая задача обеспечения массовой грамотности населения - организация непрерывной подготовки в области информационно-психологической безопасности, начиная с младших классов начальной школы и заканчивая пост вузовской подготовкой. Анализ структуры деструктивного информационного воздействия на молодое поколения и особенностей процесса подготовки в школе и в ВУЗе показал так же необходимость использования междисциплинарного подхода при реализации процесса подготовки по вопросам информационной безопасности, а, в ряде случаев, и существенного пересмотра структуры дисциплин и всего учебного плана с целью их переориентации на пропаганду традиционных национальных истинно русских культурных ценностей, воспитание молодого поколения детей в духе любви к Родине и патриотизма.

В докладе рассматриваются особенности методологии организации образования в области информационно-психологической и когнитивной безопасности в условиях информационных и ментальных войн, основанной на вышеперечисленных особенностях образовательного процесса, связанных с непрерывным его характером и междисциплинарностью.

Особое внимание обращается на насущную необходимость нормативного возвращения в учебный процесс функции воспитания во всех его аспектах, повышения уровня культуры, цифровой грамотности и реализации методов цифровой гигиены.

СПИСОК ЛИТЕРАТУРЫ

1. А. М. Ильницкий. Безопасность страны как фундамент развития. М.: «Арсенал Отечества», № 1 (51), 2021.
2. Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400.
3. Р. М. Юсупов, В. Э. Жигадло. О проблемах защиты от разрушительного воздействия информации. // Перспективные направления развития отечественных информационных технологий. Материалы конференции, Ч. 1., Севастополь, 22-26 сентября 2020 г. / Севастопольский государственный университет, науч. ред. Б.В. Соколов. – Севастополь: 2020. – С.35-37.

УДК 004

ГУМАНИТАРНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СИСТЕМА ОБРАЗОВАНИЯ

Кононов Олег Александрович, Кононова Ольга Васильевна
Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП)
Большая Морская ул., 67, Санкт-Петербург, 190000, Россия
e-mail: o2kon@mail.ru

Аннотация. Рассмотрены актуальные вопросы внедрения гуманитарных аспектов информационной безопасности в систему образования.

Ключевые слова: гуманитарные аспекты; социальные аспекты; этические аспекты; информационные технологии; информационная безопасность.

HUMANITARIAN ASPECTS OF INFORMATION SECURITY AND EDUCATION SYSTEM

Kononov Oleg, Kononova Olga
Saint Petersburg State University of Aerospace Instrumentation (SUAI)
67 Bolshaya Morskaya St, St. Petersburg, 190000, Russia
e-mail: o2kon@mail.ru

Abstract. Topical issues of introducing humanitarian aspects of information security into the education system are considered.

Keywords: humanitarian aspects; social aspects; ethical aspects; information technology; information security.

Широкое использование информационных технологий в современном обществе порождает проблемы, связанные с информационной безопасностью личности, общества, и государства, что обусловлено все большей «прозрачностью» и уязвимостью различных сторон жизни и деятельности людей для внешнего воздействия. На решение этих проблем нацелены социальные институты информационной безопасности, определяющие систему «правил игры» в обществе и активно формирующиеся в настоящее время. Это правовые, этические (моральные), корпоративные и технические нормы [1]. Все они затрагивают глобальные вопросы становления информационного общества.

Особое значение здесь имеют этические нормы. Во-первых, по той причине, что саморегуляция на основе нравственных норм является одним из естественных и эффективных способов защиты от антисоциального поведения участников информационного взаимодействия. Во-вторых, в перспективе, выработанные обществом нормы морали могут стать базой для формирования новых и совершенствования существующих правовых норм, обеспечиваемых силой государственного воздействия. Таким образом, обогатившись новым содержанием, адекватным новой реальности информационного общества, этические нормы могут стать настоящей гарантией обеспечения информационной безопасности личности и общества. Именно они определяют границы должного и возможного поведения.

Важность этого института информационной безопасности способствовала появлению отрасли знаний – «информационной этики». Этот термин стал употребляться учеными и специалистами по компьютерной этике и смежным дисциплинам с 2002 года. Информационная этика занимается изучением природы социального воздействия компьютерных технологий на общество, формулированием на этой основе моральных норм и проведением политики их внедрения в сознание разработчиков и пользователей компьютерных технологий. Информационная этика – обширная дисциплина, включающая в себя профессиональную этику, потребительскую этику и некоторые вопросы политики государства. Естественно, что первоначально она возникла как элемент профессиональных знаний и культуры в области информационных технологий.

На сегодняшний день до 90% всех технологий, влияющих на уровень профессиональной этики любой отрасли знаний, связаны с информацией, то есть с ее сбором, передачей, обработкой, способами хранения, техническими средствами и т.п. Это обстоятельство определяет повышенный уровень требований к специалистам – программистам, системным администраторам, и, конечно, к аналитикам, связанным с информационно-аналитическим обеспечением безопасности. Поэтому вопросы профессиональной этики в современном обществе носят информационный оттенок, причем эта тенденция будет сохраняться [1].

Первый кодекс компьютерной этики был разработан и принят в Институте инженеров электроники и электротехники (IEEE) в 1979 г. Принятие кодекса было продиктовано пониманием того, что инженеры, учёные и технологи результатами своей деятельности определяют качество и условия жизни всех людей в информационном обществе. Поэтому в преамбуле кодекса подчёркивается жизненно важная необходимость соблюдения всех норм этики при разработке и эксплуатации средств информационных технологий. Позднее были разработаны и приняты кодексы этики Ассоциацией разработчиков компьютерных технологий (ACM), Ассоциацией пользователей информационных технологий в США (ITAA), Ассоциацией сертифицированных компьютерных профессионалов (ICCP). В 1987 г. был разработан и принят кодекс компьютерной этики для преподавателей высшей и средней школ. Эти кодексы послужили основой для создания специальных курсов, которые сейчас преподаются во всех школах и большинстве университетов США. В обиход широко вошли понятия компьютерная этика, этика рекламодателей, нэтикет или этика поведения в сети Интернет.

На основе этических стандартов, используемых в перечисленных выше кодексах, Международная федерация по информационным технологиям (IEIP) рекомендовала принять кодексы компьютерной этики национальным организациям других стран с учётом местных культурных и этических традиций [1].

Во всех кодексах наряду с перечисленными заповедями и общечеловеческими моральными нормами, такими как честное исполнение своих обязанностей, профессиональная и социальная ответственность, повышение квалификации, расовое равноправие и т.п., содержатся нормы, основанные на соблюдении четырёх главных моральных принципов: privacy (тайна частной жизни), accuracy (точность), property (частная собственность) и accessibility (доступность).

Еще в 1996 году был разработан Торгово-промышленной палатой Российской Федерации «Национальный кодекс деятельности в области информатики и телекоммуникаций» [1].

Кодекс включал различные моральные нормы и был открыт для добровольного присоединения любого физического или юридического лица, действующего в области информатики или телекоммуникаций. Кодекс распространялся на все виды деятельности: производство, продажу, пользование средствами информатики и телекоммуникаций и определял, что эта деятельность должна быть законной, пристойной, честной и правдивой.

К сожалению, подобные кодексы часто существуют отдельно от пользователей компьютерной техники.

Значительный вклад в решение задачи внедрения в сознание участников информационного взаимодействия необходимости соблюдения норм компьютерной этики и привития навыков ее применения может и должна внести система образования, как социальный институт «производства социального человека»

[2]. Разъяснение и пропаганду этих норм необходимо проводить в лекционных курсах информатики, информационных технологий и других информационных дисциплин. Студенты должны понимать основные правовые, социальные и этические аспекты обеспечения информационной безопасности общества. Они должны сознавать свою личную роль в этом процессе. Студенты должны также развивать в себе способность задавать серьезные вопросы о социальном влиянии информатизации и оценивать предлагаемые ответы на них. Социально-личностное развитие обучаемых по различным специальностям, как техническим, так и сугубо гуманитарным, имеет чрезвычайно важное значение для обеспечения информационной безопасности общества. Об этом говорится и в одном из пунктов проекта «Этического кодекса для информационного общества» Юнеско [3], а именно:

– всем действующим лицам в информационном обществе следует стремиться поднять каждого участника на тот уровень, где он поймет, как работает система и как он может действовать коллективно со всеми, разделяя ответственность за успех системы в целом;

– открытое, интегрированное и межкультурное образование, совмещенное с обучением навыкам информационного и коммуникационного управления, является решающим; не следует ограничивать его получением технических знаний, но также включать осведомленность о моральных принципах и ценностях;

– людям следует быть готовыми к получению базовых навыков в области информационно-коммуникационных технологий и этики в информационном обществе.

Одним из элементов решения этой задачи может стать введение информационной этики в разряд дисциплин, изучаемых в высшей школе. Целями этой дисциплины должны стать: ознакомление студентов с историческими и философскими предпосылками этических традиций, связанных с социальными аспектами построения информационного общества; внедрение в сознание обучаемых необходимости следования на практике принципам, декларированным в кодексах информационной этики; развитие навыков информационной этики. Введение данной дисциплины позволит привлечь внимание к этическим требованиям глобальной информационной инфраструктуры, к которым относятся:

– вопросы языка и грамотности и разрыв между странами в области развития информационных технологий;

– риски, связанные с применением компьютерных систем, их оценка и управление ими;

– интеллектуальная собственность и обмен ею;

– этические и законодательные основы личной безопасности, конфиденциальность информации, гражданские свободы (свобода самовыражения) в киберпространстве.

В период пандемии, в связи с существенным ростом ликвидности данных, увеличения объемов работ в дистанционном формате необходимо особенно обратить внимание на изучение информационной этики.

Таким образом, необходимо еще раз подчеркнуть, что рассмотрение социальных и этических аспектов информационных технологий должно стать обязательной темой для разговора при проведении занятий по всем информационным дисциплинам, что будет способствовать формированию здорового современного информационного общества.

СПИСОК ЛИТЕРАТУРЫ

1. Кононов О.А., Кононова О.В. Социальные и этические аспекты обеспечения информационной безопасности // Проблемы управления, №1. М.: ИПУ РАН, 2009. – С.76-80
2. Кононов О.А., Кононова О.В. Образовательный процесс и ИКТ. XV Санкт-Петербургская международная конференция «Региональная информатика – 2016 (РИ-2016)»: материалы конференции. – СПб.: СПОИСУ, 2016. - С.368.
3. Этический кодекс для информационного общества. https://ifap.ru/ofdocs/unesco/etcodex.pdf (дата обращения 30.08.2021).

УДК 004.588

ОБОСНОВАНИЕ МЕТОДИКИ ЗАЩИТЫ ДИСТАНЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ, ПРИМЕНЯЕМЫХ ПРИ ПОДГОТОВКЕ СОТРУДНИКОВ ОВД

Локнов Алексей Игоревич, Коссаковская Маргарита Сергеевна
Санкт-Петербургский университет Министерства внутренних дел Российской Федерации
Летчика Пилютова ул., 1, Санкт-Петербург, 198206, Россия
e-mails: info_for_aleksey@mail.ru, margoshakuzya@mail.ru

Аннотация. Анализируются дистанционные технологии как методы, условия и факторы для более полной реализации личностного потенциала и проявления субъективных свойств в учебно-познавательной, информационно-поисковой, научно-исследовательской, учебно-профессиональной или контрольно-оценочной деятельности.

Ключевые слова: дистанционные технологии; образовательные технологии; дистанционное обучение; инновации.

JUSTIFICATION OF THE PROTECTION METHODS OF REMOTE EDUCATIONAL TECHNOLOGIES USED IN THE TRAINING OF ATS EMPLOYEES

Loknov Alexey, Kossakovskaya Margarita
St. Petersburg University of the Russian interior Ministry
1 Pilot Pilyutov St, St. Petersburg, 198206, Russia
e-mails: info_for_aleksey@mail.ru, margoshakuzya@mail.ru

Abstract. The article analyzes the remote technology as the methods, conditions and factors for a more complete realization of personal potential and the existence of subjective properties in the educational-cognitive, information retrieval, research, training or assessment activities.

Keywords: distance learning technology; educational technology; distance learning; innovation.

На сегодняшний день под дистанционными образовательными технологиями понимаются образовательные технологии, реализуемые в основном с применением средств информатизации и телекоммуникации, при опосредованном или не полностью опосредованном взаимодействии обучающегося и педагогического работника [1]. Как отмечают исследователи, использование дистанционных технологий оказывают «усиленное» влияние на процесс понимания и запоминания [2].

Впервые в России о возможности внедрения дистанционных технологий говорилось в тексте Объединенного проекта, утвержденного приказом Минобразования РФ от 16 июня 2000 № 1991 «О создании Объединенного проекта по разработке нормативно-правовых документов и отраслевых стандартов дистанционного обучения» специалистами была заложена определенная основа дистанционных образовательных технологий. Несмотря на то, что с 1991 года прошел уже не один десяток лет, до широкого внедрения дистанционного образования (особенно в системе ведомственного образования) нам еще далеко. И это несмотря на то, что активное применение дистанционных технологий может значительно повысить качество образовательного процесса, оптимизировать расходы на его обеспечение, а также повысить уровень овладения информацией, техникой.

Как показывает практика, успешность внедрения дистанционных технологий напрямую зависит от правильно выбранной программной платформы и информационной системы, реализующей процесс обучения. Как правило, реализация обучения происходит с помощью модулей и учебно-методической составляющей электронные учебно-методические комплексы, тестирование, консультирование на основе оффлайн-консультаций, организация дистанционных «он-лайн семинаров», электронная почта, электронный журнал и т.д. [3].

Необходимость учета специфики дистанционных технологий как компонента инновационного учебного процесса требует обращения к основам педагогического и организационного проектирования. При построении структурно-функциональной модели проектирования учебного процесса необходимо использование дистанционных технологий, направленных на осуществление нормативной функции, учитывающей особенности направления профессиональной подготовки. Здесь предполагается:

– изучение и анализ нормативно-правовой основы, опыта организации, условий и факторов, влияющих на особенности и эффективность организации учебного процесса с использованием дистанционных технологий;

– адаптацию учебных планов к использованию дистанционных технологий при различных формах обучения;

– разработку учебно-методического обеспечения с учетом специфики учебного процесса;

– подбор методов, средств, форм организации учебной работы, форм контроля учебного процесса с учетом специфики дистанционных технологий;

– реализацию учебного процесса;

– оценку эффективности учебного процесса.

Одной из попыток внедрения дистанционных технологий в ведомственном образовании служила единая информационная телекоммуникационная система органов внутренних дел (ЕИКТС), которая предназначена для осуществления широкомасштабного многовидового обмена информацией среди подразделений МВД России [4].

Основной задачей данной системы являлась организация дистанционного обучения сотрудников органов внутренних дел без отрыва от выполнения ими своих служебных обязанностей.

Анализ практики разработки и внедрения дистанционных технологий в образовательных организациях МВД России показывает, что в отдельных случаях в недостаточной степени используется потенциал дистанционных образовательных технологий, многие преподаватели оказались неготовыми к использованию дистанционных образовательных технологий в учебном процессе с обучающимися.

Таким образом, достоинства дистанционных технологий очевидны: прежде всего, это неограниченная масштабность, формирование единого образовательного пространства, обеспечение подготовки высококвалифицированных сотрудников органов внутренних дел; определение основ профессиональной переподготовки на основе дистанционных образовательных программ; создание возможностей для получения образования на протяжении всей жизни; формирование социальной мобильности, поисковой грамотности, воспитание в духе гражданственности.

СПИСОК ЛИТЕРАТУРЫ

1. Полат Е.С. Теория и практика дистанционного обучения. Учеб. пособие для студ. высш. пед. учеб. завед. – Москва, 2004. – С. 12.
2. Деменченок О.Г., Ширяева Н.К., Демаков В.И. Проведение учебных занятий с применением мультимедийной техники. – Иркутск, 2010. – С. 4.
3. Федеральный закон Российской Федерации от 29 декабря 2012 г. № 273 – ФЗ «Об образовании в Российской Федерации» форме (Электронный ресурс) // Режим доступа: http://base.consultant.ru (Дата обращения: 25.07.2021 г.).
4. Стратегия развития информационного общества в России (Электронный ресурс) // Режим доступа: http://base.consultant.ru (Дата обращения: 25.07.2021 г.).

УДК 004.7

ИНТЕЛЛЕКТУАЛЬНАЯ АВТОМАТИЗАЦИЯ РАЗРАБОТКИ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Птицына Лариса Константиновна[1], Птицын Никита Алексеевич[1], Птицын Алексей Владимирович[2]
[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
р. Мойки наб., 61, Санкт-Петербург, 191186, Россия
[2] Университет ИТМО
Кронверкский пр., 49, Санкт-Петербург, 197101, Россия
e-mails: ptitsina_lk@inbox.ru, nikita_pti@inbox.ru, pticin@inbox.ru

Аннотация. Приведены ключевые основания для актуализации введения средств интеллектуальной автоматизации в процесс разработки образовательных программ по информационной безопасности. Показана востребованность автоматической систематизации и представления в глобальном информационном пространстве знаний об образовательных программах по информационной безопасности. Рассмотрены факторы для обоснования выбора инструментария онтологического моделирования при разработке образовательных программ по информационной безопасности. Определены альтернативы выбора среды для онтологического моделирования. Описан прием сравнительного анализа онтологий рабочих учебных планов. Раскрыты достоинства онтологического моделирования рабочих учебных планов образовательных программ при выборе приоритетных направлений их развития.

Ключевые слова: интеллектуальная автоматизация; сопровождение; систематизация; онтология; представление знаний; инструментарий; анализ знаний.

ONTOLOGICAL APPROACH TO SUPPORTING THE LIFE CYCLE OF EDUCATIONAL PROGRAMS ON INFORMATION SECURITY

Ptitsyna Larisa[1], Ptitsyn Nikita[1], Ptitsyn Alexey[2]
[1] The Bonch-Bruevich Saint Petersburg State University of Telecommunications
61 Moika Emb, St. Petersburg, 191186, Russia
[2] ITMO University
49 Kronverksky Av, St. Petersburg, 197101, Russia
e-mails: ptitsina_lk@inbox.ru, nikita_pti@inbox.ru, pticin@inbox.ru

Abstract. The reasons for updating the introduction of intelligent automation tools into the process of supporting the life cycle of educational programs on information security are considered. The demand for automatic systematization and presentation in the global information space of knowledge about educational programs on information security is shown. The grounds for choosing the tools of the ontological approach to support the life cycle of educational programs on information security are given. The alternatives of choosing the environment for the implementation of the ontological approach are presented. The advantages of ontological modeling of working educational programs in environments for the implementation of the ontological approach are disclosed.

Keywords: intelligent automation; accompaniment; systematization; ontology; knowledge representation; tools; knowledge analysis.

В результате стремительного развития достижений гипертехнологий IT-индустрии цифровая трансформация во всех сферах жизнедеятельности социума признается одной из основных движущих сил развития национальной экономики и необходимым условием для обеспечения её безопасности.

Подготовка кадров по информационной безопасности является одним из основных направлений развития национальной цифровой экономики. Наблюдаемое разрастание масштабов и степени использования информационной инфраструктуры в жизнедеятельности представителей социума и профессиональной деятельности субъектов экономики в условиях пандемии повышает значимость этого направления. Подготовки кадров по информационной безопасности требует реализации технологического сопровождения, соответствующего современному уровню развития знаний в этой предметной области и требованиям образовательных и профессиональных стандартов.

Подготовка технологического сопровождения относится к трудоемким и ответственным крупногранулярным процессам, степень автоматизации которых непрерывно повышается. Однако степень интеллектуализации реализуемой автоматизации на этапах разработки концепции образовательной программы и рабочего учебного плана не согласуется с современными достижениями в развитии искусственного интеллекта. Рассмотренные причины актуализируют введение средств интеллектуальной автоматизации в процесс сопровождения жизненного цикла образовательных программ по информационной безопасности.

Используемые оболочки для разработки и представления рабочих учебных планов не обладают современными моделями приобретения знаний, предусматривающих возможность автоматизации при систематизации, представлении и обработке знаний, которые необходимы для выбора приоритетных направлений их проектирования.

Для снижения трудоемкости реализации технологического сопровождения, соответствующего современному уровню развития знаний в этой предметной области и требованиям образовательных и

профессиональных стандартов, необходимы автоматическая систематизация, представление в глобальном информационном пространстве знаний об образовательных программах по информационной безопасности и автоматическая обработка этих знаний. Для разрешения выявленной проблемной ситуации предлагается онтологический подход к сопровождению технологического сопровождения образовательных программ по информационной безопасности, гибкий по отношению к расширению знаний в соответствующей предметной области [1-4].

О перспективности предлагаемого подхода свидетельствует успешный опыт интеллектуализации систематизации профессиональных стандартов для научно-образовательной сферы, полученный при построении, представлении и обработке соответствующих онтологических моделей [5], а также при выполнении проектов по представлению цифрового следа в процессе персонализации подготовки кадров для цифровой экономики, описанных в [6-8].

При введении онтологического подхода в методологию сопровождения жизненного цикла образовательных программ по информационной безопасности предоставляются разнообразные альтернативы в выборе инструментальных сред онтологического моделирования. Альтернативы характеризуются представительным множеством отличительных признаков существующих систем их классификации. Отличительные признаки классификации могут быть задействованы для определения критериев выбора инструментальной среды онтологического моделирования.

В качестве отличительных признаков выступают требования к платформам информатизации, элементы спецификаций функциональных возможностей, элементы различий в компонентах поддерживаемых методологий онтологического проектирования, характеристики формализмов, языков и форматов. При обширном многообразии отличительных признаков открываются возможности реализации многокритериального выбора инструментальной среды онтологического моделирования на основе использования формальных методов сравнительного анализа и оптимизации.

Введение инструментальной среды онтологического моделирования в сопровождение жизненного цикла образовательных программ по информационной безопасности расширяет степень интеллектуализации автоматизированных процессов подготовки необходимых учебно-методических комплексов и снижает степень субъективизма в оценивании их состоятельности и уровня развития.

Научная новизна представляемого обновления методологии сопровождения технологического сопровождения образовательных программ по информационной защищенности состоит в сквозном объединении интеллектуальных автоматизированных процессов создания, представления, анализа и критериального выбора компонентов образовательных программ по информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Птицына Л. К., Птицын А. В. Расширение знаний о защите информации в образовательных программах магистратуры // Новые информационные технологии в образовании и науке: материалы XII междунар. науч.-практ. конф., Екатеринбург, 25 февраля – 1 марта 2019 г.: // ФГАОУ ВО «Рос. гос. проф.-пед. ун-т». Екатеринбург, 2019. С. 629-635.
2. Птицына Л. К., Птицын А. В. Технологический базис формирования кадрового обеспечения цифровой экономики // Новые информационные технологии в образовании: материалы XI междунар. науч.-практ. конф., Екатеринбург, 27 февраля – 3 марта 2018 г.: // ФГ АОУ ВО «Рос. гос. проф.-пед. ун-т». Екатеринбург, 2018. С. 583-589.
3. Птицына Л. К., Маргаритова Я. С. Концепция анализа влияния методов и средств извлечения знаний на безопасность персональных данных // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII Международная научно-техническая и научно-методическая конференция: сб. науч. ст. в 3 т. / Под ред. С. В. Бачевского, сост. А. Г. Владыко, Е. А. Аникевич. СПб. : СПбГУТ, 2018. Т. 2. С. 487-491.
4. Птицына Л. К., Тарабаров А. В. Анализ методов комплексирования средств защиты информации // Актуальные проблемы инфотелекоммуникаций в науке и образовании. VII 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, 2018. Т. 2. С. 541-544.
5. Птицына Л. К., Птицын А. В. Интеллектуализация систематизации профессиональных стандартов для научно-образовательной сферы // Наука. Информатизация. Технологии. Образование : материалы XIV международной научно-практической конференции «Новые информационные технологии в образовании и науке НИТО-2021», г. Екатеринбург, 1–5 марта 2021 г. // ФГАОУ ВО «Российский государственный профессионально-педагогический университет». Екатеринбург, 2021. 576 с. (С. 151-157).
6. Птицына Л. К., Птицын А. В., Птицын Н. А. Индивидуализация и персонализация процессов формирования компетенций при подготовке кадров для сферы ИТ-технологий // Современное образование: содержание, технологии, качество. Материалы XXVI международной научно-методической конференции. СПб.: Изд-во СПбГЭТУ. 2020. С. 466-468.
7. Птицына Л. К., Птицын Н. А., Птицын А. В. Интеллектуализация определения цифрового следа при персонализации подготовки кадров для цифровой экономики // Наука. Информатизация. Технологии. Образование : материалы XIV международной научно-практической конференции «Новые информационные технологии в образовании и науке НИТО-2021», г. Екатеринбург, 1–5 марта 2021 г. // ФГАОУ ВО «Российский государственный профессионально-педагогический университет». Екатеринбург, 2021. С. 144-151.
8. Птицына Л. К., Птицын Н. А., Птицын А. В. Онтологическое представление и обработка знаний об индивидуализации и персонализации образовательных траекторий // Современное образование: содержание, технологии, качество. Материалы XXVII международной научно-методической конференции. СПб.: Изд-во СПбГЭТУ. 2021. С. 391-393.

УДК 004.89

МЕТОД РАСПОЗНАВАНИЯ ИНФОРМАЦИОННЫХ УГРОЗ С ИСПОЛЬЗОВАНИЕМ РЕКУРРЕНТНОЙ НЕЙРОННОЙ СЕТИ

Фаткиева Роза Равильевна, Пузако Иван Александрович
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
Профессора Попова ул., 5, Санкт-Петербург, 197376, Россия
e-mail: rikki2@yandex.ru

Аннотация. Рассматриваются методы и средства по нахождению потенциально опасного содержания в текстовой информации. В результате работы были исследованы существующие подходы к анализу текстовой информации, разработана модель обнаружения информационных угроз на базе рекуррентной нейронной сети.

Ключевые слова: обработка текстов; рекуррентные нейронные сети; распознавание террористических угроз.

RECOGNITION OF INFORMATION THREATS USING RECURRENT NEWRAL NETWORK

Fatkieva Roza, Puzako Ivan
Saint Petersburg State Electrotechnical University
5 Professor Popov St, St. Petersburg, 197376, Russia
e-mail: rikki2@yandex.ru

Abstract. Methods for finding potentially dangerous content in text information. As a result of the work, the existing approaches to the analysis of text information were investigated, and a model for detecting information threats based on a recurrent neural network was developed.

Keywords: word processing; recurrent neural networks; recognition of terrorist threats.

Введение. Использование современных технологии способствует все более интенсивному использованию Интернета и вовлечению широких слоев населения в процессы обработки информации и передачи знаний. Однако этот же факт способствует распространению терроризма, одной из серьезных угроз современной цивилизации, который влияет на качество жизни людей во всем мире. Целью терроризма является создание нестабильности, через использования основных отрицательных эмоций: страх, тревога и неуверенность в завтрашнем дне. Число преступлений террористического характера в России с начала 2020 года выросло в сравнении с аналогичным периодом предыдущего года более чем на треть. По данным МВД с января по сентябрь 2020 зафиксировано 1851 преступления террористического характера (рост на 33,9% по сравнению с предыдущим годом), 651 преступлений экстремистской направленности (рост на 43,3 %) [1].

При этом формирование «общественного мнения» участниками преступлений чаще всего осуществляется в виде электронных текстовых сообщений или записей в социальных сетях. С увеличением использования сайтов социальных сетей, таких как Twitter, Facebook, Instagram и др. растет возможность влияния на формирования мнений, чувств, эмоций и намерений, которые отражают их принадлежность или склонность к какой-либо организации, отношение к каким-либо политическим событиям. Поэтому социальные сети являются уязвимыми и доступными платформами для укрепления и создания террористических групп, пропаганды, сбора средств и распространение их влияния на общественные настроения. С другой стороны мнения, высказываемые на таких сайтах, дают важную информацию о деятельности и поведении онлайн-пользователей. Обнаружение экстремистского контента необходимо для анализа настроений пользователей по отношению к какой-либо экстремистской группе и предотвращения связанных с ними противоправных действий. Это также полезно для профилактики, с точки зрения классификации экстремистской принадлежности пользователя, путем фильтрации его сообщений перед их дальнейшей передачей. В связи с этим встает задача поиска методов автоматического анализа большого потока текстовых данных на естественном языке, с целью выявления несанкционированного контента. Однако сообщения на естественном языке зачастую является неструктурированными и сложными для понимания, что создает проблему в правильной их обработке автоматическими методами. В настоящее время нейронные сети являются наиболее мощным инструментом для обработки текстовых сообщений. Их популярность во многом вызвана их способностью находить сложные скрытые зависимости в данных, хотя это и требуют большого объёма данных для обучения. Существующие исследования основаны на классических методах машинного обучения или используют классические схемы представления признаков, за которыми следует классификатор. В исследовании [2] проводится сравнение полносвязных нейросетей с рекуррентными нейросетями в задаче определения эмоциональной окраски текстов. Показано, что рекуррентные архитектуры (LSTM и GRU) демонстрируют более высокий результат поиска за счет возможности обрабатывать информацию о последовательности слов в тексте, в отличие от полносвязных сетей, которые учитывают только вхождения тех или иных слов. В работе [3] при сравнении подходов машинного обучения к задаче определения эмоциональной окраски текстов участвовали алгоритмы классического машинного обучения: KNN, SVM, случайные леса, логистическая регрессия, нейросетевые подходы: RNN, CNN, LSTM, GRU, LSTM+Attention, с разными способами векторного представления слов. Показано, что наилучший результат показала комбинация архитектур LSTM+AM, за счет учета внутренних состояний рекуррентных слоев, которые влияют более правильный учет последовательности. Представленная в исследовании [4] модель Bi-LSTM+CRF, решает задачу нахождения именованных сущностей в документе. К рекуррентной архитектуре добавлено условное случайное поле для минимизации ошибок выставления меток на словах за счёт учета проставленных меток на соседних словах данного слова. В [5] показан стандартный подход для предобработки текстовых данных–векторизации текстов, отбор наиболее значимых признаков с использованием статистических методов. Проведенное сравнение множества классических алгоритмов машинного обучения показало, что наилучший результат достигается при использовании линейно разделимой выборки SVM, так как этот алгоритм хорошо подходит для задач с большой размерностью данных и является интерпретируемым. В работе [6] представлен способ классификации закреплённых сообщений в Twitter. В качестве моделей для принятия решений использованы kNN и SVM.

Показан способ взвешивания значимых слов с помощью алгоритма поиска экстремума унимодальных функций ternary search. Наилучшие результаты получены с помощью алгоритма SVM так как он является более сложным, что позволяет учитывать больше информации при обучении. В статье [7] анализируются онлайн-программы для анализа тональности текстов, которые могут давать положительное, отрицательное или нейтральное мнение о тексте. В [8] описан подход к задаче идентификации языка по входному тексту. Решение такой задачи применительно к коротким текстам остается сложной задачей обработки естественного языка. Разработанный метод сочетает векторное представление слов и рекуррентную архитектуру LSTM. Экспериментальная оценка на открытых наборах данных показала, что предложенный метод имеет высокую точность: около 100% на длинных текстах и около 80% на коротких из-за меньшего количества информации, извлекаемого из предложения. Однако в представленных работах [1-9] отсутствуют методы лексического анализа текстов, на основе методов глубокого обучения, которые показывают эффективность в распознавании текстовых сообщений двоякой направленности.

Метод распознавания информационных угроз с использованием рекуррентной нейронной сети. На практике основными вариантами обработки текстовых данных являются свёрточные и рекуррентные архитектуры нейронных сетей. При построении метода в качестве рекуррентного блока использовалась ячейка долгой краткосрочной памяти LSTM (Long short-term memory), которая имеет более сложную архитектуру, чем простая рекуррентная сеть. Для выявления текста, с связанного с терроризмом и экстремизмом задача сформулирована как бинарная классификация, с выставлением метки вероятности целевого класса на тексте, состоящая из следующих шагов:

Шаг.1. *Первичная обработка текста* необходима поскольку рекуррентные архитектуры обрабатывают тексты последовательно, считывая слово за словом, поэтому исходные тексты должны быть разбиты на слова.

Шаг.2 *Получение очищенного текста* (с удалением лишних символов и знаков, не имеющих смысловую нагрузку (предлоги, артикли)) и поиск начальной словарной формы каждого слова в некотором словаре.

Шаг 3. *Кодирование полученного очищенного текста* с некоторым случайным вектором длины 100. В результате обучения каждый полученный вектор должен будет представлять смысл и частный контекст слова в некотором латентном пространстве. В результате преобразования два схожих по смыслу слова смогут иметь меньшую дистанцию в пространстве, а различные по смыслу слова – большую.

Шаг 4. *Использование реккурентного блока нейронной сети (LSTM).* Рекуррентный слой описывает следующий алгоритмом работы:

4.1. Получить и обработать очередной элемент входной последовательности, заранее закодированный в некоторый вектор.

4.2. Вычислить новое значение ячейки памяти, исходя из её прошлого значения и входного элемента.

4.3. Вычислить выходное состояние, которое получается с учетом элемента входной последовательности, скрытого состояния из предыдущего шага и состояние ячейки памяти в сети, которая может хранить информацию о долгосрочных зависимостях между словами.

Получение векторных репрезентаций для всех уникальных слов позволяет каждый текст представить в виде некоторой матрицы, которая последовательно считывается по столбцам нейронной сетью. Каждое слово обрабатывается, учитывая переданное ранее скрытое состояние сети, полученное в результате обработки предыдущей последовательности. В конце прохода нейронная сеть возвращает закодированную в виде вектора размерностью 100 информацию о прочитанном тексте и подает ее на полносвязный слой с выходной размерностью 1 и сигмоидальной функцией активации, в результате чего на выходе модели получается вероятность (вещественное число от 0 до 1) отнесения текста к террористическому, которая может быть интерпретирована как уверенность модели в предсказании.

Шаг 5. *Оценка вероятности принадлежности текста к классу*. Для оценки классификации текста моделью с предсказанной вероятностью используется метрика качества «кривая точность-полнота» (precision-recall curve). Она больше подходит, чем метрика доли верных ответов с учетом установленного порогового значения, так как в оценочной выборке террористических текстов намного меньше, чем тексов обычного содержания. Для выставления окончательного бинарного ответа из вещественного определяется порог, после которого можно считать ответ модели положительным. Однако для общей оценки модели с вероятностным ответом целесообразно использовать не одну точку с конкретным значением метрики, а множество точек, образующих кривую. Это дает возможность оценить работу модели в общем и выбрать оптимальный порог для положительного срабатывания модели. Также для подтверждения состоятельности модели возможно использовать кривую со случайным вероятностным предсказанием, при этом, в случае достаточно большого расхождения между оценками можно делать вывод о том, что нейросеть смогла подстроиться под реальную зависимость между входными текстами и целевыми метками терроризма.

Для практического применения разработанного метода была предложена архитектура рекуррентной нейронной сети с использованием библиотеки глубокого обучения pytorch языка python3, которая позволила создать класс моделей, с множеством слоев (слой векторных репрезентаций слов; слой прореживания; рекуррентный блок LSTM; полносвязный слой нейросети; слой активации сигмоидальной функции). Обучение модели осуществлялось в течение 30 запусков на всем наборе данных с помощью алгоритма стохастического градиентного спуска «Adam» [10] и выборки текстов, оставленных в протеррористических сообществах в соцсети

Twitter при атаке на Париж в 2015 году [11]. Запуск модели на отложенных тестовых данных показал возможность определения текстов террористической направленности с 95 % вероятностью.

Разработанный метод, реализующий запуск обученной модели распознавания террористических текстов может быть использован для поиска текстов со схожей тематикой среди больших коллекций документов внутри социальной сети или комментариев пользователей на различных каналах. Дальнейшее направление исследования связано с улучшением алгоритма сбора и анализа большего количества данных, полученных и сети Интернет, покрывающих заданное количество тем, связанных с экстремистской или террористической тематикой.

СПИСОК ЛИТЕРАТУРЫ

1. Информационное агентство Regum. В России в 2020 году участились террористические преступления — МВД. // [Электронный ресурс]. URL: https://regnum.ru/news/polit/3095681.html (дата обращения: 12.10.2021).
2. Abbas, S.K., George, L.E. “The performance differences between using recurrent neural networks and feedforward neural network in sentiment analysis problem”; DOI: 10.24996/ijs.2020.61.6.31.
3. Onan, A A. “Mining opinions from instructor evaluation reviews: A deep learning approach”; DOI: 10.1002/cae.22179.
4. Viani, N., Miller, T.A., Napolitano, C., Priori, S.G., Savova, G.K., Bellazzi, R., Sacchi, L. “Supervised methods to extract clinical events from cardiology reports in Italian”; DOI: 10.1016/j.jbi.2019.103219.
5. Ghulam Mujtaba1, Liyana Shuib, Ram Gopal Raj, Roshan Gunalan “Detection of suspicious terrorist emails using text classification”; DOI: 10.22452/mjcs.vol31no4.3.
6. Aditi Sarker, Partha Chakraborty, S. M. Shaheen Sha, Mahmuda Khatun, Md. Rakib Hasan, Kawshik Banerjee “Improvised Technique for Analyzing Data and Detecting Terrorist Attack Using Machine Learning Approach Based on Twitter Data”; DOI: 10.4236/jcc.2020.87005.
7. Mihaljević, J. “Analysis and creation of free sentiment analysis programs”; DOI: 10.22572/mi.25.1.4.
8. Oro, E., Ruffolo, M., Sheikhalishahi, M. “Language identification of similar languages using recurrent neural networks”; DOI: 10.5220/0006678606350640.
9. Метод стохастического градиентного спуска с автоматической адаптацией скорости обучения. // [Электронный ресурс]. URL: https://towardsdatascience.com/adam-latest-trends-in-deep-learning-optimization-6be9a291375c (дата обращения: 12.10.2021).
10. Источник данных для обучения модели. // [Электронный ресурс]. URL: https://www.kaggle.com/fifthtribe/how-isis-uses-twitter (дата обращения: 12.10.2021).

МОЛОДЕЖНАЯ НАУЧНАЯ ШКОЛА «БЕЗОПАСНЫЕ ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

УДК 004.056

ИССЛЕДОВАНИЕ МЕТОДИК ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ WEB-ПРИЛОЖЕНИЙ IAST И SAST

Акилов Марк Валерьевич, Ковцур Максим Михайлович, Несудимов Евгений Юрьевич, Потемкин Павел Андреевич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: markakilov@yandex.ru, maxkovzur@mail.ru, enesudimov@gmail.com, potiomkinpa98@gmail.com

Аннотация. В связи с использованием автоматизации и стандартизации процессов для поддержания качества и стабильности разрабатываемого ПО, возникла проблема анализа безопасности, из-за сильного замедления выпуска программного продукта на рынок. Для решения данного вопроса необходима интеграция проверки безопасности в современные и автоматизированные процессы DevOps – DevSecOps. Важнейшей концепцией DevSecOps является внедрение средств автоматизированного тестирования безопасности. Целью данной работы является исследование IAST и SAST, их преимуществ и недостатков, а также возможностей совместного применения.

Ключевые слова: SAST; IAST; DAST; DevOps; тестирование; безопасность; веб-приложение; код; инструмент; разработка; уязвимость.

RESEARCH METHODS FOR DETECTING VULNERABILITIES OF WEB-APPLICATIONS IAST AND SAST

Akilov Mark, Kovzur Maxim, Nesudimov Evgeny, Potiomkin Pavel

The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: markakilov@yandex.ru, maxkovzur@mail.ru, enesudimov@gmail.com, potiomkinpa98@gmail.com

Abstract. In connection with the use of automation and standardization of processes to maintain the quality and stability of the developed software, the problem of security analysis arose, due to a strong slowdown in the release of a software product to the market. To address this issue, it is necessary to integrate security auditing into modern and automated DevOps processes - DevSecOps. The most important DevSecOps concept is the implementation of automated security testing tools. The aim of this work is to study IAST and SAST, their advantages and disadvantages, as well as the possibilities of their joint application.

Keywords: SAST; IAST; DAST; DevOps; testing; security; web application; code; tool; development; vulnerability.

Использование веб-приложений возросло во многих типах организаций в последнее врем. Эти приложения должны постоянно развиваться в кратчайшие сроки, чтобы противостоять конкурентам. Это увеличивает риск написания небезопасного кода.

Для обеспечения должного уровеня проверки безопасности приложений были разработаны инструменты тестирования безопасности приложений (*AST*) [4]. Выделяют статический (*SAST*), динамический (*DAST*) и интерактивный (*IAST*) виды тестирования безопасности приложений.

SAST (*Static Application Security Testing*) - производит тестирование «белого ящика». Данный вид тестирования анализирует как исходный код, так и исполняемый файл, в зависимости от обстоятельств.

DAST (*Dynamic Application Security Testing*) - это тестирование, которое позволяет анализировать запущенное приложение, атакующее все внешние исходные входные данные веб-приложения.

IAST (*Interactive Application Security Testing*) - данный вид тестирования позволяет анализировать код, но, в отличие от *SAST*, делает это в режиме реального времени и в интерактивном режиме, аналогичном инструментам *DAST*.

Несколько инструментов одного и того же типа могут быть объединены для достижения лучшей производительности с точки зрения истинных и ложных срабатываний [2]. Таким образом, целью данной работы является исследование IAST и SAST, их преимуществ и недостатков, а также возможностей совместного применения.

Для того чтобы изучить эффективность каждого инструмента по отдельности и в совместном применении необходимо определить ряд наиболее распространенных и опасных уязвимостей безопасности веб-приложений. Такой список уже был составлен открытым проектом по обеспечению безопасности веб-приложений (OWASP). Список OWASP Top Ten объединяет наиболее важные категории уязвимостей.

По версии OWASP от 2017 года существуют следующие десять видов уязвимостей веб приложений: инъекции, уязвимости аутентификации, раскрытие конфиденциальных данных, внешние объекты XML (XXE), нарушенный контроль доступа, неверная конфигурация безопасности, межсайтовый скриптинг (XSS), небезопасная десериализация, использование компонентов с известными уязвимостями, недостаточное ведение журнала и мониторинг.

Исходя из результатов ряда исследований, наиболее адекватным тестовым стендом для использования инструментов SAST, DAST и IAST является проект OWASP benchmark project.

Это веб-приложение на языке Java, которое содержит тестовые случаи для обнаружения истинных и ложных срабатываний. Из всех видов уязвимостей, представленных на тестовом стенде, случайным образом были отобраны 320 тестовых случаев и распределены поровну между собой. Из них половина случаев ложного срабатывания, а половина - истинно положительные.

Инструменты SAST и IAST выбираются в соответствии с платформой Java 2, Enterprise Edition (J2EE), наиболее используемой технологией в разработке веб-приложений, языком программирования, используемым J2EE, является Java, один из помеченных как более безопасный.

С учетом сравнений и анализа доступности коммерческих и открытых исходных инструментов были выбраны следующие инструменты:

FindSecurityBugs - SAST инструмент с открытым исходным кодом.

Contrast Community Edition - бесплатная версия коммерческого инструмента IAST от Contrast Security.

Для определения эффективности работы инструментов SAST и IAST исследование было проведено относительно следующих метрик:

Истинно положительная оценка (ИПО) - отношение обнаруженных уязвимостей к числу реально существующих уязвимостей в коде:

Ложно положительная оценка (ЛПО) - Соотношение ложных тревог для уязвимостей, которые на самом деле не существуют в коде:

Для исследования эффективности определения уязвимостей при совместной работе инструментов SAST и IAST необходимо понимать в каких случаях система из двух инструментов возвращает истинно положительный, истинно отрицательный, ложноположительный или ложноотрицательный результат.

По результатам исследования нами были составлены графики зависимостей ИПО и ЛПО от каждого вида уязвимостей для инструмента SAST, инструмента IAST и для их совместного применения.

СПИСОК ЛИТЕРАТУРЫ

1. Al-Amin, S.; Ajmeri, N.; Du, H.; Berglund, E.Z.; Singh, M.P. Toward effective adoption of secure software development practices. Simul. Model. Pr. Theory 2018, 85, p. 33–46.
2. Antunes, N.; Vieira, M. Assessing and Comparing Vulnerability Detection Tools for Web Services: Benchmarking Approach and Examples. IEEE Trans. Serv. Comput. 2015; pp. 269–283.
3. Antunes, N.; Vieira, M. Assessing and Comparing Vulnerability Detection Tools for Web Services: Benchmarking Approach and Examples. IEEE Trans. Serv. Comput. 2015$ pp. 269–283.
4. Felderer, M.; Büchler, M.; Johns, M.; Brucker, A.D.; Breu, R.; Pretschner, A. Security Testing: A Survey. In Advances in Computers; Elsevier: Cambridge, MA, USA, 2016; pp. 18-19.
5. Goseva-Popstojanova, K.; Perhinschi, A. On the capability of static code analysis to detect security vulnerabilities. Inf. Softw. Technol. 2015, 68, pp. 18–33.

УДК 004.056

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ КЛЮЧЕВЫХ АСПЕКТОВ ФОРМИРОВАНИЯ РАСПРЕДЕЛЕННОГО РЕЕСТРА

Акилов Марк Валерьевич, Кушнир Дмитрий Викторович, Баталов Антон Сергеевич, Ковцур Максим Михайлович

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails markakilov@yandex.ru, dmitry.kushnir@gmail.com, lein.mydream@gmail.com, maxkovzur@mail.ru

Аннотация. С ростом уровня интеграции блокчейнов в повседневную жизнь общества растет потребность в моделировании подобных цепей и затрат ресурсов. В данной статье рассматривается алгоритм работы блокчейн на примере bitcoin. Приводится результат работы созданной, в ходе анализа, программы для эмуляции работы блокчейн.

Ключевые слова: блокчейн; bitcoin; распределенные системы хранения; децентрализованные системы хранения.

RESEARCH OF PECULIARITIES OF BLOCKCHAIN TECHNOLOGY OPERATION

Akilov Mark, Kushnir Dmitry, Batalov Anton, Kovzur Maxim
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails markakilov@yandex.ru, dmitry.kushnir@gmail.com, lein.mydream@gmail.com, maxkovzur@mail.ru

Abstract. With the increase in the level of integration of blockchains into the daily life of society, there is an increasing need for modeling such chains and resource costs. This article examines the blockchain algorithm using the example of bitcoin. The result of the work of the program created in the course of the analysis for emulating the work of the blockchain is given.

Keywords: blockchain; bitcoin; distributed storage systems; decentralized storage systems.

Изначально в идею блокчейна легло стремление сформировать такие альтернативные технологии, которые исключили бы банки как посредников, исключили бы мошенничество и риски, а нормы программного кода заменили бы правовые нормы [1, 2].

В настоящее время появились и другие формы эффективного использования технологии блокчейна: сфера финансовых услуг, платежные сервисы, в государственном секторе – это госуслуги, реестры недвижимости, электронное голосование. Есть примеры применения блокчейна в транспортной логистике, здравоохранении, управлении интеллектуальной собственностью [3-5].

Блокчейн (англ. block chain — цепь из блоков) – это технология децентрализованного распределенного хранения данных о транзакциях, совершенных участниками системы. Состоит из последовательно соединенных блоков. В заголовок каждого последующего блока включается хэш предыдущего. Таким образом составляется неразрывная цепь. Разорвать или изменить ее возможно, только если пересчитать все блоки и собрать цепочку заново с точки разрыва. Для этого необходимо использовать вычислительные ресурсы, эквивалентные или большие, чем те, что были затрачены при сборке оригинальной цепи.

Ключевые особенности блокчейна:

Децентрализация процессов хранения и обработки информации.

В блокчейне вся записанная информация хранится у каждого участника сети в полном объеме. Эта особенность позволяет создавать географически распределенные сети без дорогостоящих дата-центров, централизованных систем хранения данных и резервного копирования, а также обеспечивать локальный доступ к данным для каждого узла сети.

Доказуемая неизменяемость данных. Блокчейн, являясь неразрывной последовательностью криптографически связанных блоков, решает проблему нелегитимного изменения данных, когда в любой момент времени имеется возможность проверить всю последовательность добавления информации, таким образом исключая возможность внесения любых изменений в отдельные участки цепи без ее полной перестройки.

Прозрачность операций. Блокчейн является одноранговой сетью, где все участники являются равноправными. Все участники блокчейна имея данные о всех транзакциях могут проверить историю своих контрагентов при выполнении операций.

Безвозвратность транзакций. Данное свойство вытекает из всего вышеизложенного, так при гарантии хранения и неизменности информации безвозвратность транзакций является обратной стороной этих свойств.

Возможность анонимизации участников. Каждый адрес в блокчейне является уникальным идентификатором, состоящий из обезличенного набора символов, и не содержит никакой информации, позволяющей провести взаимно однозначное соответствие кошелька и его владельца, а какой-либо анализ затруднителен при условии большого количества транзакций, к примеру, в повседневной жизни.

Отсутствие необходимости в доверии. Данная особенность позволяет проводить транзакции при условии, что они корректны и подтверждено право обладания соответствующим исходящим адресом. В транзакциях используется механизм децентрализованного посредничества(escrow).

Поддержание работы сети самими участниками. Каждый пользователь блокчейна может создать собственный узел (в публичных блокчейнах) и стать владельцем созданных им токенов внутри цепи. Все это накладывает на них и определенный уровень ответственности по поддержанию работы самого блокчейна, так как в публичных блокчейнах нет никакой организации, которая будет делать это вместо них.

К вопросу о доверии в блокчейне. Вопрос доверия является одним из основополагающих в технологии блокчейна. Доверие достигается с помощью аналога онлайн голосования, постоянно проводимого всеми узлами сети с децентрализованным управлением. В разных блокчейнах это голосование имеет разные формы, но во всех публичных блокчейнах для формирования единственно правильной последовательности блоков необходимо решение большинства или достижение так называемого консенсуса.

Функционирование блокчейна невозможно без консенсуса, то есть процесса согласования вносимых изменений [1]. Механизм консенсуса в системе также помогает предотвратить определенные виды атак. Теоретически злоумышленник может нарушить консенсус, контролируя 51% сети. Механизмы консенсуса разработаны, чтобы сделать эту «атаку 51%» невозможной.

Существует множество алгоритмов консенсуса, перечислим некоторые из них:

Proof-of-Work (PoW) – доказательство работы. Вклад участника в достижение консенсуса определяется выполняемым им объемом вычислений. Метод PoW используется в Bitcoin и блокчейнах, созданных на его основе.

Proof-of-Stake (PoS) – доказательство доли. Вклад участника в достижение консенсуса определяется долей токенов блокчейна, которыми он владеет, от их общего количества.

Delegated Proof-of-Stake – этот алгоритм очень похож на PoS, но пользователи с большим количеством монет могут голосовать и выбирать представителей (других пользователей, которым они доверяют) для проверки транзакций, а ведущие представители (которые набрали наибольшее количество голосов) получают право проверять транзакции.

Leased Proof of Stake (LPoS) – усовершенствованная версия алгоритма Proof of Stake (PoS). Традиционно в алгоритме Proof of Stake каждый узел содержит определенную сумму криптовалюты и может добавить следующий блок в цепочку блоков. Однако, с помощью Leased Proof of Stake, пользователи могут сдавать в аренду свои монеты пользователям, держащим полные узлы (full nodes).

Proof-of-Capacity (Proof-of-space) – подтверждение емкости (PoC) это алгоритм согласованности используется в блокчейне и позволяет майнинг оборудованию использовать в сети доступное пространство на жестком диске для определения прав на майнинг вместо использования вычислительной мощности устройства.

Proof-of-Weight – каждому пользователю в сети, использующему Proof-of-Weight, присваивается «вес». Этот вес основан на том, сколько денег пользователь держит на своей учетной записи. Пока общая взвешенная часть пользователей честна, обычно две трети или больше, сеть будет оставаться безопасной.

Proof-of-Authority – доказательство полномочий. Находящийся в разработке алгоритм консенсуса, который предполагается использовать в управляемых (частично централизованных) блокчейнах. В этом алгоритме транзакции, подписанные участниками с повышенными полномочиями, будут иметь преимущество.

В качестве примера для разработки модели блокчена был взят алгоритм, успешно использующийся на текущий момент в блокчейне Bitcoin. В случае имитационной модели основные реализуемые операции выглядят следующим образом:

- проведение транзакции;
- рассылка транзакции всем участникам сети;
- проверка транзакций, пришедших от других участников сети;
- создание блоков;
- передача блоков на проверку;
- проверка блоков;
- добавление блоков в базу данных, при удачной проверке;
- графическое представление для визуализации работы.

СПИСОК ЛИТЕРАТУРЫ

1. Табернакулов А. Блокчейн на практике / Александр Табернакулов, Ян Койфманн. — Москва: Альпина Паблишер, 2019. — 260 с.
2. Б. Сингхал, Г. Дамеджа, П.С. Панда. Блокчейн. Руководство для начинающих разработчиков: Пер. с англ. / Б. Сингхал, Г. Дамеджа, П. С. Панда. – СПБ.: БХВ-Петербург, 2020. – 288м.: ил.
3. Литвин А.А. Возможности блокчейн-технологии в медицине (обзор)/ Литвин А.А., Коренев С.В., Князева Е.Г., Litvin V. // Современные технологии медицины. -2019. -№4. -191.
4. Бондарь В.А. Возможности использования технологии блокчейн в системах электронного документооборота // Документ. Архив. История. Современность: сборник статей/ Уральский федеральный университет имени первого Президента России Б.Н. Ельцина. – Екатеринбург - № 19 -2019. - С.280-290.
5. Дорожная карта развития «сквозной» цифровой технологии «Системы распределенного реестра» [Электронный ресурс] URL: sdo.krsk.irgups.ru/pluginfile.php/25100/mod_resource/content/0/Дорожная карта Блокчейн.pdf (дата обращения 05.06.2021)

УДК 004.89

ТЕХНОЛОГИЧЕСКИЙ БАЗИС СОВРЕМЕННЫХ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

Берлин Александр Романович, Литвинов Владислав Леонидович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: vlad.litvinov61@gmail.com, aleksanderberlin@gmail.com

Аннотация. Переход от традиционных к интеллектуальным системам поддержки принятия решений (СППР) – основной вектор их развития. В работе рассмотрены современные технологии разработки интеллектуальных СППР. Показано, что будущее интеллектуальных СППР за гибкостью применяемых моделей данных, так как ни один из известных подходов (классические модели, машинное обучение, теория игр) не универсален с точки зрения эффективности принятых решений.

Ключевые слова: система поддержки принятия решений; дата майнинг; интеллектуальная информационная система; нейронные сети.

TECHNOLOGICAL BASIS OF MODERN DECISION SUPPORT SYSTEMS

Berlin Aleksander, Litvinov Vladislav
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: vlad.litvinov61@gmail.com, aleksanderberlin@gmail.com

Abstract. The transition from traditional to intelligent decision support systems (DSS) is the main vector of their development. The paper considers modern technologies for the development of intelligent DSS. It is shown that the future of intelligent DSSs lies in the flexibility of the applied data models, since none of the known approaches (classical models, machine learning, game theory) is universal in terms of the efficiency of the decisions made.

Keywords: decision Support System; Data Mining; Intelligent Information System; neural networks.

Введение. Системы поддержки принятия решений (СППР) (Decision Support System, DSS) – интерактивные компьютерные системы, которые помогают лицу, принимающему решение (ЛПР), использовать информацию и модели для решения слабоструктурированных или трудноформализуемых задач. Согласно энциклопедическому словарю [1] СППР – это комплекс математических и эвристических методов и моделей, объединенных общей методикой формирования альтернативных решений в организационных системах, определения последствий реализации каждой альтернативы и обоснования выбора наиболее приемлемого решения. Переход от традиционных СППР к интеллектуальным требует уточнения этого определения.

В настоящее время существует несколько определений интеллектуальных систем поддержки принятия решений (ИСППР), которые практически связаны с одним и тем же функционалом. В общем виде, ИСППР – это такая система, которая ассистирует ЛПР в принятии этих решений, используя инструментарии Data Mining, моделирования и визуализации, обладает дружелюбным пользовательским интерфейсом, устойчива по качеству, интерактивна и гибка по настройкам [2].

Необходимость развития технологического базиса ИСППР диктуется следующими причинами:

– растущая сложность моделей данных в принятии решений;
– необходимость в точной оценке последствий различных альтернативных решений;
– необходимость предсказательного функционала;
– необходимость мультипотокового входа (для принятия решения нужны выводы на основе данных, экспертные оценки, известные ограничения и т.п.).

Работа по достижению поставленной цели сводится к решению следующих основных задач:

– исследование и разработка методов автоматизации разработки ИСППР (в том числе, с использованием моделей нейронных сетей);
– исследование и разработка структурных и семантических моделей ИСППР (с использованием языковых и программных средств структуризации информации);
– исследование и разработка методов оценки информационной эффективности ИСППР (с использованием подходов теории информации).

Проектирование интеллектуальных систем поддержки принятия решений требует формализации описания предметной области, что может быть сделано средствами онтологического подхода. При этом необходимо получить модель собственно системы *MS* (*R*), в соответствии с принципом последовательного раскрытия неопределенности ранга *R* [3]. При проектировании реализуется принцип эволюционного развития, при котором сначала формируется топология системы, затем выбираются структуры связей и, наконец, оптимизируются параметры.

В основной функциональный набор современных ИСППР входят [4]: финансовое планирование и бюджетирование; формирование консолидированной отчетности; создание информационной системы стратегического управления на основе ключевых показателей деятельности (Balance Scorecards) с преднастроенными библиотеками показателей; анализ взаимоотношений с клиентами и поставщиками; анализ рыночных тенденций; функционально-стоимостный анализ (ABC-Costing); функционально-стоимостное управление (Activity Based Management, ABM); система постоянных улучшений; многомерный анализ данных (OLAP); выявление скрытых закономерностей (Data Mining); выявление моделей (структур) данных; статистический анализ и прогнозирование временных рядов; событийное управление бизнесом (Event-driven BI); анализ рисков; формирование преднастроенных запросов; интеллектуальный поиск (по неполным данным и неформальным запросам); бизнес-моделирование и анализ эффективности выполнения бизнес-процессов; референтные отраслевые модели. При этом особенностью является значительная бóльшая, чем в других информационных системах, наукоёмкость обработки данных.

В соответствии с предлагаемой концепцией процесс проектирования ИСППР можно разбить на ряд этапов.

– анализ предметной области;
– сбор данных;
– анализ данных;
– выбор моделей;
– экспертный анализ/интерпретация моделей;
– внедрение моделей;
– оценка ИСППР;

– внедрение ИСППР;
– сбор обратной связи (на каждом этапе).

Цель настоящего исследования состоит в анализе возможностей применения технологий машинного обучения и Data Mining для повышения эффективности ИСППР, а также построении имитационной модели интеллектуальной ИСПРР. В качестве инструментария предлагается использовать технологии, которые уже хорошо зарекомендовали себя [5], в том числе нейросетевые технологии. В качестве среды имитационного моделирования используется отечественное программное обеспечение – среда AnyLogic. Особенностью рассматриваемого класса задач является использование нейросетевых технологий компьютерного анализа и синтеза естественных языков (Natural Language Processing, NLP) [6].

Заключение. Таким образом, в работе предложен оригинальный подход к построению интеллектуальных СППР в сочетании с эффективными возможностями современных нейронных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Экономико-математический энциклопедический словарь / Гл. ред. В.И. Данилов-Данильян. М.: Большая Российская энциклопедия: ИНФРА-М, 2003. – 688 с. – ISBN 5-85270-217-X; ISBN 5-16-000594-3.
2. Литвинов В. Л., Литвинова Е.В. Интеллектуализация технологического базиса дисциплины «Системы поддержки принятия решений» в подготовке магистров по направлению «Информационные системы и технологии» // Современное образование: содержание, технологии, качество. Материалы XXVI международной научно-методической конференции. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2020. С.105-107.
3. Губин А.Н., Литвинов В.Л., Филиппов Ф.В. Информационная эффективность интеллектуальных систем поддержки принятия решений //В сборнике: Информационные системы и технологии в моделировании и управлении. Сборник трудов V Международной научно-практической конференции. Отв. редактор К.А. Маковейчук. 2020. С. 19-23.
4. Попов А. Л. Системы поддержки принятия решений: Учебно-метод. пособие / Попов А.Л. – Екатеринбург: Урал. гос. ун-т, 2008. 80 с.
5. Интеллектуальные системы поддержки принятия решений – краткий обзор. URL: https://habr.com/ru/company/ods/blog/359188/ (Дата обращения 29.06.2021).
6. Vladislav L. Litvinov. Research of Neural Network Methods of Text Information Classification. Published: Oct 2019 in III International Conference on Control in Technical Systems (CTS). DOI: 10.1109/CTS48763.2019.8973314.

УДК 004.056

ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В КИБЕРФИЗИЧЕСКИХ СРЕДАХ И РАСПРЕДЕЛЕННЫХ ЦИФРОВЫХ СИСТЕМАХ УПРАВЛЕНИЯ

Верхова Галина Викторовна, Шабанов Александр Павлович, Васильев Матвей Александрович
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: galina500@inbox.ru, saxa@shpg.spb.ru, waytokey@mail.ru

Аннотация. Представлены результаты исследований в области идентификации пользователей в распределенных вычислительных системах и средах. Приведены особенности построения распределенных цифровых систем управления и организации процесса идентификации пользователей в таких системах. Указаны пути формирования интероперабельных цифровых сред и их интеграцию в единую киберфизическую среду.

Ключевые слова: идентификация пользователей; цифровая распределенная система; цифровая экосистема; сервер идентификации; интероперабельная цифровая среда.

USER IDENTIFICATION IN CYBER-PHYSICAL ENVIRONMENTS AND DISTRIBUTED DIGITAL CONTROL SYSTEMS

Verhova Galina, Shabanov Aleksandr, Vasil'ev Matvej
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: galina500@inbox.ru, saxa@shpg.spb.ru, waytokey@mail.ru

Abstract. The results of research in the field of user identification in distributed computing systems and environments are presented. The features of the construction of distributed digital control systems and the organization of the user identification process in such systems are given. The ways of forming interoperable digital environments and their integration into a single cyber-physical environment are indicated.

Keywords: user identification; digital distributed system; digital ecosystem; identification server; interoperable digital environment.

Единая киберфизическая среда призвана обеспечить сквозное инфокоммуникационное взаимодействие между участниками, представляющими собой физических лиц, объединения физических и юридических лиц, а также техногенных объектов [1-4]. Киберфизическая среда необходима для организации эффективного функционирования распределенных предприятий и производств, обеспечивающих на базе технологий искусственного интеллекта максимальную степень автоматизации при создании глубоко кастомизированной продукции на всех этапах жизненного цикла. Интероперабельность локальных киберфизических сред обеспечит сквозное инфокоммуникационное взаимодействие между участниками вне зависимости от того, в какой киберсреде они зарегистрированы [5].

Киберфизические среды базируются на технологии распределенных цифровых систем управления. Одной из основных проблем формирования распределенных интероперабельных цифровых систем, способных к сквозному информационному взаимодействию, является организация процесса идентификации пользователей. Сервер идентификации в таких системах будет представлять собой распределенную систему, что принципиально отличает его от обычных (не интероперабельных) цифровых систем управления, имеющих как монолитную, так распределенную архитектуру. Система идентификации пользователей является частью ядра киберфизической среды, в состав которого, помимо системы идентификации, входит менеджер связей и система цифровых двойников [6] участников киберсреды, на основе которых формируются их информационные профили.

СПИСОК ЛИТЕРАТУРЫ

1. Акимов С.В., Верхова Г.В., Меткин Н.П. Теоретические основы CALS. СПб: Издательство СПбГУТ, 2018. 263С.
2. Guamushig T., Lopez C., Santorum M., Aguilar J. Characterization of a Fourth Generation Virtual Organization Based on Industry 4.0. 2019 International Conference on Information Systems and Software Technologies (ICI2ST), Quito, Ecuador, 2019. P. 182-186.
3. Pavlenko V., Shostak I., Morozova O., Danova M. Information support for business processes at virtual enterprises with multi-agent technologies. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kiev, 2018. P. 526-533.
4. Verkhova G.V., Akimov S.V. The role of the unified educational cyber environment in improving the quality of training of engineer personnel // Proceedings of 2018 XVII Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region (PTES). 2018. P. 70-74.
5. Верхова Г.В., Акимов С.В. Интеграция локальных интероперабельных киберсред виртуальных организаций в единую киберсреду постиндустриального общества // В сборнике: Долновая электроника и инфокоммуникационные системы. Сборник статей XXIV Международной научной конференции. Санкт-Петербург, 2021. С. 34-39.
6. Brylina O.G., Kuzmina N.N. Osintsev K.V. Modeling as the Foundation of Digital Twins // 2020 Global Smart Industry Conference (GloSIC), Chelyabinsk, Russia, 2020. P. 276-280.

УДК 004.056.53

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ЗАПОЛНЕНИЯ ТАБЛИЦЫ АССОЦИАЦИЙ ОБОРУДОВАНИЯ MIKROTIK

Ворошнин Григорий Евгеньевич[1], Ковцур Максим Михайлович[1], Киструга Антон Юрьевич[2], Докшин Александр Денисович[1]

[1] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия

[2] ООО "Фаст Лейн"
Профессора Попова ул., 37В, пом/комн 1н/71-73, Санкт-Петербург, 197136, Россия
e-mails: voroshnin.g@yandex.ru, maxkovzur@mail.ru, anton.kistruga@gmail.com, a.dokshin007@gmail.com

Аннотация. Широкое распространение глобальных и локальных сетей привело к многообразию сетевого оборудования и компаний, производящих его. Одной из крупных компаний является MikroTik, получившая популярность в малых корпоративных сетях благодаря широкому функционалу и низкой стоимости производимого сетевого оборудования. Сетевое оборудование может иметь уязвимости, в частности в настоящей работе рассматривается уязвимость оборудования MikroTik к критическому заполнению таблицы ассоциаций.

Ключевые слова: информационная безопасность; безопасность беспроводных сетей; устойчивость сетевого оборудования; MikroTik; заполнение таблицы ассоциаций.

INVESTIGATION OF THE EFFECT OF FILLING AN ASSOCIATION TABLE ON MIKROTIK

Voroshnin Grigory[1], Kovtsur Maxim[1], Kistruga Anton[2], Dokshin Alexander[1]

[1] The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia

[2] LLC “Fast Lane”
37B/1n/71-73 Professor Popov St, St. Petersburg, 197136, Russia
e-mails: voroshnin.g@yandex.ru, maxkovzur@mail.ru, anton.kistruga@gmail.com, a.dokshin007@gmail.com

Abstract. The widespread use of global and local networks has led to a variety of network equipment and companies that produce it. One of the large companies is MikroTik, which has gained popularity in small corporate networks due to its wide functionality and low cost of manufactured network equipment. Network equipment may have vulnerabilities, for example, in this paper we consider the vulnerability of MikroTik equipment to critical filling of the association table.

Keywords: information security; security of wireless networks; stability of network equipment; MikroTik; filling in the association table.

Из-за использования технологией Wi-Fi общедоступной среды передачи, становится возможным эксплуатация различных уязвимостей сетевого оборудования. Выявлению уязвимостей и разработке методов по обнаружению и противодействию эксплуатации уязвимостей посвящено не мало статей [1-4], но оборудование MikroTik исследовано крайне мало [5-7].

Стандартами IEEE 802.11 определен процесс подключения клиентов к точке доступа Wi-Fi. В ходе подключения клиент проходит аутентификацию и ассоциацию, таким образом перемещаясь из состояния 1 в

состояние 3. Для поддержания связи с точкой доступа, клиенту необходимо оставаться в состоянии 3. Состояния всех клиентов хранятся в таблице ассоциаций, объем которой ограничен обычно количеством записей, либо размером выделенной для хранения записей памяти.

Критическое заполнение данной таблицы произойти из-за большого количества клиентов, пытающихся подключиться к сети. Такое может произойти при массовом скоплении людей на каких-либо собраниях, при неправильно разработанной архитектуре сети, не подразумевающей увеличения количества клиентов, или из-за умышленной атаки на сеть злоумышленником

В ходе эксперимента на оборудовании MikroTik было выяснено, что основными последствиями критического заполнения таблицы ассоциаций для него стало невозможность подключения новых клиентов и повышенная нагрузка на CPU оборудования. Также возможными последствиями может быть истощение ресурсов беспроводного интерфейса оборудования и зашумление беспроводной среды.

Для обеспечения устойчивости оборудования и сети в целом, необходимо принимать меры по обнаружению и противодействию таким ситуациям. В целях профилактики необходимо применять методы резервирования, рассчитывая возможные потребности в новых подключениях клиентов. При эксплуатации уязвимости злоумышленником временным выходом может служить смена канала работы точки доступа с дальнейшим позиционированием станции злоумышленника с целью ее обезвреживания.

Заполнение таблицы ассоциаций является серьезной опасностью, приводящей к нарушению работы сети. На оборудовании MikroTik это выражалось в невозможности подключения новых клиентов и повышенной нагрузке на CPU. С учетом этого необходимо применять меры профилактики и предотвращения появления такой ситуации в сети или намеренной эксплуатации данной уязвимости.

СПИСОК ЛИТЕРАТУРЫ

1. Шелухин, О. И. Особенности DDoS атак в беспроводных сетях / О. И. Шелухин, А. Г. Симонян, Ю. А. Иванов // T-Comm: Телекоммуникации и транспорт. – 2012. – Т. 6. – № 11.
2. Капарбек, Б. Анализ угроз информационной безопасности в беспроводных сетях / Б. Капарбек, Г. Э. Жалилов // Современные проблемы механики. – 2020. – № 39(1).
3. Красов А.В., Обеспечение безопасности передачи MULTICAST-трафика в IP-сетях / Красов А.В., Сахаров Д.В., Ушаков И.А., Лосин Е.П. // Защита информации. Инсайд. 2017. № 3 (75). С. 34-42
4. Герлинг Е.Ю., Модели нарушителей информационной безопасности / Герлинг Е.Ю., Кулишкина Е.И., Бирих Э.В., Виткова Л.А. // Известия высших учебных заведений. Технология легкой промышленности. 2017. Т. 35. № 1. С. 27-30.
5. Шамсутдинов, Р. Р. Использование маршрутизаторов Mikrotik Rb-951 в качестве средств защиты информационной инфраструктуры малых организаций / Р. Р. Шамсутдинов // European research: innovation in science, education and technology: XXXVII INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE, London, United Kingdom, 07–08 февраля 2018 года. – London, United Kingdom: PROBLEMS OF SCIENCE, 2018. – С. 26-28.
6. Васин, Н. Н. Исследование стабильности работы маршрутизатора Mikrotik с большим объемом маршрутной информации / Н. Н. Васин, А. С. Кондаков // III Научный форум телекоммуникации: теория и технологии ТТТ-2019 : Материалы XXI Международной научно-технической конференции, Казань, 18–22 ноября 2019 года. – Казань: Казанский государственный технический университет им. А.Н. Туполева, 2019. – С. 61-62.
7. Давидюк, Н. В. Обеспечение безопасности абонентского телетрафика путём конфигурирования и настройки маршрутизатора (на примере MikroTik RouterBOARD): Практикум / Н. В. Давидюк. – Санкт-Петербург: Общество с ограниченной ответственностью "Издательский центр "Интермедия", 2020. – 68 с. – ISBN 9785438301950.

УДК 004.056.53

АНАЛИЗ СОВРЕМЕННЫХ СРЕДСТВ АВТОМАТИЗИРОВАННОЙ ПРОВЕРКИ ФУНКЦИЙ БЕЗОПАСНОСТИ КОММУТАЦИОННОГО ОБОРУДОВАНИЯ

Карельский Павел Владимирович, Ковцур Максим Михайлович, Штеренберг Станислав Игоревич, Малинин Никита Игоревич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: pasha.karelscky@yandex.ru, maxkovzur@mail.ru, shterenberg.stanislaw@yandex.ru

Аннотация. Автоматизация – это процесс введения в алгоритм действий, необходимых для выполнения той или иной задачи, элементов, выполняемых техническими средствами, в результате чего уменьшается потребность в персональном участии человека в работе по созданию, преобразованию и эксплуатации продуктов, энергии или информации. Стандартизация процесса является необходимым компонентом из-за того, что при произвольном изменении процесса работы, изменении последовательности выполняемых действий невозможно внедрить элементы автоматизации в систему.

Ключевые слова: информационная безопасность; система автоматизации; Ansible.

LEARNING TOOLS FOR AUTOMATION SYSTEM

Karelsky Pavel, Kovtsur Maxim, Shterenberg Stanislav, Malinin Nikita

The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: pasha.karelscky@yandex.ru, maxkovzur@mail.ru, shterenberg.stanislaw@yandex.ru

Abstract. Automation is the process of introducing into the algorithm the actions necessary to perform a particular task, elements performed by technical means, as a result of which the need for a person's personal participation in the creation, transformation and operation of products, energy or information decreases. Process standardization is a necessary component due to the fact that with an arbitrary change in the work process, changing the sequence of actions performed, it is impossible to introduce automation elements into the system.

Keywords: information security; automation system; Ansible.

В рамках данного доклада предлагается автоматизация ряда задач с помощью инструмента Ansible. Ansible — это простая общедоступная платформа автоматизации IT решений работающая на Python, которая упрощает развертывание и обслуживание приложений и систем. Ansible позволяет автоматизировать все, от развертывания кода до конфигурации сети и управления облаком, на языке YAML, который приближается к простому английскому, с использованием SSH и без агентов для установки в удаленных системах. Ansible имеет модульную структуру и состоит из нескольких компонентов.

В состав системы входят:

Inventory – файл, в котором содержаться указания по подключению к удаленным устройствам, такие как IP адрес и метод подключения. Удаленные устройства в этом файле могут быть сгруппированы для одновременной работы с ними [1].

Playbooks – файл, в котором содержаться команды, предназначенные для выполнения на удаленных устройствах. Playbook написан на YAML. Этот язык имеет максимально упрощенный синтаксис, который поймет любой специалист, имевший опыт работы с системами типа Lnux, вне зависимости от навыков программирования на других языках.

Файл конфигурации – указывает на расположение файла inventory, директорию с модулями Ansible, пользователя и ряд других стандартных параметров [2].

Ansible имеет ряд ограничений. Главное из них – это возможность работы исключительно через SSH соединение. Поскольку предложенная в данной работе методика подразумевает стартовую конфигурацию тестируемого оборудования «с нуля», необходимо использовать последовательный интерфейс RS-232, не предназначенный для связи по протоколу SSH. Вследствие этого в рамках данного исследования промежуточным звеном между платформой автоматизации и сетевым оборудованием является персональный компьютер, с установленной на нем операционной системой Kali Linux, имеющий несколько консольных портов, к которым подключается настраиваемое оборудование по RS-232. Таким образом оператор Ansible будет подключаться не напрямую к оборудованию, а к ПК, которому подключено тестируемое оборудование, по протоколу SSH, и через интерфейс командной строки (shell) Linux транслировать необходимые команды на сетевое оборудование, перенаправляя их на интерфейс последовательного порта ttyS*.

Помимо конфигурации оборудования Ansible также позволяет автоматизировать работу других элементов стенда тестирования [3, 4].

Автоматизация тестирования создает ограничение в использовании программного обеспечения. Это ограничение заключается в невозможности использовать программное обеспечения с графическим пользовательским интерфейсом в качестве автоматизируемого элемента. Из этого следует, что при подборе инструментов для проведения тестирования приходится выбирать только из консольных приложений, выполняющих требующие задачи, для корректного введения команд управления в скрипты. Тем не менее это не следует рассматривать как недостаток конкретного выбранного инструмента автоматизации, то есть Ansible. Для любой системы автоматизации привязка управления приложением исключительно через графический интерфейс приводит к невозможности его внедрения в названную систему. В ходе исследования изучалась также концепция построения системы автоматизации на Bash-скриптах. Плюсом такой системы являлась кроссплатформенность, а также независимость от существующего ПО для автоматизации. С другой стороны, для такого варианта значительно сложнее создать единую систему, способную охватить процесс тестирования целиком. Кроме того, для передачи задач другим исполнительным узлам требовалось бы введение дополнительных инструментов. На рисунке 8 представлен пример Bash-скрипта для конфигурации тестируемого оборудования [5].

В нем используются команды для пакетного клиента ctel, который позволяет передавать команды удаленным устройствам. Данные команды передаются на сетевой контроллер BT-5005, на котором обрабатываются и передаются через консольный интерфейс на настраиваемое устройство. Пример наглядно показывает, что в сравнении системой Ansible, в варианте автоматизации Bash-скриптами возникает гораздо больше промежуточных элементов, что является нежелательным качеством любой системы.

СПИСОК ЛИТЕРАТУРЫ

1. Красов, А.В., Косов Н.А., Холоденко В.Ю. Исследование методов провижининга безопасной сети на мультивендорном оборудовании с использованием средств автоматизированной конфигурации // Colloquium-journal. 2019. № 13-2 (37). С. 243-247.
2. Миняев А.А., Красов А.В. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 26-32.
3. Ansible Documectation [Электронный ресурс], URL: www.docs.ansible.com/ (дата обращения: 16.04.2021)
4. Netsniff-NG Toolkit [Электронный ресурс], URL: www.netsniff-ng.org/ (дата обращения: 16.04.2021)
5. Ахрамеева К.А., Малинин Н.И., Герлинг Е.Ю., Бочаров М.В., Куликов И.А. Автоматизированное тестирование функций безопасности клиентских портов коммутатора // Заметки ученого. 2021 №5 С. 55-61.

УДК 004.056.5

ИССЛЕДОВАНИЕ МЕТОДИКИ СРАВНЕНИЯ VPN РЕШЕНИЙ

Ковцур Максим Михайлович, Сахаров Дмитрий Владимирович, Мисливский Борис Сергеевич, Михайлова Анастасия Валерьевна

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: mislivskyboris@yandex.ru, sguard7@mail.ru, maxkovzur@mail.ru, ova.007@yandex.ru

Аннотация. Рассмотрены понятия и теоретические сведения о технологии VPN, включая следующие технологии: IPsec и OpenVPN. Изучены особенности функциональности сетевой операционной системы pfSense. Был осуществлен обзор инструментов для оценки количественных критериев эффективности VPN.

Ключевые слова: VPN; IPsec; OpenVPN; pfSense; сравнение.

STUDY OF VPN SOLUTIONS COMPARISON

Kovzur Maxim, Mislivskij Boris, Saharov Dmitrij, Mihajlova Anastasija

The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: mislivskyboris@yandex.ru, sguard7@mail.ru, maxkovzur@mail.ru, ova.007@yandex.ru

Abstract. The concepts and theoretical information about VPN technology, including the following technologies: IPsec and OpenVPN, are considered. The features of the functionality of the pfSense network operating system have been studied. A review of tools for assessing quantitative criteria for VPN performance was carried out.

Keywords: VPN; IPsec; OpenVPN; pfSense; comparison.

В настоящее время был осуществлен массовый и быстрый переход на дистанционный формат работы. Вместе с ростом количества удаленных рабочих мест появляются проблемы, связанные с обеспечением конфиденциальности, целостности и доступности корпоративных данных. Для решения данных проблем и организации защищенного канала связи с удаленными сотрудниками применяется технология VPN.

VPN (англ. Virtual Private Network) используется для создания изолированных сетей на базе открытых каналов связи, например Интернет. За счет использования средств криптографии такие виртуальные частные сети могут обеспечивать требуемый уровень безопасности и секретности, являясь более экономичным аналогом выделенных линий. Популярным способом для организации удаленного доступа являются продукт OpenVPN и решения на базе стандарта IPsec.

Для сравнения данных протоколов туннелирования необходимо определиться с критериями оценивания. Критерии можно разделить две большие группы: качественные и количественные. Количественные критерии могут быть выражены в числовом виде и измерены экспериментальным путем. Проводить такое измерение VPN протоколов удобнее с помощью специализированной сетевой операционной системы, которая будет отличаться быстротой развертывания, функциональностью и встроенной поддержкой рассматриваемых решений. Выбор был сделан в пользу проекта с открытым исходным кодом pfSense.

pfSense — это сетевая операционная система, основанная на ядре FreeBSD, включающая в себя функционал маршрутизатора, межсетевого экрана, а также VPN-сервера и ряда других. Для настройки и управления используется веб-интерфейс, из которого также возможна установка дополнительных пакетов из репозитория. Операционная система может быть установлена как на аппаратном обеспечении, так и в среде виртуализации.

pfSense поддерживает создание всех видов IPsec туннелей, имеется реализация OpenVPN. Также в дистрибутиве присутствует функционал формирователя трафика (traffic shaping) под названием Limiters, поддержка отказоустойчивых кластеров и подробная служба мониторинга состояния система, включающая отображение использования памяти, загрузки центрального процессора и использования сетевых ресурсов.

Для выполнения сравнения необходимо выполнить следующие действия:

- Создать виртуальные машины;
- Установить на них операционные системы для клиентов и сервера VPN;
- Настроить рассматриваемые VPN подключения;
- Установить дополнительные инструменты для тестирования;
- Произвести измерения и выполнить анализ полученных данных.

Для разворачивания стенда была выбрана среда виртуализации VirtualBox. Виртуальный стенд состоял из следующих объектов:

- Удаленный пользователь ПК-1;
- Локальный пользователь ПК-2;
- VPN-шлюз;

и выполнял следующий сценарий: «из внешней сети удаленный пользователь ПК-1 пытается подключиться к локальному пользователю ПК-2. Для корректности подключения используется VPN-шлюз, развернутый на третьей виртуальной машине».

Сравниваемым критерием была выбрана пропускная способность туннеля. Для получения данных был установлен пакет iperf3, который способен создавать TCP и UDP трафик, а также измерять скорость передачи данных в канале.

Оптимальный выбор решения для организации VPN — важная задача, для которой требуется сравнение по множеству качественных и количественных критериев. Использование сетевой операционной системы pfSense позволяет ускорить развертывание различных протоколов туннелирования и быстрее сравнить их по количественным параметрам.

СПИСОК ЛИТЕРАТУРЫ

1. Некоторые аспекты организации удаленной работы персонала в условиях пандемии / И. И. Сергеева, М. А. Степанова, А. Ю. Бабак, А. Е. Дутиков // Экономическая среда. – 2021. – № 1(35). – С. 47-52.
2. Гостеева, А. И. Сравнительный анализ технологий организации VPN-соединений / А. И. Гостеева, Е. Е. Истратова // Программно-техническое обеспечение автоматизированных систем : Материалы Всероссийской молодежной научно-практической конференции, Барнаул, 16 декабря 2020 года / Под редакцией А.Г. Якунина. – Барнаул: Алтайский государственный технический университет им. И.И. Ползунова, 2021. – С. 128-131.
3. Плетеный, Д. С. Сравнение VPN - соединений для применения в защищенных корпоративных сетях / Д. С. Плетеный, В. В. Аленченко // Аллея науки. – 2020. – Т. 2. – № 5(44). – С. 979-984.
4. Старун, И. Г. Построение математической модели расчета комплексной оценки VPN / И. Г. Старун, А. Н. Югансон, Ю. А. Гатчин // Вестник Тамбовского государственного технического университета. – 2019. – Т. 25. – № 4. – С. 535-546.
5. Экспериментальная оценка количественных характеристик MPLS оборудования для L2 VPN / И. П. Зуев, П. В. Карельский, М. М. Ковцур, П. Э. Луеке // Региональная информатика и информационная безопасность : Сборник трудов, Санкт-Петербург, 23–25 октября 2019 года. – Санкт-Петербург: Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2019. – С. 41-43.
6. Степанова, И. В. Использование перспективных технологий для развития распределенных корпоративных сетей связи / И. В. Степанова, М. О. А. Абдулвасеа // T-Comm: Телекоммуникации и транспорт. – 2017. – Т. 11. – № 6. – С. 10-15.

УДК 004.89

ТЕХНОЛОГИЧЕСКИЙ БАЗИС СОВРЕМЕННЫХ СИСТЕМ УПРАВЛЕНИЯ ВЗАИМООТНОШЕНИЯМИ С КЛИЕНТАМИ В ОБЛАСТИ ПОЧТОВЫХ ОТПРАВЛЕНИЙ

Литвинов Владислав Леонидович, Мурашко Артем Николаевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: vlad.litvinov61@gmail.com, artmur01@yandex.ru

Аннотация. Переход от традиционных к интеллектуальным системам управления взаимоотношениями с клиентами (Customer Relationship Management, CRM) – основной вектор их развития. Главные задачи, которые выполняет CRM – это организация внутренней работы сотрудников (планировщик задач, статистика, отчеты) и организация работы с клиентами (воронка продаж, напоминание о звонках, отслеживание статусов оплаты, переписка и общение). CRM в одном месте объединяет инструменты для работы менеджеров и владельцев бизнеса (почта и мессенджеры, рекламные инструменты, аналитика, отчеты и планировщики задач, телефония и другие). В работе рассмотрены основные подходы к интеллектуализации процессов сбора и анализа информации о потребителях, поставщиках, партнёрах, а также о внутренних процессах компании в области почтовых отправлений.

Ключевые слова: система управления взаимоотношениями с клиентами; CRM; интеллектуальная информационная система; нейронные сети.

TECHNOLOGICAL BASIS OF MODERN CUSTOMER RELATIONSHIP MANAGEMENT SYSTEMS

Litvinov Vladislav, Murashko Artem
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: vlad.litvinov61@gmail.com, artmur01@yandex.ru

Abstract. The transition from traditional to intelligent systems of customer relationship management (Customer Relationship Management, CRM) is the main vector of their development. The main tasks that CRM performs are organizing the internal work of employees (task planner, statistics, reports) and organizing work with clients (sales funnel, call reminders, tracking payment status, correspondence and communication). CRM in one place brings together tools for managers and business owners (mail and messengers, advertising tools, analytics, reports and task schedulers, telephony and others). The paper discusses the main approaches to the intellectualization of the processes of collecting and analyzing information about consumers, suppliers, partners, as well as about the internal processes of the company in the field of mailings.

Keywords: Customer Relationship Management System; CRM; intelligent information system; neural networks.

Введение. В настоящее время наблюдается существенное повышение интереса исследователей и разработчиков к созданию проактивных систем управления взаимоотношениями с клиентами (Customer Relationship Management, CRM). Использование современных информационных технологий при реализации CRM-концепции позволяет в оперативном режиме формировать базу данных о клиентах, проводить анализ и

прогнозы об их возможном поведении, что, в конечном итоге, способствует более эффективной организации продаж и упрощению контактов с потребителями [1].

По назначению можно выделить следующую классификацию CRM:

– автоматизированная система управления продажами (sales force automation);

– управление маркетингом;

– управление клиентским обслуживанием и колл-центрами (системы по обработке обращений абонентов, фиксация и дальнейшая работа с обращениями клиентов).

В настоящее время на рынке программного обеспечения существует множество готовых решений в области CRM: от сложных корпоративных информационных систем для крупных предприятий до отдельных программ для автоматизации управления заказами клиентов для небольших предприятий.

Битрикс – крупнейший игрок на рынке с громоздким функционалом, подходит для больших производственных компаний, позволяет автоматизировать бизнес-процессы.

AmoCRM – подходит отделам продаж и компаниям, которые хотят отслеживать сделки и вести отчеты. CRM легко интегрируется с социальными сетями.

Мегаплан – чаще всего используется производственными предприятиями. Имеет API для обмена данными между Мегапланом и вашим приложением, интернет-магазином или сервисом. Это простой способ создавать, редактировать и получать информацию из разных каналов в одном интерфейсе. Легко интегрируется с 1С [2].

Salesfors – занимает 20% американского рынка CRM. В тарифах Salesforse можно выбирать отдельно инструменты, которые будут использоваться.

Билайн CRM – простая и бесплатная CRM для выполнения небольших задач. Подойдет для начала маленьком бизнесу или предпринимателю. Есть бесплатный функционал с ограничениями.

Sale SAP CRM (S2) – имеет хорошие возможности для автоматизации и упрощения работы менеджера отдела продаж: автоматические отправки писем при выполнении условий (или смс), выставление счетов, удобная история работы с клиентом.

Тем не менее в большинстве случаев внедрение CRM-систем по-прежнему ограничено использованием программного обеспечения лишь в качестве автоматизированной системы управления контактами. Это позволяет структурировать информацию о клиентах, но упускается из виду более широкая перспектива возможностей.

Например, в задачах управления заказами [3]: история контактов; работа с клиентами, включая все активности, связанные с клиентом; прием и оформление заказов от клиентов; создание коммерческих предложений; прогнозирование, анализ цикла продаж, региональный анализ, запланированная и произвольная отчетность.

В задачах поддержки и сервиса: регистрация обращений, переадресация обращений, движение заявок от клиента внутри компании, отчетность, управление решением проблем, информация по заказам, управление гарантийным/контрактным обслуживанием.

В задачах маркетинга: управление маркетинговыми кампаниями, управление потенциальными сделками, (полная информация о продуктах и услугах компании) интегрированная с Интернетом, конфигуратор продукции, сегментация клиентской базы, создание и управление списком потенциальных клиентов.

Цель настоящего исследования состоит в анализе возможностей применения технологий машинного обучения и Data Mining для повышения эффективности CRM-систем в области почтовых отправлений. В качестве инструментария предлагается использовать технологии, которые уже хорошо зарекомендовали себя в задачах интеллектуального интернет-маркетинга [4], в том числе нейросетевые технологии. Особенностью рассматриваемого класса задач является использование нейросетевых технологий компьютерного анализа и синтеза естественных языков (Natural Language Processing, NLP) [5].

Заключение. Таким образом, в работе рассмотрены подходы к построению интеллектуальной CRM-системы в сочетании с эффективными возможностями современных нейронных сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Зотов Даниил. CRM система: что это простыми словами + топ лучших. [Электронный ресурс]. URL: https://ztvd.ru/crm-sistema-chto-eto/ (дата обращения: 30.06.2021).
2. Мегаплан – система для удаленной работы. [Электронный ресурс]. URL: https://megaplan.ru/crm-for-business/. (дата обращения: 30.06.2021).
3. Шполянская И. Ю. Использование технологий Data Mining с целью создания аналитических CRM-систем для малого бизнеса. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/ispolzovanie-tehnologiy-dataminings-tselyu-sozdaniya-analiticheskih-crm-sistemdlya-malogo-biznesa/viewer (дата обращения: 30.06.2021).
4. Короткова М.И., Литвинов В.Л., Соколова К.В. Применение инструментальных средств машинного обучения в задачах интернет-маркетинга. В сборнике: 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. 436-441.
5. Vladislav L. Litvinov. Research of neural network methods of text information classification // Proceedings of 2019 3rd International Conference on Control in Technical Systems, CTS 2019 (2019). P. 225-227. DOI: 10.1109/CTS48763.2019.8973314.

УДК 004.7

ЭФФЕКТИВНАЯ ОРГАНИЗАЦИЯ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ РАСПРЕДЕЛЕННОЙ ОБРАБОТКЕ ДАННЫХ

Птицына Лариса Константиновна, Жаранова Анастасия Олеговна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: ptitsina_lk@inbox.ru, zharanovaan@gmail.com

Аннотация. Актуализировано формирование технологий, обеспечивающих безопасное функционирование распределенных информационных систем. Акцентировано внимание на значимости определения степени качества функционирования комплексных систем защиты информации при распределенной обработке данных с целью преодоления неопределенности относительно наилучшего варианта организации системы. Представлен ряд оснований для использования инструментального средства, позволяющего оценить степень влияния механизмов комплексирования и степени распределенности на качество функционирования комплексных систем защиты информации.

Ключевые слова: защита информации; распределенные системы; комплексные системы защиты информации; качество; архитектура.

EFFECTIVE ORGANIZATION OF COMPLEX INFORMATION SECURITY SYSTEMS FOR DISTRIBUTED DATA PROCESSING

Ptitsyna Larisa, Zharanova Anastasia
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: ptitsina_lk@inbox.ru, zharanovaan@gmail.com

Abstract. The formation of technologies that ensure the safe functioning of distributed information systems is updated. Attention is focused on the importance of determining the degree of quality of the functioning of complex information security systems in distributed data processing in order to overcome uncertainty about the best option for organizing the system. A number of reasons for using a tool that allows us to assess the degree of influence of aggregation mechanisms and the degree of distribution on the quality of functioning of complex information security systems are presented.

Keywords: protection of information; distributed systems; complex information security systems; quality; architecture.

В условиях появления сложных информационно-телекоммуникационных систем и использования удаленных хранилищ в совокупности с разнородными технологиями передачи данных и различными средами проводного и беспроводного секторов при разнообразной степени территориальной распределенности оборудования актуализируется вопрос развития распределенных информационных систем. В связи с этим образуется объективная необходимость развития их информационно-технического сопровождения в целях обеспечения их безопасного функционирования.

При стремительном развитии информационных систем и технологий и высоком уровне технических средств открываются широкие возможности по представлению распределенной архитектуры комплексных систем защиты информации распределенных систем. Из-за крупномасштабности и функциональной значимости подобных систем непозволительно игнорировать вопрос качества их функционирования, так как это может повлечь высокие экономические потери. Помимо этого, объективности требует выбор одного из множества альтернативных вариантов реализации комплексных систем защиты информации распределенных систем. Достичь объективности возможно за счет анализа влияния распределенности на динамические характеристики задействованных механизмов и средств [1, 2].

Благодаря специфике комплексных систем защиты информации возможно применение различных реализаций наборов защитных средств, что повышает возможности охвата внешних негативных воздействий за счет увеличения числа обнаруживаемых угроз, уменьшает время на выполнение процессов по обеспечению информационной защищенности, повышает точность принимаемых решений в процессе защиты.

Качество функционирования комплексной системы защиты информации зависит от выбранного варианта построения системы. Для преодоления неопределенности относительно наилучшего варианта организации системы необходимо производить моделирование комплексной системы защиты информации, при котором является возможным определение влияния архитектуры на временные характеристики системы.

Получаемые результаты поддаются сравнительному анализу на предмет использования различных архитектур комплексных систем защиты информации. При выборе основной упор делается на оценки вероятностно-временного характера, определяющиеся плотностями и функциями распределения. В их число входит риск срыва временного регламента по обнаружению угрозы, который также может быть выражен через плотность распределения вероятностей дискретного времени.

Современные средства защиты информации способны отражать определенное количество внешних негативных воздействий из всех возможных угроз. Исходя из этого, информационная защита может

осуществляться некоторым набором средств из всего возможного комплекса, изменения состава которого напрямую зависят от характера возможных внешних воздействий.

Описание структуры части комплекса зависит от состава механизмов и средств с их взаимосвязями, определяющимися функциями распределения. Набор технических средств и механизмов защиты определяет функциональную спецификацию программного средства и исходные данные для оценки динамического профиля механизмов защиты информации относительно выбранного варианта системы.

Отсутствие объективных методологических и инструментальных средств по оценке качества функционирования комплексной системы защиты информации влечет за собой ряд серьезных проблем, в числе которых:

– низкое качество функционирования комплексных систем защиты информации и ее неэффективность в отношении заранее определенного набора потенциально возможных внешних воздействий;

– экономические убытки из-за сложности объективной оценки затрат на реализацию комплексной системы защиты информации;

– стремительная потеря востребованности комплексной системы защиты информации ввиду устаревания заложенных в нее механизмов защиты.

Все вышеперечисленное указывает на острую необходимости разработки методологических и инструментальных средств по оценке качества функционирования комплексных систем защиты информации.

Наличие инструментального средства по оценке качества функционирования комплексной системы защиты информации позволит объективно формировать требования и ограничения системы в процессе проектирования и разработки. Результатом разработки с использованием средств по оценке качества функционирования систем становится функционально эффективная система, удовлетворяющая заданным требованиям и ограничениям и учитывающая динамику развития окружающей среды.

Необходимо математическое обеспечение, позволяющее определять динамические характеристики систем и используемое для исследования влияния временных характеристик и архитектур комплексных систем защиты информации на качество их функционирования [3, 4].

При исследовании влияния способов организации комплексных систем защиты информации необходимо ориентироваться на:

– параллельное функционирование технических средств и механизмов защиты;
– применение функции синхронизации «И» при объединении результатов работы средств;
– применение функции синхронизации «ИЛИ» при объединении результатов работы средств;
– уровни комплексирования;
– степень параллелизма;
– длительности процессов реакции на появляющиеся негативные воздействия.

Учтенные параметры могут варьироваться при анализе динамических характеристик комплексных систем защиты информации, что позволяет производить анализ различных архитектур систем и оценивать их эффективность в процессе защиты информации.

Использование инструментального средства позволяет оценить степень влияния механизмов комплексирования и степени распределенности на качество функционирования комплексных систем защиты информации, проводить, сокращать временные затраты на противодействие внешним техническим угрозам, оценивать эффективность комплексных систем защиты информации.

Таким образом, учет выявленных положений при разработке комплексных систем защиты информации способствует повышению уровню защищенности информации при распределенной обработке данных.

СПИСОК ЛИТЕРАТУРЫ

1. Птицына Л. К., Птицын А. В. Расширение возможностей объектно-ориентированного анализа для обеспечения управляемого качества комплексных систем защиты информации // Информационные технологии в проектировании и производстве. 2011. № 2. С. 55-60.
2. Птицын А.В. Аналитическое моделирование комплексных систем защиты информации. Новые формализации аналитического исследования комплексных систем защиты информации / А.В. Птицын, Л.К. Птицына. Гамбург. Saarbrucken: LAP LAMBERT Academic Publishing. 2012. 293 с.
3. Птицына Л. К., Жаранова А. О. Аналитическое моделирование распределенной комплексной системы защиты информации // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 9 / СПОИСУ. – СПб., 2020. С. 284-288.
4. Птицына Л. К., Жаранова А. О. Формирование расширенной объектно-ориентированной модели комплексной системы защиты информации // Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)»: Материалы конференции. Часть 2. \ СПОИСУ. – СПб, 2020. С. 300-301.

УДК 621.391.28

ИССЛЕДОВАНИЕ ВЛИЯНИЯ РАБОТЫ ПРОТОКОЛА ARQ НА ХАРАКТЕРИСТИКИ РАДИОКАНАЛА LTE

Птицына Лариса Константиновна, Мошак Андрей Николаевич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: ptitsina_lk@inbox.ru, a.moshak@mail.ru

Аннотация. Проводится анализ работы механизма ARQ в радиоканале сети LTE. Строится модель уровня управления радиоканалом RLC архитектуры радиодоступа E-UTRAN сети LTE. Исследуется влияние работы протокола ARQ на характеристики радиоканала сети LTE с учетом длины протокольного блока уровня RLC, величины уровня ошибок и закона их распределения в радиоканале.

Ключевые слова: E-UTRAN; архитектура сети LTE; протоколы HARQ; ARQ.

RESEARCH OF IMPACT OF ARQ PROTOCOL ON LTE RADIO CHANNEL CHARACTERISTICS

Ptitsyna Larisa, Moshak Andrey
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: ptitsina_lk@inbox.ru, a.moshak@mail.ru

Abstract. The analysis of operation of the ARQ mechanism in a radio channel of LTE network is carried out. The RLC radio control layer model of the E-UTRAN radio access architecture of the LTE is constructed. Influence of ARQ protocol operation on characteristics of radio channel of LTE network is investigated taking into account length of protocol block of RLC layer, value of error level and law of their distribution in radio channel.

Keywords: E-UTRAN; LTE network architecture; HARQ protocols; ARQ**.**

Пакетная мобильная сеть связи LTE (Long Term Evolution) в настоящее время рассматриваются как наиболее перспективное направление реализации стандарта беспроводной связи поколения 4G [1-3]. Сеть LTE обеспечивает радиодоступ и мультисервисное обслуживание в пакетной форме как сервисных потоков данных SDF (*Service Data Flow*) реального времени (например, речь, видео) или потоков с гарантированной битовой скоростью передачи GBR (Guarantied Bit Rate), так и эластичных данных SDF (например, web browsing, загрузка файлов и др.) или потоков non-GBR, для которых такой гарантии сеть не дает.

При этом сетью должна обеспечиваться в сеансе связи изохронность передачи пакетов данных реального времени GBR и заданное время передачи пакетов эластичных данных non-GBR с требуемой достоверностью.

В этой связи, одной из ключевых задач, решаемых разработчиками любых систем связи (и в первую очередь систем радиосвязи) является задача обнаружения и исправления ошибок, количество которых в сотовых сетях определяется двумя факторами – внешними помехами возникающих, например, из-за шумов, помех и замирания сигнала, а также интерференцией, возникающей от передатчиков соседних базовых станций. Последний фактор является особенно важным для одночастотных систем мобильной связи LTE. Для защиты от ошибок в радиоканале, применяются методы повторной передачи искаженных или утраченных частей блоков данных.

В сети радиодоступа E-UTRAN (Evolved Universal Terrestrial Radio Access Network) сети LTE используется двухуровневая система защиты от ошибок, объединяющая

1) гибридный протокол «Автоматический запрос на повтор» Hybrid ARQ (Automatic Repeat Query), или HARQ, реализованный на физическом уровне PHY (Physical layer) архитектуры плоскости пользователя радиодоступа. Этот протокол обнаруживает и восстанавливает поврежденные блоки данных на приеме и

2) протокол «Автоматический запрос на повтор» ARQ, реализованный на уровне управления радиоканала RLC (Radio Link Control).

Этот протокол обнаруживает ошибку при приеме блока данных и задействуется для повтора невосстановленных HARQ блоков данных если ошибка не устранена.

Классический механизм ARQ предполагает автоматический запрос на повторную передачу поврежденного блока данных в случае обнаружения ошибки. При этом поврежденный блок на приемной стоне отбрасывается и запрашивается повторная передача этого же блока.

Обычно ARQ использует метод, называемый выборочной ретрансляцией, в котором приемник ожидает получение нескольких блоков данных до их подтверждения. Этот метод с одной стороны позволяет передатчику продолжать отправлять пакеты, не дожидаясь их подтверждения, а с другой стороны вносит существенную задержку в случае необходимости повторной передачи.

Следовательно, схема ARQ подходит только для потоков эластичных данных non-GBR без гарантии скорости передачи пакетов в сессии. Кроме уже упомянутой задержки, недостатком схемы ARQ является дополнительная нагрузка на канал связи, поскольку даже единичная ошибка требует повторной передачи всего пакета данных. В этой связи возникает проблема оценки повторной передачи на пропускную способность радиоканала. Чем эффективнее организован протокол повторной передачи, тем рациональнее используются радиоресурсы.

Таким образом, при построении модели логического уровня RLC архитектуры E-UTRAN кроме оценки протокольной избыточности, вносимой заголовками протокольных блоков уровня, большое значение имеет оценка влияния работы протокола ARQ на характеристики радиоканала. В этой связи точное определение таких его характеристик как распределение кратностей переспроса, достоверность, задержка, вероятность невыполнения темпа передачи информации по тракту передачи и т.д., определяющих работу протокола ARQ, является актуальной задачей.

Рассмотрим радиоканал с решающей обратной связью (РОС), в котором используются групповые (n, k) коды, обнаруживающие ошибки. Работа радиоканала происходит следующим образом. На приемном конце производится проверка блока из *n* символов. Если при этом обнаруживается ошибка, то по обратному каналу передается сигнал, требующий повторной передачи блока. Если ошибка не обнаружена, то блок считается правильно принятым, и по обратному каналу посылается сигнал, требующий передачи следующего блока информации.

Уровневая модель логического уровня RLC архитектуры плоскости пользователя радиоканала можно представить выражением [4]

$$V_{RLC}^{non-CBR} = V_{RAN} \frac{(L_{IP} - H_{IP})\,\beta_{ARQ}}{L_{IP} - H_{IP} + H_{PDCP} + H_{RLC}} \tag{1}$$

Здесь: V_{RAN} - скорость в передачи в радиоканале (бит/с); $\frac{(L_{IP} - H_{IP})}{L_{IP} - H_{IP} + H_{PDCP} + H_{RLC}}$ - протокольная избыточность, вносимая уровнем RLC; $L_{IP}, H_{IP}, H_{PDCP}, H_{RLC}$ - соответственно длина внешнего пакета данных non-GBR, поступающих на уровень PDCP и заголовков: пакета данных, протокольных блоков PDCP и RLC (бит); β_{ARQ} - коэффициент, учитывающий работу протокола ARQ на подуровне RLC и определяет издержки, связанные с дополнительной пропускной способностью радиоканала, затрачиваемую на повторную передачу ошибочных протокольных блоков данных RLC PDU.

Функционал (1) моделируют уровневое логическое соединение для передачи AM PDU RLC и определяют требуемую долю пропускной способности V_{RAN} радиоканала для их передачи. При этом, он зависят не только от необходимой для их работы служебной информации соответствующих объемов и длины протокольных блоков уровня, но и от протокола функционирования механизма ARQ организации обратной связи на уровне RLC для защиты от ошибок в радиоканале.

В [5] показано, что если распределение числа переспрашиваемых PDU RLC подчинено геометрическому закону и они не зависимы друг от друга, то для радиоканала с решающей обратной связью процесс работы механизма ARQ может быть формализован в виде:

$$\beta_{ARQ} = \sum_{k=1}^{\infty} \frac{1}{k} p_0 (1 - p_0)^{k-1} = -\frac{p_0}{1 - p_0} \ln p_0, \tag{2}$$

где p_0 - вероятность отсутствия ошибок в транспортном блоке данных подуровня MAC длины L_{RLC}. В частности, для биномиального канала с вероятностью ошибки в нем равной p , $p_0 = (1-p)^{L_{RLC}}$. Для каналов с группирующимися ошибками выражение для p_o может быть получено, например, из работ [6,7].

В докладе исследуется влияние протокола ARQ на пропускную способность радиоканала сети LTE в модели логического уровня RLC. Приводится зависимости β_{ARQ} от длины PDU RLC L_{RLC}, бит при различных значениях вероятности ошибки в нем p , Показано, например, что при $p = 1 \times 10^{-3}$ увеличение длины PDU RLC от $L_{RLC} = 1 \times 10^3$ (бит) до $L_{RLC} = 1 \times 10^4$ (бит) значение коэффициента β_{ARQ} уменьшается от $\beta_{ARQ} = 0.43$ до $\beta_{ARQ} = 0{,}03$, т.е. количество переспросов увеличивается и может блокировать систему. В радиоканалах высокого качества (например, $p = 1 \times 10^{-7}$ механизм ARQ практически не влияет на пропускную способность радиоканала в широком диапазоне длин PDU RLC: от $L_{RLC} = 1 \times 10^4$ (бит) до $L_{RLC} = 1 \times 10^6$ (бит).

СПИСОК ЛИТЕРАТУРЫ

1. Ghosh A. Fundamentals of LTE / A. Ghosh, J. Zhang, J.G. Andrews, R. Muhamed. – USA: Prentice Hall, 2010. – 464 p.
2. Dahlman E. 4G: LTE/LTE-Advanced for Mobile Broadband, Second Edition /E.Dahlman, S. Parkvall, J. Skold. – [2nd Edition] – Academic Press, 2013. – 544 p.
3. Sesia S., Toufik I., Baker M. LTE - the UMTS long term evolution. –John Wiley, 2015. – 752 p. https://en.m.wikipedia.org/wiki/E-UTRA
4. Мошак Н.Н., Птицына Л.К., Давыдова Е.В., Рудинская С.Р. МЕТОД РАСЧЕТА ОСНОВНЫХ ЧИСЛОВЫХ ХАРАКТЕРИСТИК ИНФОТЕЛЕКОММУНИКАЦИОННОЙ ТРАНСПОРТНОЙ СИСТЕМЫ СЕТИ LTE // Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 6 / СПОИСУ. – СПб., 2019. – 446 с. ISBN 978-5-907223-38-7.
5. Птицына Л.К. Мошак А.Н. МОДЕЛЬ ПРОТОКОЛА ARQ В РАДИОКАНАЛЕ СЕТИ LTE. Региональная информатика (РИ-2020). XVII Санкт-Петербургская международная конференция «Региональная информатика (РИ-2020)». Санкт-Петербург, 28-30 октября Р32 2020 г.: Материалы конференции. Часть 2. \ СПОИСУ. – СПб, 2020. – 335 с. ISBN 978-5-907223-86-8, с. 302-303
6. Л.П.Пуртов, А.С.Замрай, А.И.Захаров. Основные закономерности распределений ошибок в дискретных каналах связи, «Электросвязь» №2, 1967, с.1-8
7. Элементы теории передачи дискретной информации, под редакцией Л.П.Пуртова. М., «Связь», 1972. С.232 с илл.

УДК 004.057.5

РАЗРАБОТКА СТРУКТУРЫ ВЕБ-ИНТЕРФЕЙСА ДЛЯ СИСТЕМЫ АНАЛИЗА ТРАФИКА БЕСПРОВОДНОЙ СЕТИ

Фёдорова Анастасия Эдуардовна, Герлинг Екатерина Юрьевна, Ахрамеева Ксения Андреевна, Андрианов Владимир Игоревич

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: fyodorova.aaee@gmail.com, gerlingeu@gmail.com, cbor.mail@gmail.com, vladimir.i.andrianov@gmail.com

Аннотация. Рассматриваются инструменты для разработки веб-интерфейса системы анализа трафика беспроводной сети, развёрнутой на маломощном устройстве, а именно уделяется внимание выбору веб-сервера, внутреннего языка программирования базы данных и средств обеспечения информационной безопасности приложения.

Ключевые слова: веб-интерфейс; беспроводные сети; система мониторинга.

WEB INTERFACE STRUCTURE DEVELOPMENT FOR WIRELESS NETWORK TRAFFIC ANALYSIS SYSTEM

Fedorova Anastasia, Gerling Ekaterina, Akhrameeva Ksenia, Andrianov Vladimir

The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: fyodorova.aaee@gmail.com, gerlingeu@gmail.com, cbor.mail@gmail.com, vladimir.i.andrianov@gmail.com

Abstract. The paper considers tools for developing a web interface for a wireless network traffic analysis system deployed on a low-power device, namely, attention is paid to the choice of a web server, an internal database programming language and information security tools for the application.

Keywords: web interface; wireless networks; monitoring system.

Веб-приложения уже давно плотно укоренились в жизни современного человека. Главным преимуществом таких приложений является возможность их использования без необходимости установки дополнительного программного обеспечения, так как вся работа происходит с помощью браузера.

Среди других положительных качеств можно выделить отсутствие необходимости обновлений на рабочем месте пользователя и хранение основных файлов конфигурации на сервере, что упрощает создание резервных копий и сохранение безопасности данных [1].

Вследствие этого всё больше пользователей прибегают к использованию веб-интерфейса для управления и настройки различных сетевых устройств, таких как маршрутизаторы [2], модемы, видеокамеры. К числу устройств данного типа может относиться система анализа трафика беспроводной сети, обладающая крайне ограниченными ресурсами.

Поскольку существующий код системы анализа трафика беспроводной сети написан для применения на одноплатном компьютере Raspberry Pi 3 Model B [3], то при разработке веб-интерфейса данной системы требуется учитывать ряд особенностей устройств этого типа, а именно ограничение в энергопотреблении, небольшой запас постоянной памяти, отсутствие возможности увеличить оперативную память и медленную скорость работы.

Для разработки структуры веб-интерфейса была выбрана операционная система Ubuntu Server, веб-сервер Apache HTTP-сервер, база данных MySQL и внутренний язык программирования PHP [4].

Концепция полученного решения подразумевает страницу для авторизации пользователя с необходимостью вводить логин и пароль, журнал логов, в котором отображаются зафиксированные системой анализа трафика аномалии и время их обнаружения [5], а также раздел с возможностью создавать дамп трафика беспроводной сети, который будет поддерживать функцию сохранения полученного пользователем дампа на персональный компьютер [6].

СПИСОК ЛИТЕРАТУРЫ

1. Герлинг, Е.Ю., Горлов, С.Е., Кириллов, Д.И. Обеспечение информационной безопасности при разработке web-приложений // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 326-330.
2. Александрова Е.С., Ковцур М.М. Разработка модели нарушителя в беспроводных сетях стандарта IEEE 802.11 // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. Санкт-Петербург. 2017. С. 24-28.
3. Габуев А.Г., Красов А.В., Ощенков Ф.Д., Тарасов Н.М. Анализ защищённости современных средств передачи информации посредством портативной лаборатории на основе микрокомпьютера Raspberry Pi // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 295-298.
4. Ахрамеева К.А., Ковцур М.М., Михайлова А.В. Обеспечение информационной безопасности баз данных web-приложений // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020). IX Международная научно-техническая и научно-методическая конференция: сборник научных статей. Санкт-Петербург, 2020. С. 107-110.
5. Ковцур М.М., Луеке П.Э. Разработка системы учёта посещаемости студентов масштаба ВУЗа // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). VIII Международной научно-технической и научно-методической конференцияи : в 4 т.. 2019. С. 532-537.

УДК 004.056.53

ПРОБЛЕМЫ БЕЗОПАСНОСТИ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ СЕТЕЙ СЕМЕЙСТВА СТАНДАРТОВ IEEE 802.11

Храмцов Дмитрий Олегович, Миняев Андрей Анатольевич, Казаков Никита Игоревич
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mails: khramtsov2010@mail.com, minyaev.a@gmail.com, kazakov.ni2.18@gmail.com

Аннотация. Рассматриваются принципы работы стандартов IEEE 802.11, а также различные атаки, которые может реализовать активный нарушитель. Определяются методы защиты для беспроводных сетей от атак.

Ключевые слова: IEEE 802.11; безопасность беспроводных сетей; методы защиты; IDS; wIPS; шифрование данных.

SECURITY ISSUES RELATED TO THE USE OF NETWORKS OF THE IEEE 802.11 FAMILY OF STANDARDS

Khramtsov Dmitrii, Minyaev Andrey, Kazakov Nikita
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mails: khramtsov2010@mail.com, minyaev.a@gmail.com, kazakov.ni2.18@gmail.com

Abstract. The principles of operation of IEEE 802.11 standards are considered, as well as various attacks that an active violator can implement. Methods of protection for wireless networks from attacks are defined.

Keywords: IEEE 802.11; wireless network security; security methods; IDS; wIPS; data encryption.

В стандарте беспроводной связи IEEE 802.11 есть как служба аутентификация, так и протокол шифрования [1], но исследования показали [2], что эти протоколы имеют серьезные недостатки. Стандарт безопасности 802.11, известный как WEP, является уязвимым для нескольких типов атак. Поскольку WEP имеет серьезные недостатки, Wi-Fi Alliance создал новый протокол, IEEE 802.11i, для устранения всех уязвимостей протокола безопасности 802.11.

Разработчики стандарта рекомендовали использовать стандарт управления доступом к сети на основе ролей IEEE 802.1X в качестве временной меры для удовлетворения требований безопасности сетей WLAN) и сохранения подлинности, конфиденциальности, и доступности данных до тех пор, пока полностью не разработается новая спецификация безопасности WLAN. В конце 2003 года Wi-Fi Alliance выпустил проект спецификации RSN [3], также называемая WPA2. Однако, в 2017 году в протоколе WPA2 была обнаружена серьезная уязвимость [4], получившая название KRACK– атака с переустановкой ключа. Этот факт, наряду со всеми ранее известными недостатками WPA2, подтолкнул Wi-Fi Alliance к разработке нового стандарта безопасности - WPA3. Wi-Fi уже давно стал неотъемлемой частью жизни миллионов людей, а с появлением IoT (Internet of Things) число беспроводных устройств во всем мире постоянно растет, поэтому вопросы защиты Wi-Fi сетей не теряют своей актуальности. Предыдущая версия протокола WPA2 была введена в 2004 году и за последние несколько лет неоднократно была дискредитирована. По этой причине в июле 2018 года Wi-Fi Alliance объявил о начале сертификации устройств, поддерживающих WPA3 - самого большого обновления безопасности за последние 14 лет [5]. Массовое внедрения данного протокола безопасности произойдет в течение нескольких лет.

DoS-атаки вынуждает компании производителей оборудования и программного обеспечения модифицировать свои системы. Впоследствии компании выпустили программное обеспечение для защиты от вирусов и систему обнаружения вторжений (IDS) для защиты от атак с использованием искаженных и вредоносных пакетов. Также были сделаны беспроводные системы предотвращения вторжений (wIPS) [6]. Для управления входящими и исходящими пакетами были разработаны различные типы межсетевых экранов с целью защиты от несанкционированного доступа.

Таким образом, удобство беспроводных локальных сетей (WLAN) привело к распространению технологии WLAN на сетевом рынке, особенно в промышленном и военном секторах. Поскольку сети на основе 802.11 широко используются дома, в правительстве и в армии, они также являются привлекательными целями для различных атак, в том числе DoS-атак.

СПИСОК ЛИТЕРАТУРЫ

1. Таненбаум Э. С. Компьютерные сети/Э. С. Таненбаум, Д. Уэзеролл;[пер. с англ. А. Гребеньков].-5-е изд //Санкт-Петербург [и др.]: Питер. – 2012.
2. Yeh J. H., Chen J. C., Lee C. C. WLAN standards //IEEE Potentials. – 2003. – Т. 22. – №. 4. – С. 16-22.
3. Frankel S. et al. Establishing wireless robust security networks: a guide to IEEE 802.11 i //NIST Special Publication. – 2007. – С. 800-97.
4. Fehér D. J., Sandor B. Effects of the WPA2 KRACK attack in real environment //2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY). – IEEE, 2018. – С. 000239-000242.
5. Koziol M. Wi-Fi gets more secure: Everything you need to know about WPA3 //IEEE Spectrum: Technology, Engineering, and Science News. – 2018.
6. Agalit M. A. et al. Hybrid Intrusion Detection System for Wireless Networks //WITS 2020. – Springer, Singapore, 2022. – С. 507-513.

УДК 004.418

АНАЛИЗ МЕТОДОВ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ МОБИЛЬНЫХ УСТРОЙСТВ С ИСПОЛЬЗОВАНИЕМ ПОВЕДЕНЧЕСКИХ АЛГОРИТМОВ

Шабарова Виктория Александровна
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия
e-mail: vikashabarova@mail.ru

Аннотация. В данной статье представлен обзор методов идентификации пользователей на основе поведенческих алгоритмов. Актуальность данной темы заключается в ненадежности и рискованности методов биометрической аутентификации. Нетрадиционные методы поведенческой биометрии могут выступать достойной и более надёжной альтернативой традиционной биометрии.

Ключевые слова: идентификация пользователя; поведенческие алгоритмы; несанкционированный доступ; поведенческий анализ; бихевиоральные паттерны; биометрическая аутентификация.

THE ANALYSIS OF MOBILE DEVICE USER IDENTIFICATION METHODS USING BEHAVIORAL ALGORITHMS

Shabarova Viktoriia
The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia
e-mail: vikashabarova@mail.ru

Abstract. This article provides an overview of user identification methods based on behavioral algorithms. The relevance of this topic lies in the unreliability and riskiness of biometric authentication methods. Unconventional methods of behavioral biometrics can act as a worthy and more reliable alternative to traditional biometrics.

Keywords: user identification; behavioral algorithms; unauthorized access; behavioral analysis; behavioral patterns; biometric authentication.

В настоящее время существует множество различных алгоритмов проверки подлинности введённых данных. Одними из самых широко используемых механизмов являются: традиционные биометрические модальности [1, 2], нетрадиционные биометрические модальности, мультимодальности, однофакторная аутентификация, многофакторная аутентификация, цифровые сертификаты и ЭЦП.[2] Объектом исследования являются биометрические методы идентификации. Предметом исследования является мультимодальная нетрадиционная биометрия и её преимущество над традиционной модальностью. Актуальность темы заключается в доказанной слабости и рискованности методов биометрической аутентификации, альтернативой которой служит, выдвигаемая мировыми трендами, поведенческая биометрия. Поведение каждого человека уникально. [1, 3]

Для того чтобы аутентифицировать пользователя по биометрическим характеристикам не требуется привлечение дополнительных документов и запоминание информации.

Основные проблемы классической биометрии.

Идентификация пользователя осуществляется только на определённом этапе взаимодействия.

Требует внедрения дополнительных устройств.

Основана на внешних (видимых) физиологических характеристиках.

Анализ поведения пользователей и выявления аномалий в их поведении может стать отличной альтернативой классической биометрии. Нейросети способны отождествлять пользователя с конкретной личностью по множеству критериев сразу, что делает поведенческую биометрию мультимодальной.

К примеру [4]:

- По наличию сохранённых файлов Cookie;
- По тенденции к посещению значимых сайтов;
- По анализу динамики электронной подписи;
- По анализу работы с клавиатурой и мышью (на ПК);
- По клавиатурному почерку (на смартфонах);
- По походке.

Поведенческую биометрию также называют пассивной, поскольку пользователям не нужно совершать каких-либо дополнительных действий. Преимуществами поведенческих алгоритмов являются: непрерывная идентификация, незаметна для пользователей, альтернатива для методов многофакторной аутентификации, сложность компрометации алгоритма со стороны злоумышленников.

СПИСОК ЛИТЕРАТУРЫ

1. Анисимов Р. Идентификация по нажатию клавиш: системы безопасности учатся анализировать поведение пользователей. [Электронный ресурс] // Журнал Forbes. АО "АС РУС МЕДИА", 04.05.2017. URL: https://www.forbes.ru/tehnologii/342733-identifikaciy (дата обращения 07.05.2021)
2. ГОСТ Р 54411-2018/ISO/IEC TR 24722:2015. БИОМЕТРИЯ. Мультимодальные и другие мультибиометрические технологии. Information technology. Biometrics. Multimodal and other multibiometric fusion (2018). // НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ

ФЕДЕРАЦИИ. Москва: Стандартинформ, 2018
3. Савинова В.М., Бесхмельницкий А.А., Бибина Е.С., Осадчая А.Д. Идентификация пользователей корпоративной системы с помощью поведенческого анализа с использованием модели искусственной нейронной сети [Электронный ресурс] // ТДР. 2017. №5. URL: https://cyberleninka.ru/article/n/identifikatsiya-pol (дата обращения: 07.05.2021).
4. Юрасов Д.С., Зикратов И. А. Различение пользователей на основе их поведения в сети Интернет [Электронный ресурс] // Научно-технический вестник информационных технологий, механики и оптики. 2013. №6 (88). URL: https://cyberleninka.ru/article/n/razlichenie-polzova (дата обращения: 08.05.2021).
5. Zanna K., King S., Neal T., Canavan S. Studying the Impact of Mood on Identifying Smartphone Users. [Электронный ресурс] // Department of Computer Science and Engineering University of South Florida, Tampa, FL USA. 27.07.2019. URL https://www.researchgate.net/publication/334129925_St (дата обращения 08.05.2021).

ОГЛАВЛЕНИЕ

CONTENTS