УФИМСКИЙ УНИВЕРСИТЕТ

приоритет2030^
лидерами становятся

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ

Материалы VIII Всероссийской молодежной научно-практической конференции с международным участием (г. Уфа, 23–24 мая 2025 г.)

Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Уфимский университет науки и технологий»

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ

Материалы
VIII Всероссийской молодежной научно-практической конференции с международным участием
(г. Уфа, 23–24 мая 2025 г.)

Научное электронное издание сетевого доступа

Уфа
Уфимский университет
2025

УДК 004.9
ББК 32.973-0812
И74

Публикуется по решению кафедры управления информационной безопасностью УУНиТ.
Протокол № 10 от 14.05.2025 г.

Редакционная коллегия:
канд. физ.-мат. наук **Д.С. Юнусова** (*отв. редактор*);
д-р техн. наук, профессор **М.Б. Гузаиров**;
д-р техн. наук, профессор **С.С. Валеев**;
д-р физ.-мат. наук, доцент **А.С. Исмагилова**;
канд. физ.-мат. наук, доцент **И.А. Шагапов**;
канд. биол. наук **Ф.Т. Байрушин**;
канд. филос. наук **Н.Г. Миронова**;
канд. юрид. наук, доцент **Р.М. Яппаров**;
канд. хим. наук **А.А. Корнилова**;
ст. преподаватель **И.В. Салов**;
ст. преподаватель **А.Ф. Фатхелисламов**

И74 **Информационные технологии обеспечения комплексной безопасности в цифровом обществе**: материалы VII Всероссийской молодёжной научно- практической конференции с международным участием (г. Уфа, 23–24 мая 2025 г.) / отв. ред. Д.С. Юнусова [Электронный ресурс] / Уфимск. ун-т науки и технологий. – Уфа: Уфимский университет, 2025. – 325 с. – URL: https://uust.ru/media/documents/digital-publications/2025/147.pdf – Загл. с титула экрана.
ISBN 978-5-7477-6144-5

Представлены статьи, подготовленные в рамках основных направлений работы конференции: математические модели и методы защиты, преобразования и передачи информации; организационно-правовые аспекты защиты информации; концепция и методы инженерно-технического обеспечения безопасности; цифровая экономика: вызовы, угрозы, перспективы; обеспечение национальной безопасности в условиях информационных войн.

Сборник представляет интерес для преподавателей, аспирантов, студентов и всех, кто интересуется актуальными исследованиями в сфере проблем информационной безопасности современного общества.

УДК 004.9
ББК 32.973-0812

ISBN 978-5-7477-6144-5 © Уфимский университет, 2025

СОДЕРЖАНИЕ

ПЛЕНАРНЫЕ ДОКЛАДЫ И ВЫСТУПЛЕНИЯ ЭКСПЕРТОВ
Байрушин Ф.Т. Автоматизация управления информационной безопасностью 8
Валеев С.С., Гузаиров М.Б. Генеративные многоагентные системы и задачи защиты информации на базе концепции нулевого доверия 13
Исмагилова А.С. Криптографические аспекты изоморфизма групп обратимых элементов 18
Корнилова А.А., Гиззатова Э.Р. Математическое моделирование временного ряда количества скомпрометированных персональных данных в мире 21
Кузнецова Е.В., Сенцова А.Ю. Применение машинного обучения в системах обнаружения вторжений для V2X-систем 25
Новикова Д.Д. Основные угрозы для детей в интернете и способы защиты 28
Ожгибесова А.С., Шабуров А.С., Южаков А.А. О разработке метода оценки рисков информационной безопасности 32
Шагапов И.А., Салов И.В. Об одном математическом подходе к построению систем защиты информации 36
Юнусова Д.С., Султанов Д.Ж. Нейросетевой анализ URL-адресов для выявления фишинговых атак 39
Яковец Е.Н. Некоторые вопросы применения новых информационных технологий в сфере противодействия терроризму 42
Яппаров Р.М. К вопросу о совершенствовании системы защиты информации в организации 47
СЕКЦИЯ 1. МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ ЗАЩИТЫ, ПРЕОБРАЗОВАНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ
Аетбаева Р.Г., Файзуллина А.С. Обнаружение мошеннических транзакций с использованием методов машинного обучения 52
Аминев Б.Р., Бурангулов Д.Б. Выявление вредоносного программного обеспечения для сбора информации в операционной системе компьютера 55
Аникин С.А. Применение метода Хольта-Винтерса для прогнозирования количества сетевых атак 60
Гаврилова А.А., Мусина К.Ш. Определение и обнаружение DDoS-атак с использованием методов машинного обучения 63
Галимова А.Р., Домрачева В.Е., Шарафутдинов Б.И., Ямилова А.Р. Особенности квантовых методов криптографии: принципы, реализация и перспективы 67
Галиуллин Р.Р., Кулдавлетов А.И. Разреженность данных и сжатие размерности 70
Ганиев М.Р., Ефимов И.О., Каримуллин Т.Ф. Современные методы совершенствования информационной безопасности 74

Драгунский Н.С., Хусамов Р.Р., Ганиев Ш.И., Шилин С.В. Анализ эмоциональной окраски текста с использованием модели DistilBERT .. 77
Иванов И.П., Хасанов Р.Р., Ишмаков Т.М. Технологии обеспечения информационной безопасности 80
Ишбаева А.Э., Мансурова А.Р., Сысоева А.В. Проблемы защиты персональных данных в эпоху больших данных 84
Ишмухаметов И.Р., Чернышев К.В. Обнаружение троянских программ88
Ляпустин Е.М., Ахметзянов Д.И., Баязитов Т.Т. Моделирование процессов и систем защиты информации 91
Пуйко Д.Д. Проблемы многофакторной аутентификации в децентрализованных киберфизических системах 95
Резбаев В.М. Математическое моделирование временного ряда похищенных записей персональных данных в мире 99
Шамсутдинов Б.С. Методы защиты QR-кодов от подделки 103
СЕКЦИЯ 2. СОВРЕМЕННЫЕ ВЫЗОВЫ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ
Агапова В.О. Анализ методов скрытия вредоносных приложений 106
Агапова В.О. Использование шифрования, защищенной памяти и KeyStore API для защиты данных в мобильных приложениях 110
Алейникова Д.И. Методика конфигурации SIEM-систем для обнаружения аномальных действий в корпоративной сети 114
Александрова В.М. Меры защиты конфиденциальной информации при взаимодействии сотрудников со сторонними организациями 118
Ализода С.С. Роль искусственного интеллекта в обеспечении сетевой безопасности 121
Ализода С.С. Эволюция киберугроз: как меняются методы атак на компьютерные сети 125
Ахмадиева Виола Ф., Ахмадиева Вилена Ф. Использование искусственного интеллекта для автоматизированного обнаружения и предотвращения кибератак на мобильные устройства 128
Ахмадиева Виола Ф., Ахмадиева Вилена Ф. Безопасность мобильных устройств: анализ угроз и методы защиты 132
Ахмадуллин Р.А. Использование нейросетей для обеспечения информационной безопасности на предприятии 136
Белов И.А. Политика в сфере информационной безопасности в России, США, Китае и ЕС 140
Галяутдинов Р.Р. Способы управления рисками с помощью искусственного интеллекта 144
Давлетшин Б.М. Метод нулевого доверия (Zero Trust) между людьми как ответная мера на распространение применения искусственного интеллекта для телефонного мошенничества 148
Дмитриева М.В. Эволюция кибератак на критическую инфраструктуру152
Драганова Д.В. Стратегия Евросоюза в области искусственного интеллекта: скоординированный план и национальные подходы 156

Загиров Р.А. Защита информации от целевого фишинга в автоматизированной системе 160
Зыков А.И. Применение методов искусственного интеллекта и машинного обучения для защиты критической информационной инфраструктуры от сетевых атак 163
Клыгин В.О. Децентрализованные идентификаторы (DIDs) как основа беспарольной аутентификации и устранение рисков централизованного хранения данных 168
Кудакаев И.Ф., Ракипов Д.А. Обнаружение спама в email 172
Мухаметшина Р.А. Оптимизация сигнатурного анализа с использованием битовых масок: сравнительное исследование 176
Николаев Ю.А. Угрозы информационной безопасности государственных муниципальных учреждений 180
Панов Н.С. Повышение безопасности VPN-сервера с помощью двухфакторной аутентификации 183
Полышева А.К. Применение современных технологий с использованием алгоритмов машинного обучения для повышения эффективности системы защиты информации 186
Савелиев Я.И. Опыт внедрения РЕД ОС в ПГУТИ, подходит ли он для решения задач информационной безопасности? 190
Ситков А.С. Как злоумышленники используют генеративный ИИ для сложных кибератак и перспективные механизмы защиты/противодействия подобным атакам 194
Фатеев Р.Р., Шигапов А.В. Выявление потенциальных угроз со стороны внутренних пользователей на основе их действий и истории работы .. 198
Хафизова Л.Ф. Современные угрозы и уязвимости информационной безопасности в области организационной защиты .. 202
Шайнурова А.Г. Расследование инцидентов с помощью искусственного интеллекта 206
Шушакова А.А. Некоторые новые виды атак на мобильные и IoT-устройства с применением технологий машинного обучения и противодействие им 210
Якупова И.Р. Проблемы безопасности IoT-устройств и направления защиты интернета вещей 213
Янов И.В. Основные угрозы и уязвимости веб-сайтов и методы защиты от них 217
СЕКЦИЯ 3. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ
Аскарова Г.Ф. Технологии защиты информации 222
Биктубаева К.С. К вопросу об обеспечении информационной безопасности объектов критической информационной инфраструктуры ……..... 226
Журавлева Ю.О. Отношение молодежи к безопасности персональных данных 230

Казанцев В.А. Обеспечение информационной безопасности при удаленной работе 233
Каримова А.Р., Эгит Д.О., Кагарманов Д.Э. Особенности расследования инцидентов информационной безопасности в системах искусственного интеллекта 236
Кириллов В.С. Модели угроз и построение систем защиты в корпоративных автоматизированных системах 240
Набиев Д.Т. Защита электронного документооборота в организации на базе платформы Docsvision 243
Насифуллина Э.И. Анализ соответствия существующих средств защиты информации требованиям ГОСТ при создании АС в защищенном исполнении 247
Резбаева В.М. Изменения в законодательстве об ответственности за утечку персональных данных 251
Рябова К.А. О необходимости применения программ безопасного поведения и культуры ИБ (SBCP) 255
Хайруллина Г.Ф. Использование ViPNet EDI в системах электронного документооборота 259
СЕКЦИЯ 4. КОНЦЕПЦИЯ И МЕТОДЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
Ахметов У.Р. Поддержка двухфакторной аутентификации (2ФА) в инфраструктуре Samba AD 263
Биктубаева К.С. Адверсарные атаки на Zero Trust-системы: уязвимости и методы защиты 267
Давлетова Д.Р. Построение модели дублирования подсистем в защите информации 272
Давлетшина Э.В. Использование RSA-ключей для авторизации 277
Загидуллина А.У. Шифрование электронной почты для личного пользования 281
Зайнуллин Б.И., Масальский Н.В. Обезличивание персональных данных как метод защиты 285
Ибрагимова А.Р. Анализ эффективности и повышение производительности проводного канала передачи данных в компьютерных сетях 289
Ибрагимова А.Р. Актуальность применения систем класса Deception для защиты предприятия от современных киберугроз 294
Ижболдина Т. К. Особенности обеспечения информационной безопасности в условиях удаленной работы 297
Искужина Э.Р. Методы и программы для выявления подслушивания сетевого трафика 302
Набиева А.И. К вопросу о совершенствовании системы технической защиты информации 306
Тактаев Т.У. Приватность в мессенджерах: насколько защищены наши переписки? 310

Хафизова А.Э. Исследование и оценка защищенности беспроводных сетевых соединений 314
СЕКЦИЯ 5. ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ИНФОРМАЦИОННЫХ ВОЙН
Бильданов С.З., Попов А.А. Современные вызовы в области обеспечения информационной безопасности 318
Ларичев Р.С. Искусственный интеллект в информационных войнах: угрозы и возможности для государств 321

ПЛЕНАРНЫЕ ДОКЛАДЫ И ВЫСТУПЛЕНИЯ ЭКСПЕРТОВ

УДК 004

Байрушин Ф.Т.
Уфимский университет науки и технологий, Уфа

АВТОМАТИЗАЦИЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Аннотация. В статье рассмотрены вопросы о назревшей необходимости автоматизации информационной безопасности на предприятии, особенности подхода к автоматизации в области управления информационной безопасности как процессу, рассмотрены уровни функционального персонала предприятия, нуждающихся в автоматизации своих функциональных, штатных процедур. Рассмотрены вопросы направленности процесса на предприятии. Затронуты некоторые системы автоматизации в области ИБ, такие как СиММА и автоматизации в области ИБ.

Ключевые слова: открытый исходный код, проприетарное программное обеспечение, метрика, скрипт, платформа автоматизации.

На сегодняшний день созрели все условия для автоматизации в области ИБ, поскольку рутинные процедуры, выполняемые специалистами ИБ, с каждым годом количественно только нарастают. Небезызвестно, что рутина в любом рабочем процессе, занимая порой все рабочее время, поглощает сотрудника как личность, подавляет творческую активность, так скажем угнетает креативную составляющую, как творческих групп, так и всего предприятия, мешает выстраивать необходимые мероприятия по коррекции своих действий во все быстрее и быстрее меняющемся в информационном мире. Скажем так – хочешь, чтобы рабочая структура перестала функционировать в области прямого своего назначения – завали ее отчетной рутиной. Так в свое время нейтрализовал девятый технический отдел разведки Великобритании МИ-6, завалив своих подчиненных рутинным составлением всевозможных отчетов и прочих бумаг, Георг Блэйк, который являлся одновременно резидентом внешней разведки СССР в период проведения нашей контрразведкой операции «Берлинский тоннель» в 1953 г., обеспечив полное фиаско чаяниям разведки противника [1].

Покажем три уровня, нуждающиеся в уходе от рутины с помощью автоматизации:

1. Уровень инженеров. Люди, работающие руками, например, создающие виртуальные машины. Когда количество создаваемых виртуальных машин достигает до нескольких десятков в день, то на их создание требуется огромное количество рабочего времени. Инженер начнет

использовать Antibl, напишет один раз Скрипт- и будет «разливать» эти виртуальные машины.

2. Уровень руководства. Средний менеджмент в тот момент, когда одна и та же задача постоянно разрастается, масштабируется и привлекает все большее количество людей, порой до нескольких сот единиц для ее решения, а именно- вовремя набирать отчеты по требованию топ-менеджмента. Что бы решить такого рода разрастающуюся проблему и необходима автоматизация.

3. Уровень топ менеджмента. Несвоевременность выполнения запросов, отчетов из-за больших объемов работ требуют автоматизации этих процессов.

Рассмотрим ситуацию. Если у компании есть какое-то решение или компания берется решать какие-то свои задачи самостоятельно изнутри, то она начинает использовать Open Source – открытый исходный код – модель разработки программного обеспечения, где исходный программный код доступен для открытого просмотра в отличие от закрытого, проприетарного программного обеспечения, которое является собственностью разработчика и не доступно для просмотра посторонними, тогда появляется необходимость в том, чтобы все эти внутренние разработки были безопасными, а анализ кода, все процессы с DLP- они так или иначе завязаны на автоматизацию, потому что иначе человеку «вручную» проверить все это невозможно.

Заметим, автоматизация впрок абсурдна, процесс должен быть воспроизводим не единожды, случись иначе, получится только автоматизированный хаос. Если процесс воспроизведен не раз, то процесс формализуем, и если его можно разложить по шагам, то его вероятно можно автоматизировать, не факт, что это будет эффективно, но пригодность автоматизированных процедур будет налицо.

Для автоматизации подобных процессов уже успешно используется СиММА – система многослойного моделирования, каталогизации и структуризации данных, согласно архитектуре предприятия с отражением ее в виде цифровых различных объектов реальности инженерной, организационной и программной природы, а также автоматизация обработки рисков.

СиММА разработана российскими специалистами, согласно программе по импортозамещению, а именно, замены импортного продукта VISIO [2].

Подходя к вопросу автоматизации, нужно подразумевать не бесконечное множество инцидентов, что могут произойти в инфраструктуре, а выделить недопустимые ключевые события, которые могут произойти, например хищение денежных средств со счетов, оборотные штрафы в результате утечки персональных данных, и далее смоделировать ситуацию возможной или невозможной реализации этого риска. Если есть возможность верифицировать, то есть, выявить высокую вероятность реализации риска, соответственно, можно спроектировать такую

автоматизированную систему безопасности, которая позволит этот риск устранить. Если это возможно, то можно говорить, что автоматизация необходима.

Автоматизация может происходить либо сверху вниз, либо снизу вверх.

Когда происходит автоматизация рутинных операций, то автоматизирование идет снизу вверх, например, проявилась проблема – написали скрипт и автоматизировали, проявилась еще одна проблем – написали скрипт и автоматизировали, потом пишется скрипт, который автоматизировал скрипты, написанные ранее, и появляется большая «гора скриптов», сложно поддерживаемая.

Но если автоматизация происходит сверху вниз, процесс развивается упорядочено, согласно разработанной стратегии, плану, проекту. Автоматизация процесса целиком – задача, цель которой не автоматизировать ради автоматизации, а достичь определенной цели, например реализовать проверки технических и организационных мер. Определить из чего состоит этот процесс и анализ, что в этом процессе можно автоматизировать на основе комплексного решения, которое по реализации выдает итог: автоматизирован контроль проверок [3].

Но при автоматизации снизу вверх картина получается несколько другая. Если автоматизировать какой-то кусочек, потом трудно будет найти место, куда его еще можно интегрировать, где он принесет пользу.

Регулярно все замечательные инициативы сверху с точки зрения пересмотра процессов рушатся из-за отсутствия четкого целеполагания, то есть определения характера и направленности действий внутри организации, обусловленных показаниями метрик, и если имеется возможность снимать метрики и построить дерево метрик, то можно легко определить на какую бизнес – метрику будет направлена централизованная автоматизация [4].

И все-таки, на практике чаще всего происходит автоматизация рутины, потому что наверху по тем или иным причинам не получается перераспределить или перепроектировать работающий, приносящий уже определенный результат, процесс. К тому же аналитик, уставший от рутинного однообразия измерения метрик, может подойти снизу, автоматизировав такой процесс.

Так что же понимается под платформами автоматизации, какие средства необходимы для этого. Автоматизация ИБ довольно-таки разнообразна и вот одна из систем:

– SGRC (Security Governance, Risk Management and Compliance) – Система управления безопасностью, рисками и соответствием законодательству. То есть, фактически, SGRC – это система для автоматизации построения комплексной системы управления информационной безопасностью (СУИБ). Системы SGRC включают в себя три основных подхода к построению СУИБ:

1. Governance. Управление, руководство – управление информационной безопасностью директоратом компании, который на основе полученных данных о системе управления информационной безопасностью, обработанных программным комплексом SGRC, вырабатывает бизнес - обоснованные директивы.

2. Risk Management. Управление рисками – создание высокого уровня информационной безопасности за счет проведения мероприятий, призванных эффективно исключать уязвимости и минимизировать риски системе ИБ.

3. Compliance. Соответствие, т.е. исключение инцидентов, связанных с нарушением законодательных предписаний, установленных государством, корпоративных стандартов и соблюдения политик и режимов на предприятии, развитие которых приводит к потере репутации, незапланированным затратам, штрафам, выставляемым со стороны контролирующих организаций.

Системы SGRC призваны для автоматизации процесса строительства СУИБ и настроены, прежде всего, на автоматизацию процессов информационной безопасности и ограниченно на ИТ-процессы. В функции SGRC-систем входят:

– управление ИТ-активами;

– управление рисками ИБ;

– документальную обработку инцидентов ИБ (поддержку расследования инцидентов ИБ, протоколирование, накопление базы знаний);

– соответствие нормативным требованиям информационной безопасности- законодательным, отраслевым, корпоративным;

– поддержку проведения внутренних аудитов ИБ и самооценок;

– управление процессами обеспечения непрерывности бизнеса и восстановления работоспособности;

– построение отчетности и дашбордов с функционалом drill-down (возможность «проваливаться» вглубь предоставляемой информации для получения детальных сведений по элементам отчета) [5].

Кроме систем SGRC, которые ориентированы на управление и обеспечение информационной безопасности, существуют неспециализированные системы GRC (Governance, Risk Management and Compliance), которые могут быть сфокусированы на управлении финансами, ИТ, бизнес-рисками. Функционал таких GRC-систем общего назначения включает в себя:

– управление политиками, аудитами и рисками;

– автоматизацию соответствия законодательству;

– управление документами и версиями;

– управление взаимоотношениями с поставщиками и контрагентами

– контроль доступа и полномочий;

– мониторинг бизнес-процессов;
– построение отчетности и диаграмм/графиков/дашбордов.

Платформы SGRC используется для накопления и анализа данных, явлений, относящихся к области информационной безопасности, нормативным и законодательным документам в отношении построения мероприятий по защите информации на предприятии, к процессам функционирования информационной структуры предприятия. Данные для обработки SGRC поступают от автоматизированных систем, таких как ERP (Enterprise Resource Planning), которая призвана быть единым центром на предприятии для обработки поступающих данных от ответственных за определенные процедуры, таких как составление отчетов на основе результатов, полученных при проведении очередного или внепланового аудита, и хранения полученной и обработанной информации, противодействует дублированию получаемых данных, нивелирует до минимума предпосылки ошибок, и которая просто объединяет всевозможные слагаемые предприятия, такие как реализация и сбыт продукции, разработка и производство, финансовая деятельность, управление личным составом в единый информационный кластер. Таким образом, чем больше процедур в области информационной безопасности с применением подобного рода программных информационных систем получится подвести под автоматизацию, тем больше освободившегося персонала можно занять на решение других немаловажных, ключевых вопросах информационной безопасности, за счет уменьшения уровня занятости на каком-то определенном, рутинном вопросе. Давно замечено, если дело касается рутинных занятий, таких как мониторинг, требующих высокой точности измерений, человек на современном этапе развития технологий все более замещается автоматами, тем самым исключается риск получения ошибочных, не соответствующих реальному состоянию исследуемой среды данных, исключается так называемый человеческий фактор. И чем более расширенно будет осуществляться автоматизированный сбор данных для SGRC-системы. чем более эти данные будут соответствовать действительному положению дел по состоянию ИБ на предприятии, и тем более реальные результаты, полученные вследствии мониторинга системы безопасности, будут отражаться в отчетах по аудиту, тем более правильными будут приниматься решения высшим руководством фирмы, в отношении реагирования на инциденты, выработки корректирующих процедур, положений по совершенствованию информационной безопасности. И чем больше будет использовано ИТ-систем для предоставления данных для SGRC, при помощи которой будет выстроена система управления ИБ, тем более она будет выверена [2].

И все же, это вопросы частные, что касается общего, то при наличии дефицита специалистов ИБ, не говоря уже о высокопрофессиональных, появление все новых и новых преступных кибертехнологий и методов и,

соответственно, стремительного возрастания загруженности персонала, вопросы по автоматизации ИБ являются жизненно важными и необходимость в этом будет только возрастать.

Список использованных источников:

1. Биография советского разведчика Джорджа Блейка: URL: https://tass.ru/info/10359633.
2. Система многослойного моделирования архитектуры: URL: https://bm-symma.ru/?ysclid=mawaxo1iy324518933.
3. Автоматизация информационной безопасности. URL: https://falcongaze.com/ru/pressroom/publications/osnovy-ib/avtomatizaciya-informacionnoj-bezopasnosti.html.

Bayrushin F.T.
Ufa University of Science and Technology, Ufa

AUTOMATION OF INFORMATION SECURITY MANAGEMENT

Abstract. The article discusses the urgent need for automation of information security at the enterprise, the specifics of the approach to automation in the field of information security management as a process, and the levels of functional personnel of the enterprise who need automation of their functional, regular procedures. The issues of the orientation of the process at the enterprise are considered. Some automation systems in the field of information security, such as SiMMA and automation in the field of information security, are affected.

Keywords: open source code, proprietary software, metric, script, automation platform.

УДК 004.056

Валеев С.С., Гузаиров М.Б.
Уфимский университет науки и технологий, Уфа

ГЕНЕРАТИВНЫЕ МНОГОАГЕНТНЫЕ СИСТЕМЫ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ НА БАЗЕ КОНЦЕПЦИИ НУЛЕВОГО ДОВЕРИЯ

Аннотация. Распределенные мультиагентные системы представляют собой перспективное направление развития технологий искусственного интеллекта. Они позволяют объединить усилия множества интеллектуальных агентов, размещенных на разных серверных площадках для совместного решения масштабных и комплексных задач. Эта парадигма решает проблему ограниченности локальных вычислительных

мощностей и дает возможность задействовать специфические компетенции отдельных моделей машинного обучения. Рассматривается аспект задач, связанных с вопросами обеспечения информационной безопасности в этих системах. Обсуждается решение задач защиты информации в мультиагентной распределенной системе на базе концепции нулевого доверия в рамках мультиагентных технологий.

Ключевые слова: программный агент, мультиагентные системы, распределенные вычисления, угрозы безопасности, концепция нулевого доверия.

Распределенные мультиагентные системы (РМС) позволяют объединить гетерогенные вычислительные системы для повышения эффективности достижения цели и относятся к классу распределенных вычислительных систем [1]. Рассмотрим далее основные особенности архитектуры РМС.

Агенты в рамках РМС могут иметь разные характеристики и специализации. Например, один агент может отвечать за обработку естественного языка, другой – за компьютерное зрение, третий – за принятие решений и управление ресурсами. Каждый агент представляет специализированный сервис, тем самым, предоставляя свои сервисы и знания другим участникам сетевого взаимодействия.

Для эффективной координации действий всех участников РМС необходима единая система протоколов обмена информацией между агентами. Это достигается благодаря использованию открытых API-интерфейсов, обеспечивающих совместимость и интеграцию компонентов независимо от среды исполнения и особенностей конкретных вычислительных платформ.

Несмотря на децентрализованный характер вычисления, система имеет иерархическую архитектуру, т. е. централизованная управляющая подсистема, размещенная в РМС, координирует процессы всей вычислительной системы. Она определяет порядок взаимодействий между агентами, распределяет задачи и ресурсы, обеспечивает мониторинг производительности и надежности каждой подсистемы.

Данный подход к организации вычислений имеет как преимущества, так и недостатки. К преимуществам можно отнести:

– возможность подключения новых вычислительных узлов, что позволяет повысить эффективность системы без значительного увеличения нагрузки на существующие подсистемы;

– повышение отказоустойчивости на основе разнообразия функционала агентов и разделению функций между ними;

– разделение задач между несколькими узлами, что позволяет в ряде случаев снижать требования к мощности отдельного сервера и оптимизировать процессы использования вычислительных ресурсов.

К недостаткам, с точки зрения информационной безопасности, следует отнести:

– нарушение конфиденциальности, связанное с распределенным характером архитектуры РМС (отсутствие единого периметра безопасности);

– так как агенты расположены на разных серверах, злоумышленники могут реализовать проникновение в РМС через наименее защищенный узел, или возможна реализация распределенной атаки (эффект слабого звена);

– обмен конфиденциальной информацией между удаленными подсистемами требует гармонизации политик безопасности, что не всегда возможно по разным причинам (необходима разработка стандартов безопасности);

– низкое качество сетевых соединений или перебои с доступом к сети могут привести к потере синхронизации между агентами, что нарушает работоспособность системы;

– сбой одного вычислительного узла способен вызвать каскадный эффект, негативно влияющий на производительность и безопасность всей сети;

– сложность мониторинга и диагностики системы, поэтому выявление причины сбоев требует больших затрат, особенно если проблема возникает одновременно на нескольких уровнях иерархии РМС;

– центр должен постоянно отслеживать состояние всех агентов, обеспечивая балансировку нагрузок и своевременное реагирование на изменения условий эксплуатации;

– «бесплатный проезд» – поставщики услуг могут эксплуатировать общие ресурсы без равноценного вклада, заменяя запрошенную мощную БЯМ (большая языковая модель) на менее простую модель для снижения своих затрат на вычисления.

Рассмотрим далее предлагаемые решения в рамках концепции нулевого доверия [2].

Концепция нулевого доверия предполагает отсутствие автоматического доверия ко всем субъектам и объектам внутри корпоративной сети, независимо от их расположения – внутренний или внешний доступ требует постоянного подтверждения подлинности и проверки полномочий каждого субъекта перед предоставлением доступа к ресурсам [3,4]. Роль многоагентной системы защиты информации (МСЗИ) становится особенно значимой, поскольку она способна обеспечить гибкое и адаптивное управление политиками безопасности в РМС путем динамического контроля состояния информационной среды организации.

Преимущества использования МСЗИ в рамках концепции нулевого доверия:

– благодаря наличию множества программных агентов, которые работают параллельно и выполняют мониторинг разных участков РМС,

МСЗИ способна значительно сократить время обнаружения угроз и ускорить реакцию на инциденты безопасности. Каждый агент МСЗИ собирает локальную информацию о своем сегменте сети РМС, обрабатывает ее и передает информацию другим агентам МСЗИ. Это ускоряет процесс выявления аномалий в РМС и повышает общую эффективность обнаружения атак, обеспечивают постоянное наблюдение за всеми элементами РМС, охватывая даже удаленные вычислительные узлы и ресурсы, позволяя эффективно контролировать безопасность больших территориально распределенных сетей;

– каждое событие, происходящее в любом узле сети РМС, фиксируется соответствующим агентом МСЗИ и передается на обработку другим компонентам системы МСЗИ. Такой подход помогает выявлять скрытые каналы передачи данных, злоупотребления привилегиями и другие типы сложных атак, которые могут остаться незамеченными традиционными средствами мониторинга системы;

– разделение функций между агентами МСЗИ позволяет детально исследовать каждое потенциально опасное действие в РМС отдельно, снижая нагрузку на центральный кластер обработки данных и повышая точность аналитики. Использование распределенных алгоритмов машинного обучения в МСЗИ также дает возможность быстро выявить новые виды угроз и своевременно обновлять политики безопасности в РМС.

Рассмотрим далее набор основных методов адаптации политик безопасности в РМС. Для эффективного функционирования РМС в среде нулевого доверия используются следующие методы адаптации правил безопасности:

– применение многофакторной аутентификации в случае любого отклонения поведения агента РМС или процесса от ожидаемых норм, обеспечивая дополнительный уровень уверенности в подлинности запросов;

– мониторинг активности в сети: постоянный контроль изменений трафика, поведенческих моделей агентов РМС и процессов помогает вовремя идентифицировать возможные атаки и предотвратить реализацию угроз;

– проверка целей внедрения нового кода в РМС, оценка его функциональности и потенциального воздействия на РМС.

Перечисленные меры дополняют друг друга, создавая комплексную защитную среду, способную оперативно адаптироваться к изменениям условий эксплуатации и угрозам.

Таким образом, использование МСЗИ для реализации задач защиты информации в РМС представляет собой необходимый инструмент в рамках концепции нулевого доверия, обеспечивающий требуемую степень надежности РМС и эффективности процедур управления рисками.

Список использованных источников:

1. Тарасов В.Б. Агенты, многоагентные системы, виртуальные сообщества: стратегическое направление в информатике и искусственном интеллекте // Новости искусственного интеллекта. 1998. № 2. С. 5–63.
2. Многоагентные системы как технологическая база реализации концепции нулевого доверия / С.С. Валеев, Н.В. Кондратьева, М.Б. Гузаиров, А.С. Исмагилова // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2024. № 3. С. 116–123. DOI 10.18137/RNU.V9187.24.03.P.116.
3. Валеев С.С., Кондратьева Н.В. Особенности проектирования систем безопасности на базе архитектуры нулевого доверия // ivdon.ru – 2023. URL: http://www.ivdon.ru/uploads/article/pdf/IVD_68__8_valeev_kondratyeva_v2.pdf_72458b243f.pdf (дата обращения: 30.04.2025).
4. Валеев С.С., Кондратьева Н.В., Мельников А.В. Архитектура предприятия и архитектура нулевого доверия // info-secur.ru – 2023. URL: https://www.info-secur.ru/index.php/ ojs/article/download/413/371/ (дата обращения: 30.04.2025).

Valeev S.S., Guzairov M.B.
Ufa University of Science and Technology, Ufa

GENERATIVE MULTI-AGENT SYSTEMS AND INFORMATION SECURITY TASKS BASED ON THE CONCEPT OF ZERO TRUST

Abstract. Distributed multi-agent systems represent a promising area for the development of artificial intelligence technologies. They allow us to combine the efforts of many intelligent agents located on different server sites to jointly solve large-scale and complex tasks. This solves the problem of limited local computing power and makes it possible to use the specific competencies of individual machine learning models. The aspect of tasks related to the issues of ensuring information security in these systems is considered. The solution of information security problems in a multi-agent distributed system based on the concept of zero trust within the framework of multi-agent technologies is discussed.

Keywords: software agent, multi-agent systems, distributed computing, security threats, zero trust concept.

УДК 51-74

Исмагилова А.С.
Уфимский университет науки и технологий, Уфа

КРИПТОГРАФИЧЕСКИЕ АСПЕКТЫ ИЗОМОРФИЗМА ГРУПП ОБРАТИМЫХ ЭЛЕМЕНТОВ

Аннотация. В настоящей работе предложен подход к описанию процесса шифрования с использованием изоморфизма групп обратимых элементов ассоциативных колец с единицей. Показано, что такой подход позволяет моделировать преобразование данных, их разделение на логически независимые компоненты и применение различных режимов обработки − изоморфизма и антиизоморфизма. В качестве конкретной реализации рассмотрен пример на основе колец Z_3 и $M_2(Z_2)$, в котором центральный идемпотент определяет разложение кольца на прямую сумму и обеспечивает согласованное применение разных алгебраических преобразований к частям сообщения. Полученные конструкции могут быть использованы при построении гибридных криптографических схем, обеспечивающих дополнительные возможности для защиты информации.

Ключевые слова: открытый ключ, закрытый ключ, группа шифрования, группа расшифрования, изоморфизм.

Настоящее исследование основано на результатах автора, которые были опубликованы в работе [1]. Цель данной работы − описать криптографическую систему, где открытый текст представлен как элемент группы обратимых элементов ассоциативного кольца с единицей.

Пусть R и S − ассоциативные кольца с единицей, множества открытых/закрытых ключей. Разложения в прямую сумму $R = R_1 \oplus R_2$, $S = S_1 \oplus S_2$ могут соответствовать разделению данных на независимые компоненты, каждая из которых обрабатывается по-разному. Группы обратимых элементов $U(R)$ и $U(S)$ можно представить как группы шифрования/расшифрования. Пусть в R определена ортогональная система идемпотентов h_i, $\sum_{i=1}^{3} h_i = 1$, $Rh_iR = R$, в S − система g_j, $\sum_{j=1}^{2} g_j = 1$, $Sg_jS = S$. Ортогональные идемпотенты могут представлять собой разделение данных на части. Центральный идемпотент $e \in R$ определяет какая часть сообщения обрабатывается изоморфизмом $\theta_1 : R_1 \to S_1$, какая антиизоморфизмом $\theta_2 : R_2 \to S_2$. Процесс преобразования данных, защищенных с помощью одной криптографической схемы, в эквивалентные данные, защищенные другой схемой, можно описать как изоморфизм $\varphi : U(R) \to U(S)$.

Теорема. Если существует изоморфизм между группами обратимых элементов φ, то существует кольцевой изоморфизм θ_1, кольцевой

антиизоморфизм θ_2, такие, что $\varphi(A) = \theta_1(eA) + \theta_2\big((1-e)A\big)$, где $e \in R$, $A \in E(R)$, $E(R)$ − группа преобразований, порожденная элементом $1 + e_i x e_j$.

Теорему можно использовать не только в абстрактной математике, но и в современной криптографии. Приведем пример, реализующий данный результат.

Пусть кольцо R моделирует систему данных или шифрования, в которой информация может быть разделена на две независимые части ($R = R_1 \oplus R_2$). Здесь $R_1 = Z_3$ − кольцо вычетов по модулю 3 − содержит три элемента $\{0, 1, 2\}$ с операциями сложения и умножения по модулю 3. Например, это может быть цифровая подпись или короткий ключ. $R_2 = M_2(Z_2)$ − кольцо матриц размера 2×2 над Z_2, содержит $2^4 = 16$ элементов. К примеру, это кольцо может использоваться для сложных структур, таких как блоки шифруемого текста. Аналогично, $S = S_1 \oplus S_2$, где $S_1 = M_2(Z_2)$, $S_2 = Z_3$. То есть кольца R и S имеют одинаковые компоненты, но они расположены в обратном порядке. Если представить переход от R к S, то его можно рассматривать как переход между двумя различными криптографическими схемами.

Группы $U(R)$ и $U(S)$ − группы обратимых элементов над ассоциативными кольцами R и S, соответствуют обратимым операциям шифрования и расшифрования.

Группа $U(R)$ представляет собой совокупность обратимых преобразований, действующихй на парах − один элемент из Z_3, другой − из $M_2(Z_2)$:

$$U(R) = U(Z_3) \oplus U\big(M_2(Z_2)\big).$$

Здесь $U(Z_3) = \{1, 2\}$, поскольку эти два элемента имеют обратные по умножению в кольце вычетов Z_3. Группа невырожденных матриц размера 2×2 над Z_2 − $U\big(M_2(Z_2)\big)$ − содержит шесть элементов:

$$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}, \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\1 & 1\end{pmatrix}.$$

Аналогично, $\mathrm{U(S)} = \mathrm{U}\big(\mathrm{M_2(Z_2)}\big) \oplus \mathrm{U(Z_3)}$. Прямая сумма коммутативна с точностью до изоморфизма.

Существование изоморфизма $\varphi: U(R) \to U(S)$ групп обратимых элементов означает, что группы шифрования/расшифрования совпадают с точностью до перестановки частей. Иначе, обе системы допускают эквивалентные наборы.

Заметим, что кольца R_1 и S_1 не изоморфны как целые, но можно рассмотреть вложение − инъективный гомоморфизм из $\mathrm{Z_3}$ в $\mathrm{M_2(Z_2)}$. Вложение позволяет сохранить структуру части данных при отображении одного кольца в другое. Антиизоморфизм можно представить в виде транспонированной матрицы: $\theta_2(A) = A^T$. Это дополняет степень защиты, усложняя восстановление исходного сообщения без знания точного типа

отображения. В качестве центрального идемпотента выберем $e = (1,0) \in R$. Тогда $eA = (a, 0)$, $(1 - e)A = (0, b)$, где $A = (a, b) \in R$.

Приведенный пример показывает, как можно формализовать процесс шифрования данных, разделенных на части при помощи алгебраических преобразований. Такая схема может быть применена при построении гибридных криптосистем, где разные части сообщения защищаются разнвми методами, но при этом сохраняется согласованность между группами.

В перспективе планируется рассмотреть общие классы колец и исследовать устойчивость схем к различным типам криптоатак.

Список использованных источников:

1. Исмагилова, А.С. Изоморфизмы групп обратимых элементов ассоциативного кольца / А.С. Исмагилова // Вестник Башкирского университета. 2005. № 4, т. 10. С. 8–11.

Ismagilova A.S.
Ufa University of Science and Technology, Ufa

CRYPTOGRAPHIC ASPECTS OF ISOMORPHISM OF REVERSIBLE ELEMENT GROUPS

Abstract. In this paper, we propose an approach to describing the encryption process using the isomorphism of the groups of invertible elements of associative rings with identity. We show that this approach allows us to model data transformation, partitioning into logically independent components, and applying different processing modes, such as isomorphism and anti-isomorphism. As a specific implementation, we consider an example based on the rings Z_3 and $M_2(Z_2)$, where the central idempotent determines the decomposition of the ring into a direct sum and ensures the consistent application of different algebraic transformations to different parts of the message. The resulting designs can be used to build hybrid cryptographic schemes that provide additional information protection capabilities.

Keywords: public key, private key, encryption group, decryption group, and isomorphism.

УДК 004.056: 519.2

Корнилова А.А., Гиззатова Э.Р.
Уфимский университет науки и технологий, Уфа

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ВРЕМЕННОГО РЯДА КОЛИЧЕСТВА СКОМПРОМЕТИРОВАННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ В МИРЕ

Аннотация. В работе приведено описание статистических данных по количеству скомпрометированных персональных данных в период с 2013 по 2024 г. Показано, что с наибольшим коэффициентом корреляции данные описываются показательной функции. Приведена попытка прогноза количества утечек информации на 2025 г.

Ключевые слова: математическое моделирование, прогноз, персональные данные, утечка.

Эпоха массовых кибер-атак, которая сегодня ведется стала тотальной во всем мире. Нет страны, в которой не фиксировались бы утечки информации национального масштаба. В 2023 г. экспертно-аналитическим центром было заявлено о 11549 утечек информации, произошедших в мире, что на 61,5 % больше, чем в 2022 г. [1]. Увеличение объема скомпрометированных персональных данных (ПДн) связано с повышением хакерских атак на фоне конфликтов во всем мире (СВО, столкновения на Ближнем Востоке и в Африке и др.) [2]. По данным экспертно-аналитического центра в 2023 г. доля внешних нарушителей выросла только в России [1]. В 2024 г. Российская Федерация заняла 2-е место по количеству утечек информации во всем мире, на первом месте оказались Соединенные штаты Америки.

Сегодня все чаще используются математические аппараты для описания различных процессов во всех областях деятельности человека [3]. Математические модели нашли широкое применение и при описании преступности [4]. С помощью математической модели удается изучить динамику преступности, прогнозировать дальнейшее ее развитие, а главное выявлять влияющих на нее факторы [5]-[6].

Целью работы является подбор модели для описания количества скомпрометированных ПДн для ее прогноза на 2025–2026 гг.

Самой простой моделью для описания статистических данных является линейная модель, которой характерна следующая зависимость:

$$Y = a + b \cdot X = a + b \cdot (T - 2012),$$

где a, b – являются некоторыми константами, T – время (год). Константы подбирают с использованием метода наименьших квадратов. Коэффициент линейной корреляции при этом равен 0.775. На рисунке представлены результаты вычислений.

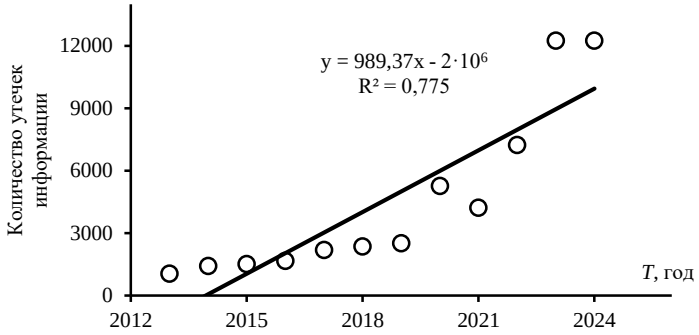

Рис. 1. Сравнение количества фактического числа утечек информации с линейной моделью (символ – статистические данные, линия – расчет)

В табл. 1 приведены результаты, полученные по различным классам математических функций, которые могут подойти к описанию имеющейся зависимости между Y (количества утечек) и T (год).

Таблица 1

Результаты проведенных вычислений

Модель	Вид уравнения	R^2
Линейная	$Y = a \cdot X + b$	0,775
Экспоненциальная	$Y = a \cdot \exp(b \cdot X)$	0,9407
Показательная	$Y = k \cdot a^{b \cdot X}$	0,9535
Степенная	$Y = a \cdot X^b$	0,8584
Гиперболическая	$Y = a + b/X$	–
Перла – Рида	$Y = k/(1 + a \cdot exp(b \cdot X))$	–
Гомпертца	$Y = a \cdot exp(b \cdot exp(c \cdot X))$	0,0823
Гомпертца – Мейкхама	$Y = a \cdot exp(b \cdot k^{c \cdot X} + d)$	0,0957

Описать статистические данные не удалось с помощью гиперболической моделью и зависимостью Перла-Рида в виду особенности функциональной зависимости. По результатам вычислений видно, что наибольший коэффициентом регрессии обладает показательная модель 0.9535, что свидетельствует о тесной связи между расчетными и статистическими данными. Показательная функция применяется для аналитического описания тенденции развития показателя с течением времени [7]:

$$Y = k \cdot a^{b \cdot X},$$

где X = время–2012; K, a, b – некоторые константы.

Расчет коэффициентов показал следующие данные:

$$Y = 635 \cdot 1.08^{3.25 \cdot T}.$$

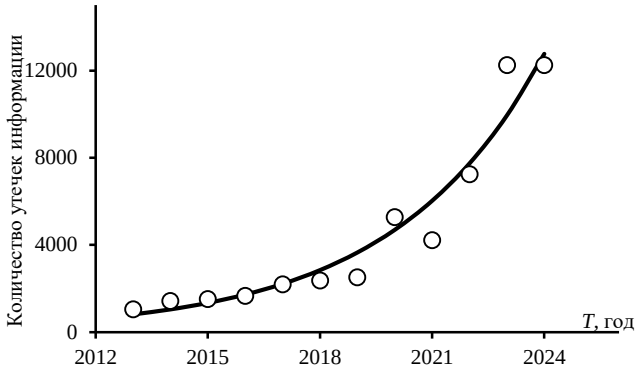

Рис. 2. Сравнение количества фактического числа утечек информации с показательной моделью (символ – статистические данные, линия – расчет)

При подстановке в полученное уравнение *T*, равное 2025–2027, получены следующие результаты:

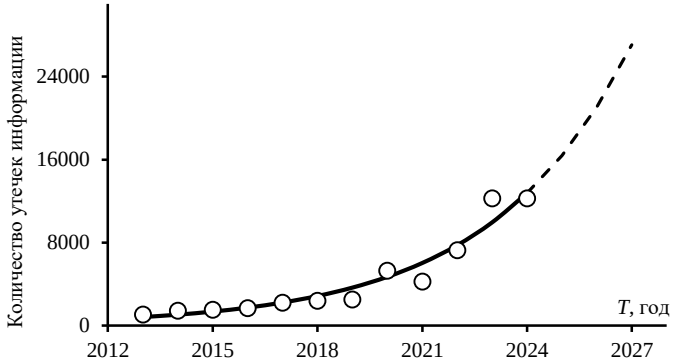

Рис. 3. Прогноз количества числа утечек информации (символ – статистические данные, линия – расчет)

Таким образом, несмотря на все объективные проблемы рынка информационной безопасности, многим крупным компаниям удается планомерно выстраивать эффективные системы безопасности и поддерживать их соответствие новым угрозам. Несмотря на это в настоящий момент следует ожидать увеличение количества утечек информации в 2025 г. в 1,5 раза по сравнению с 2024 г. В марте Роскомнадзор опубликовал информацию об утечке 24 млн записей россиян с начала 2025 г. [8].

Список использованных источников:

1. Утечки информации в мире, 2022–2023 гг. // Экспертно-Аналитический центр InfoWatch. 2024 г. URL: https://www.infowatch.ru/ sites/default/files/ analytics/files /issledovaniye-utechek-informatsii-v-mire-za-2022-2023-gody.pdf?ysclid=m9kwhev 8ln209074874 (дата обращения: 17.04.2025).

2. Количество слитых персональных данных в 2024 г. выросло на треть // Платформа для бизнес-планирования. 05.03.2025 г. URL:

https://safe.cnews.ru/news/line/2025-03-05_kolichestvo_slityh_personalnyh (дата обращения: 17.04.2025).

3. Галимнуров А.А. Применение математического моделирования для прогнозирования спреда корпоративных облигаций / А.А. Галимнуров, А.С. Исмагилова // Инженерный вестник Дона. 2025. № 2(122). С. 721–737.

4. Постовалов О.В. Математическое моделирование на основе теории причинности в приложении к криминалистической характеристике и профилактике преступлений // Правовое государство: теория и практика. 2020. С. 152–160.

5. Судакова Т.М. Математическое моделирование в разработке и совершенствовании методологических основ криминологии // Уголовно-правовые науки. 2023. Т. 24. № 3. С. 388–395.

6. Дианов Д.В. Прикладные статистические исследования экономической безопасности. М.: Русайнс. 2022. 194 с.

7. Сизова Т.М. Статистика для бакалавров. Часть II. СПб: Университет ИТМО, 2016. 70 с.

8. Роскомнадзор: в сеть утекло 24 млн записей россиян с начала 2025 г. Iaassaaspaas. Обзор ИТ решений для бизнеса и государства. 13.03.2025 г. URL: https://iaassaaspaas.ru/news/okolo-milliarda-strok-personalnyh-dannyh-uteklo-v-set-za-polgoda-nikakie-shtrafy-ne-pomogayut (дата обращения: 17.04.2025).

Kornilova A.A., Gizzatova E.R.
Ufa University of Science and Technology, Ufa

MATHEMATICAL MODELING OF THE TIME SERIES OF THE QUANTITY OF COMPROMISED PERSONAL DATA IN THE RUSSIAN FEDERATION

Abstract. The paper describes statistical data on the amount of compromised personal data in the Russian Federation in the period from 2013 to 2024. It is shown that the data are described by the exponential function with the highest correlation coefficient. An attempt to predict the number of information leaks for 2025 is given.

Keywords: mathematical modeling, forecast, personal data, leak.

УДК 004.832.2

Кузнецова Е.В., Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ДЛЯ V2X-СИСТЕМ

Аннотация. В статье рассматриваются методы машинного обучения (МО), применяемые для обнаружения вторжений в системах V2X (Vehicle-to-Everything). Показана эффективность ключевых алгоритмов МО в контексте обеспечения информационной безопасности автомобильных сетей: метода K-ближайших соседей, многослойного перцептрона, сетей с долгой краткосрочной памятью (LSTM) и деревьев решений. Особое внимание уделено сравнительному анализу их производительности на основе стандартных оценочных метрик.

Ключевые слова: машинное обучение, обнаружение вторжений, V2X, подключенные автомобили, кибербезопасность.

Введение

С развитием технологий V2X, обеспечивающих обмен данными между транспортными средствами и инфраструктурой, резко возросла уязвимость таких систем к киберугрозам [1]. Традиционные методы защиты зачастую не справляются с новыми типами атак, что делает машинное обучение (МО) перспективным инструментом для мониторинга и предотвращения вторжений. В данной работе мы проанализируем современные ML-алгоритмы, доказавшие свою эффективность обеспечения информационной безопасности автомобильных сетей.

Обзор методов машинного обучения

Машинное обучение (ML) представляет собой набор подходов в области искусственного интеллекта, позволяющих разрабатывать компьютерные системы, способные к самообучению [2]. Методы машинного обучения подразделяются на классическое обучение, нейросети и глубокое обучение, обучение с подкреплением, ансамблевое обучение. Как видно из рис. 1, существует большое разнообразие алгоритмов МО.

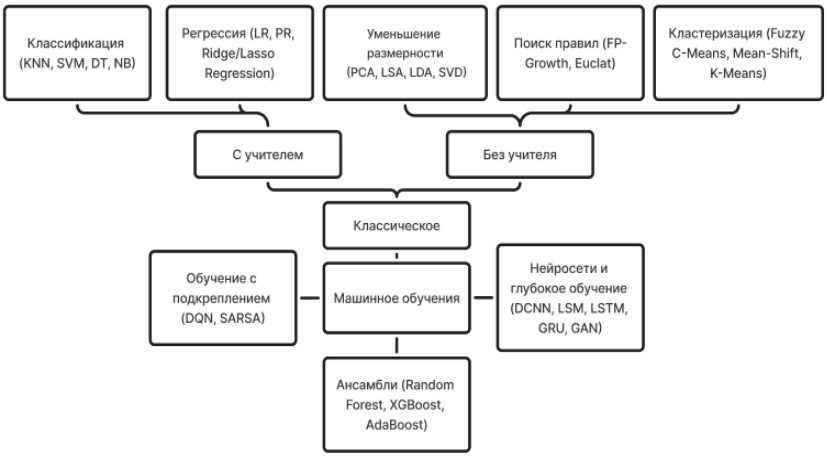

Рис. 1. Алгоритмы машинного обучения

Для систем обнаружения вторжений в V2X чаще всего используются такие модели обучения как: многослойный перцептрон [3], сети с долгой краткосрочной памятью (LSTM), классические методы обучения с учителем [4], среди которых выделяются: метод k-ближайших соседей и деревья принятия решений.

Метод k-ближайших соседей (k-Nearest Neighbor)

Алгоритм KNN, основан на принципе «похожие объекты ведут себя аналогично», и он успешно применяется для классификации устройств в сетях VANET (Vehicular ad-hoc network) [5]. Его ключевое преимущество – простота интерпретации результатов: автомобиль идентифицируется как «доверенный» или «подозрительный» на основе анализа поведения ближайших соседей.

Многослойный перцептрон (MLP, Multi-Layer Perceptron).

MLP – это тип искусственной нейронной сети, который состоит из нескольких слоев нейронов, включая входной слой, один или несколько скрытых слоев и выходной слой. Исследование [6] подтвердило, что такая модель эффективно выявляет отклонения в поведении узлов VANET за счет обучения с обратным распространением ошибки.

Сети с долгой краткосрочной памятью (LSTM, Long Short Term Memory)

Для борьбы с Sybil-атаками в Системах Кооперативного Интеллектуального Транспорта (C-ITS) предложено использовать LSTM [7] – особый тип нейросетей, специализирующийся на анализе временных последовательностей. Хотя метод уступает другим в точности (Таблица 1), его сила в прогнозировании сложных многоэтапных атак.

Деревья решений (DT, Decision Trees)

Деревья решений представляют собой модель, которая принимает решения на основе последовательности вопросов, задаваемых о входных данных. Данный метод основывается на правиле: «Если <условие>, то <ожидаемый результат>». В работе [8] показано, что деревья решений в

CAN-сетях особенно эффективны против атак типа «отказ в обслуживании» и спуфинга.

Сравнительный анализ

Таблица 1 наглядно демонстрирует, что: KNN лидирует по F1-мере (99.37),

MLP достигает рекордного показателя качества (99.40 %), а LSTM имеет сбалансированные, но менее выдающиеся показатели.

Таблица 1

Производительность моделей обучения

Метод	Точность	Полнота	F1-мера	Качество
KNN [9]	98,95	96,23	99,37	97,99
MLP [7]	97,95	97	97,46	99,40
DT [8]	98,19	98,16	-	98,19
LSTM [6]	95,6	89,6	92,5	96,4

Вывод

Проведенное исследование подтверждает, что классические ML-алгоритмы (KNN, DT) и многослойный перцептрон демонстрируют наилучшие результаты в задачах обнаружения вторжений для V2X. Несмотря на потенциал LSTM, применение этого метода неэффективно из-за низких показателей, в особенности показателя полноты. Перспективы для дальнейшей работы – изучение и проектирование гибридных моделей, сочетающих преимущества всех рассмотренных подходов.

Список использованных источников:

1. Lu R., L. Zhang, J. Ni, and Fang Y. “5g vehicleto-everything services: Gearing up for security and privacy,” Proceedings of the IEEE, 2019.

2. IBM machine learning definition. URL: https://www.ibm.com/cloud/learn/machine-learning.

3. Hossain M.D., Inoue H., Ochiai H., Fall D., and Kadobayashi Y., “An effective in-vehicle can bus intrusion detection system using cnn deep learning approach,” in GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, 2020.

4. Uprety A., Rawat D.B., and Li J., “Privacy preserving misbehavior detection in iov using federated machine learning,” in 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), 2021.

5. Montenegro J., Iza C., and Aguilar Igartua M., “Detection of position falsification attacks in vanets applying trust model and machine learning,” in Proceedings of the 17th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks, 2020.

6. Ghaleb F.A., Zainal A., Rassam M.A., and Mohammed F., “An effective misbehavior detection model using artificial neural network for vehicular ad hoc network applications,” in 2017 IEEE Conference on Application, Information and Network Security (AINS). IEEE, 2017.

7. Khan I.A., Moustafa N., Pi D., Haider W., Li B., and Jolfaei A., “An enhanced multi-stage deep learning framework for detecting malicious activities from autonomous vehicles”, 2021.

8. Moulahi T., Zidi, S., Alabdulatif A., Atiquzzaman M. Comparative Performance Evaluation of Intrusion Detection Based on Machine Learning in In-Vehicle Controller Area Network Bus. IEEE, 2021.

9. Refat R.U.D.; Elkhail A.A.; Hafeez A.; Malik H. Detecting CAN Bus Intrusion by Applying Machine Learning Method to Graph Based Features. In Intelligent Systems and Applications, Germany, 2022.

Kuznetsova E.V., Sentsova A.U.
Ufa University of Science and Technology, Ufa

APPLICATION OF MACHINE LEARNING IN INSURANCE DETECTION SYSTEMS FOR V2X SYSTEMS

Abstract. The article discusses machine learning (ML) methods used for intrusion detection in V2X (Vehicle-to-Everything) systems. The effectiveness of key ML algorithms in the context of ensuring information security of vehicular networks is demonstrated: K-nearest neighbors method, multilayer perceptron, long short-term memory (LSTM) networks, and decision trees. Particular attention is paid to a comparative analysis of their performance based on standard evaluation metrics.

Keywords: machine learning, intrusion detection, V2X, connected cars, cybersecurity.

УДК 377.8

Новикова Д.Д.
Поволжский государственный университет телекоммуникаций и информатики, Самара

ОСНОВНЫЕ УГРОЗЫ ДЛЯ ДЕТЕЙ В ИНТЕРНЕТЕ И СПОСОБЫ ЗАЩИТЫ

Аннотация. В статье рассматриваются ключевые угрозы, с которыми сталкиваются дети в информационном пространстве: кибербуллинг, вредоносный контент, вовлечение в незаконную деятельность и интернет-зависимость. Описаны основные методы защиты детей: правовое регулирование, технические средства, развитие цифровой грамотности,

психологическая поддержка и сотрудничество между государственными структурами, бизнесом и гражданским обществом. Проведен анализ актуальной статистики. Сделаны выводы о необходимости комплексного подхода к обеспечению безопасности детей в сети Интернет.

Ключевые слова: безопасность детей, информационное пространство, интернет-угрозы, цифровая грамотность, кибербуллинг, родительский контроль.

Информационные технологии прочно вошли в повседневную жизнь детей, предоставляя широкие возможности для обучения, общения и досуга. Однако вместе с позитивными аспектами возрастают и риски негативного воздействия цифровой среды. По данным Лаборатории Касперского, в 2024 г. 60 % детей сталкивались с нежелательным контентом в интернете, а около 30 % подвергались кибербуллингу. В связи с этим возрастает необходимость изучения основных угроз и способов защиты детей в информационном пространстве. Рассмотрим наиболее популярные из них.

Кибербуллинг – это систематическое использование электронных средств для нанесения вреда другим пользователям. Для детей кибербуллинг особенно опасен тем, что унижения и оскорбления распространяются быстро, на широкую аудиторию, и их трудно удалить. Исследования показывают, что жертвами кибербуллинга часто становятся дети с низкой самооценкой или слабо выраженными социальными навыками, что приводит к депрессии, тревожным расстройствам и даже суицидальным мыслям.

По данным ВЦИОМ (2024), 25 % подростков в России признались, что хотя бы раз подвергались кибербуллингу, а 7 % сталкивались с этим регулярно [1]. Особую обеспокоенность вызывает факт, что многие дети скрывают факты травли от родителей и педагогов, опасаясь осуждения или усиления травли. Дети становятся удобной целью мошенников по нескольким причинам: доверчивость, стремление к быстрым результатам (победе в игре, популярности в соцсетях) и отсутствие навыков распознавания угроз. Распространенные схемы: обман о выигрыше в конкурсах, фальшивые предложения «быстрых заработков», просьбы перевести деньги «другу в беде», фишинговые письма с зараженными ссылками.

Исследование Positive Technologies показывает, что около 12 % детей в возрасте от 10 до 15 лет хотя бы раз становились жертвами попыток онлайн-мошенничества, причем в 4 % случаев мошенникам удавалось получить личные данные или деньги [2].

Интернет-зависимость характеризуется патологическим стремлением ребенка проводить чрезмерное количество времени онлайн за счет сна, учебы, физической активности и реального общения. Наиболее подвержены дети и подростки, испытывающие дефицит эмоциональных связей в реальной жизни.

Формы проявления интернет-зависимости: бессонница, тревожность при невозможности выйти в сеть, потеря интереса к учебе и хобби, нарушения пищевого поведения.

Совокупный анализ данных различных исследований (Лаборатория Касперского, ВЦИОМ, Positive Technologies, Лига безопасного интернета) позволяет сделать вывод, что: более 65 % детей в возрасте от 8 до 16 лет в России хотя бы раз сталкивались с интернет-угрозами различного характера. Из них:

- 27 % стали жертвами кибербуллинга,
- 53 % сталкивались с вредоносным контентом,
- 12 % становились объектами мошеннических действий,
- 17–18 % проявляли признаки интернет-зависимости.

Эти цифры подчеркивают масштаб проблемы и необходимость комплексного подхода к обеспечению безопасности детей в цифровом пространстве. Стоит отметить, что ключевую роль в создании безопасной цифровой среды для детей играют правовые меры. На международном уровне защита детей в интернете обеспечивается Конвенцией ООН о правах ребенка. В России действует ряд нормативных актов:

- Федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства РФ № 1101 об ограничении доступа к запрещенной информации.

Эти документы закрепляют ответственность владельцев сайтов и операторов связи за распространение запрещенной информации и позволяют оперативно блокировать опасные ресурсы [3].

Кроме того, с 2021 г. в России активно развивается практика маркировки контента по возрастным категориям и применения «реестра запрещенных сайтов» (Роскомнадзор).

Технические инструменты создают дополнительный барьер на пути вредоносного контента:

- фильтрация трафика (например, через «семейные» DNS-серверы типа Yandex.DNS);
- родительский контроль в устройствах и приложениях (настройка лимитов времени, блокировка приложений);
- антивирусные решения с функцией веб-контроля, защищающие от фишинга и вредоносных ссылок;
- мониторинг активности: специальные программы позволяют родителям видеть, какие сайты посещает ребенок и сколько времени он проводит в сети.

Современные системы, такие как Kaspersky Safe Kids или Norton Family, предлагают не только блокировку контента, но и отчеты об активности, уведомления о выходе за пределы разрешенного времени, а

также контроль над геолокацией ребенка. Однако важно понимать: технические средства являются вспомогательным инструментом и не заменяют воспитательные меры.

Развитие критического мышления и цифровой грамотности среди детей и родителей является важнейшей долгосрочной стратегией защиты.

Необходимо обучать детей:

- различать достоверные и фальшивые источники информации;
- осознавать риски публикации личных данных в интернете;
- правильно реагировать на случаи угроз и кибербуллинга (не вступать в диалог, сохранять доказательства, обращаться за помощью).

Организация уроков цифровой безопасности в школах, проведение тренингов для родителей и создание обучающих онлайн-курсов доказали свою эффективность.

По данным проекта «Урок цифры» Минцифры России, участие в образовательных инициативах в 2024 г. приняли более 2,5 млн школьников [4].

Эффективная защита детей требует комплексного подхода:

- государство должно создавать законодательную базу и развивать инфраструктуру фильтрации контента;
- бизнес – в первую очередь IT-компании и разработчики приложений – обязан внедрять встроенные механизмы защиты (например, автоматическое ограничение возрастного доступа);
- гражданские организации должны проводить кампании по повышению осведомленности, поддерживать просветительские инициативы, обеспечивать общественный контроль.

Успешные примеры включают кампанию «Безопасный интернет» от Лиги безопасного интернета и международные проекты типа WePROTECT Global Alliance.

Таким образом, обеспечение безопасности детей в информационном пространстве требует многоуровневого взаимодействия всех заинтересованных сторон: родителей, педагогов, государства, бизнеса и самих детей. Статистические данные свидетельствуют о серьезности проблемы, но эффективное применение правовых, технических, образовательных и психологических мер позволяет значительно снизить риски.

Формирование культуры ответственного и осознанного пользования интернетом с раннего возраста должно стать приоритетной задачей на уровне государственной политики и образовательных программ.

Список использованных источников:

1. Детский кибербуллинг и как с ним бороться // ВЦИОМ Новости: [сайт]. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/detskii-kiberbulling-i-kak-s-nim-borotsja (дата обращения: 28.04.2025).

2. Новое исследование Positive Technologies // Cyber Media: [сайт]. URL: https://securitymedia.org/news/novoe-issledovanie-positive-technologies-

bolee-treti-izuchennykh-sim-kart-dayut-vozmozhnost-dlya-pop.html (дата обращения: 28.04.2025).

3. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию» // КонсультантПлюс: [сайт]. URL: https://www.consultant.ru/document/cons_doc_LAW_108808/d44bdb356e6a691d0c72fef05ed16f68af0af9eb/ (дата обращения: 28.04.2025).

4. Новый сезон «Урока Цифры» // Национальные проекты РФ: [сайт]. URL: https://национальныепроекты.рф/news/v-novom-sezone-uroka-tsifry-prinyali-uchastie-bolee-2-5-mln-shkolnikov/ (дата обращения: 28.04.2025).

Novikova D.D.
Volga Region State University of
Telecommunications and Informatics, Samara

THE MAIN THREATS TO CHILDREN ON THE INTERNET AND WAYS TO PROTECT THEM

Abstract. The article examines the key threats faced by children in the information space: cyberbullying, malicious content, involvement in illegal activities and Internet addiction. The main methods of child protection are described: legal regulation, technical means, development of digital literacy, psychological support and cooperation between government agencies, business and civil society. The analysis of current statistics is carried out. Conclusions are drawn about the need for an integrated approach to ensuring the safety of children on the Internet.

Keywords: child safety, information space, Internet threats, digital literacy, cyberbullying, parental control.

УДК 004.056

Ожгибесова А.С., Шабуров А.С., Южаков А.А.
Пермский национальный исследовательский
политехнический университет, Пермь

О РАЗРАБОТКЕ МЕТОДА ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Приводится обзор существующих методов оценки рисков информационной безопасности. Предлагается подход по совершенствованию методов оценки рисков, ориентированный на сохранении живучести информационных систем. Приведена математическая постановка задачи оценки рисков на основе применения методов нечеткой логики.

Ключевые слова: риск информационной безопасности, защита информации, живучесть информационных систем, нечеткая когнитивная карта.

В условиях количества и сложности кибератак оценка рисков информационной безопасности (ИБ) становится важнейшим инструментом для защиты данных, инфраструктуры и бизнес-процессов. Традиционные методы оценки рисков ИБ имеют общие недостатки, ограничивающие эффективность их применения [1]. Как правило, реализация традиционных подходов либо требует значительного количества ресурсов, либо имеют ограничения по применению (CRAMM, OCTAVE). Часть методов недостаточно гибки и сложно адаптируются к применению современных технологий (COBIT for Risk), или субъективны, узконаправленны и игнорируют устойчивость и возможность восстановления (FRAP, OCTAVE), акцентируя оценку на сохранении традиционных критериев обеспечения ИБ, а не на сохранении устойчивости функционирования систем в условиях риска и т. д.

Для преодоления этих недостатков необходимы новые, более гибкие подходы, ориентированные на противодействие современным киберугрозам и позволяющие автоматизировать процессы управления рисками ИБ в режиме реального времени, на основе применения технологий IoT, ML, AI и т. п.

В то же время значительное повышение актуальности проблем кибербезопасности, особенно для объектов класса КИИ, требует оценивать риски ИБ, с учетом сохранения надежности и работоспособности объектов защиты информации, а также сохранении живучести подобных систем [2], даже в условиях реализации стратегии принятия рисков ИБ.

К методам оценки рисков ИБ, ориентированных на сохранении живучести систем, способности их восстановления после инцидентов, а также устойчивости информационных систем, относятся: Survivability Analysis Framework (SAF), Mission-Oriented Riskand Design Analysis (MORDA), Resilience-Based Risk Management (RBRM) и Cyber Resilience Review (CRR). Каждый из данных методов имеет свои уникальные особенности, цели и подходы к оценке рисков, основные из которых приведены в табл. 1.

Анализ сравнительных характеристик базовых методов оценки рисков ИБ, позволяет сделать следующие выводы:

1) SAF подходит для глубокого анализа критических функций системы, но требует значительных затрат ресурсов;

2) MORDA ориентирована на системы, где важно выполнение конкретных миссий, но менее применима для систем общего назначения;

3) RBRM фокусируется на восстановлении после инцидентов, что делает ее полезной для систем с высокой важностью непрерывности, но требует значительных ресурсов для анализа рисков;

4) CRR – простой и доступный инструмент для оценки киберустойчивости, но не обеспечивает глубокого анализа данных.

Таблица 1

Сравнительные характеристики методов оценки рисков ИБ

	SAF	**MORDA**	**RBRM**	**CRR**
Основная цель	Сохранение критических функций	Оценка рисков для выполнения миссии	Повышение устойчивости и восстановления	Оценка киберустойчивости
Область приме-нения	Универсальная	Критические системы	Системы с высокой важностью непрерывности	Организации любого уровня
Методы анализа	Анализ угроз, уязвимостей	Сценарии угроз, анализ миссии	Анализ восстановления, сценарии инцидентов	Анкетирование, самооценка
Глубина анализа	Высокая	Высокая	Средняя	Низкая-средняя
Ресур-соемкость	Высокая	Высокая	Средняя	Низкая
Резуль-таты	Стратегии повышения живучести	Меры по снижению рисков для миссии	Планы повышения устойчивости	Рекомендации по улучшению

Таким образом, необходимо совершенствовать методы оценки рисков ИБ, с учетом ориентированности оценки на сохранении живучести ИС в условиях сохранения риска, путем нахождения оптимального баланса между универсальностью применения, необходимой глубиной анализа, оптимальной ресурсоемкостью и простотой применения технологий оценки. При этом, оценку целесообразно осуществлять на основе построения нечетких когнитивных карт (НКК), что неоднократно подтверждено [3, 4].

Для постановки задачи нахождения приемлемого уровня риска ИБ с учетом ориентированности на сохранении живучести ИС, обозначим:

$A = \{a_1, a_2, \dots a_n\}$ – множество ключевых активов;

$T = \{t_1, t_2, \dots t_p\}$ – множество угроз;

$V = \{v_1, v_2, \dots v_q\}$ – множество уязвимостей.

Для каждого актива $a_i \in A$ определяется подмножество соответствующих угроз $T_i \subseteq T$ и уязвимостей $V_i \subseteq V$. При этом, связь формализуется как:

$$R = \{(a_i, t_j, v_k) | a_i \in A, t_j \in T_i, v_k \in V_i\}. \quad (1)$$

Определим множество функциональных состояний ИС $S = \{s_1, s_2, \dots s_m\}$, где каждое состояние s_k характеризует степень работоспособности при частичных отказах ИС.

Живучесть системы L можно формализовать как функцию:

$L: S \to [0,1]$, $L(s_k)$-уровень живучести в состоянии s_k.

Для каждого состояния s_k вычисляется:

$$L(s_k) = \frac{\sum_{i=1}^{n} \alpha_i \cdot \delta_i(s_k)}{\sum_{i=1}^{n} \alpha_i}, \quad (2)$$

где α_i вес (значимость) актива a_i; $\delta_i(s_k) \in \{0,1\}$ – индикатор функционирования актива в состоянии s_k.

Построение НКК для оценки рисков ИБ предполагает представление ее в виде графа $G = (C, E, W)$, где $C = \{c_1, c_2, \dots c_l\}$ – концепты (факторы риска, уязвимости, угрозы); $E \subseteq C \times C$ – множество направленных связей; $W = \{w_{ij}\}, w_{ij} \in [-1,1]$ – веса влияния концепта c_j на концепт c_i.

Нечеткие значения концептов $A = \{a_1, a_2, \dots a_n\}$ задаются в виде чисел в интервале [0,1] и обновляются по формуле:

$$a_i^{(t+1)} = f\left(\sum_{j=1}^{l} w_{ij} \cdot a_i^{(t)}\right), \quad (3)$$

где $f(x)$ – функция активации, например:

$f(x) = \frac{1}{1+e^{-x}}$, или $f(x) = \min(1, \max(0, x))$.

Для каждого пути P_{ij} между концептами $c_j \to c_i$ можно вычислить агрегированное влияние с учетом длины пути и затухания:

$$Imp(c_j, c_i) = \sum_{k=1}^{K} \lambda^k \cdot \prod_{(u,v) \in P_{ij}^{(k)}} w_{uv}\ , \quad (4)$$

где $\lambda \in [0,1]$ – коэффициент затухания; K – максимальная длина пути; $P_{ij}^{(k)}$ – пути длины k между c_jи c_i.

Расчет уровня риска для актива α_i, связанного с угрозой t_j и уязвимостью v_k, определяется как нечеткая функция:

$$R_{ijk} = \mu T(t_j) \otimes \mu V(v_k) \otimes \mu C(c_m), \quad (5)$$

где $\mu T(t_j), \mu V(v_k), \mu C(c_m) \in [0,1]$ – степени принадлежности соответствующих концептов;

$\otimes$ – нечеткая операция агрегации (например, минимум, произведение или правило Мамдани).

Тогда общий риск для ИС будет определяться как:

$$R_{общ} = \sum_{(\alpha_i, t_j, v_k) \in R} \beta_{ijk} \cdot R_{ijk}, \quad (6)$$

где β_{ijk} – весовая значимость тройки (α_i, t_j, v_k).

Итоговый риск корректируется коэффициентом живучести ИС:

$$R_{кор} = R_{общ} \cdot (1 - L(s_{тек})), \quad (7)$$

где $L(s_{тек})$ – живучесть в текущем состоянии системы.

Разработанная математическая постановка задачи может являться основой предлагаемого метода оценки рисков ИБ, учитывающего особенности обеспечения живучести ИС различного назначения.

Список использованных источников:

1. Плетнёв П. В., Белов В. М. Сравнительный анализ существующих методов определения рисков информационной безопасности // Ползуновский вестник. 2011. № 3-1. URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-suschestvuyuschih-metodov-opredeleniya-riskov-informatsionnoy-bezopasnosti (дата обращения: 13.04.2025).
2. Махутов Н.А., Петров В.П., Резников Д.О. Оценка живучести сложных технических систем // Проблемы безопасности и чрезвычайных ситуаций. 2009. № 3. С. 47–66. (дата обращения: 17.04.2025).
3. Ожгибесова А. С. Об оценке рисков информационной безопасности на основе применения нечетких когнитивных карт в интеллектуальных транспортных системах управления дорожным движением / А.С. Ожгибесова, А.С. Шабуров, А.А. Южаков // Вестник УрФО. 2024. № 2(52). С. 56–67.
4. Васильев В.И. Автоматизация процесса оценки информационных рисков с использованием нечетких когнитивных карт / В.И. Васильев, Р.Т. Кудрявцева, В.А. Юдинцев // Вестник УГАТУ. 2014. Т. 18, № 3 (64). С. 253–260. (дата обращения: 28.04.2025).

Ozhgibesova A.S., Shaburov A.S., Yuzhakov A.A.
Perm National Research Polytechnic University, Perm

ON THE DEVELOPMENT OF A METHOD FOR ASSESSING INFORMATION SECURITY RISKS

Abstract. This paper provides an overview of existing methods for assessing information security risks. A proposed approach for improving risk assessment methods is focused on maintaining the resilience of information systems. A mathematical formulation of the risk assessment problem is presented based on the application of fuzzy logic methods.

Keywords: information security risk, information protection, survivability of information systems, fuzzy cognitive map.

УДК 004.056

Шагапов И.А., Салов И.В.
Уфимский университет науки и технологий, Уфа

ОБ ОДНОМ МАТЕМАТИЧЕСКОМ ПОДХОДЕ К ПОСТРОЕНИЮ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. В статье предложен математический подход к построению систем обработки и защиты информации из заданных подсистем. Подход показывает: откуда, в каком количестве и как могут быть получены новые

свойства системы. Работа может быть полезна для количественной и качественной оценки систем защиты информации до их построения.

Ключевые слова: математический подход, подсистема, система защиты информации, количественная и качественная оценка.

Современные вызовы окружающей действительности показывают, что вопросы построения систем обработки информации и систем защиты информации требуют более глубокого анализа и тщательной оценки. История вопроса показывает, что проблемы безопасности информации становятся все более острыми.

По мнению авторов, в этих вопросах могли бы помочь использование математических подходов.

Работа является естественным развитием идей, предложенных в наших предыдущих публикациях [1], [2]. В них было предложено следующее: при создании систем обработки и защиты информации важно учитывать один принципиальный момент: подобные системы интересуют не только пользователя, но и потенциального злоумышленника. Следовательно, построенную систему надо исследовать не только на наличие заложенных нужных (положительных) свойств, но и на наличие потенциально вредных (отрицательных) свойств [3], [4].

Ниже будут рассмотрены вопросы происхождения, количества и способов появления системных (новых) свойств при конструировании систем.

Очевидно, что новая система строится для решения неразрешенной задачи. Очень часто, как элементы, для этого используются уже известные типовые системы со своими имеющимися свойствами. В дальнейшем, мы их будем называть подсистемами. Таким образом, нужная система будет строиться из совокупности заданных подсистем.

Рассмотрим пример. Пусть задана совокупность двух подсистем, при этом каждая подсистема имеет свои свойства (у первой подсистемы 3 свойства, у второй – 2) (рис. 1).

Рис. 1. Исходные данные

Считаем, что подсистемы с их свойствами подобраны таким образом, что с ними можно производить определенные операции и строить новую систему с новыми свойствами. Допускаем, что среди этих свойств будут, в

том числе и необходимые нам свойства. Возникает вопрос: откуда они могут появиться, как создаются и какое их количество?

Применим несложный математический аппарат. Очевидно, построенная система уже имеет совокупность свойств, которые присущи заданным подсистемам. Нас интересуют новые свойства, которых нет ни у одной подсистемы. Естественно считать, что новое свойство должно строиться на уже имеющихся свойствах.

Предлагается следующая интерпретация. Любое новое свойство является результатом применения некоторой бинарной операции над существующими свойствами рассматриваемых подсистем (с каждой по одному свойству). В результате получится, что в нашем примере новая система потенциально будет иметь $N=3*2=6$ свойств (см. рис. 2**)** Бинарные операции демонстрируют, каким образом могут возникать новые свойства.

Бинарные операции существенно зависят от природы множества: как самих подсистем, так и присущих им свойств. Например, для множеств применимы операции объединения, пересечения, разности и т. д. Для числовых структур – операции сложения, умножения и т. д. Для функций сложение, умножение, композиция и т. д. Для булевых структур характерны свои операции. Более общим является групповой подход, когда элементы и сама операция могут быть абстрактными и «непохожими» на классические математические.

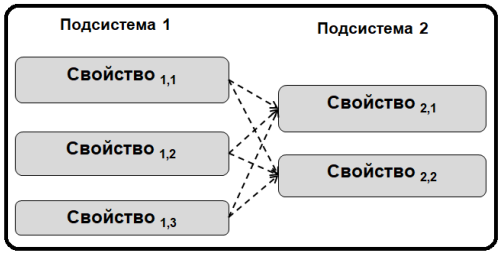

Рис. 2. Всевозможные свойства системы

Одна из сложностей при построении систем заключается как раз в правильной интерпретации исходных данных, а также в необходимости «увидеть» и «дополнить» их до нужной структуры, ввести соответствующие операции.

Другая возникающая задача – интерпретация полученных результатов для конкретного случая.

Для систем защиты информации не исключен вариант, когда обнаружение всего лишь одного нового вредного свойства может привести к отказу от построения именно такого варианта системы защиты информации.

Таким образом, предложенный математический подход к построению систем защиты информации может позволить количественно и качественно проанализировать и оценить систему защиты информации до ее построения.

Список использованных источников:

1. Шагапов И.А. К вопросу построения системы защиты информации / И.А. Шагапов // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19–20 мая 2023 г. Уфа: Уфимский университет науки и технологий, 2023. С. 51–54.
2. Шагапов И.А. О некоторых особенностях построения систем защиты информации / И.А. Шагапов // Естественные и технические науки. 2023. № 12 (187). С. 305–307.
3. Исмагилова А.С. Количественная оценка рекомпозиционной системы защиты информации / А.С. Исмагилова, И.А. Шагапов, И.В. Салов // Инженерный вестник Дона. 2024. № 8(116). С. 273–281.
4. Исмагилова А.С. Теоретико-графовая интерпретация системы защиты информации / А.С. Исмагилова, И.А. Шагапов, И.В. Салов // Инженерный вестник Дона. 2024. № 9 (117). С. 171–179.

Shagapov I.A., Salov I.V.
Ufa University of Science and Technology, Ufa

ABOUT ONE MATHEMATICAL APPROACH TO CONSTRUCTING INFORMATION SECURITY SYSTEMS

Abstract. The article proposes a mathematical approach to building information processing and protection systems from given subsystems. The approach shows where, in what quantity and how new properties of the system can be obtained. The work can be useful for quantitative and qualitative assessment of information protection systems before their construction.

Keywords: mathematical approach, subsystem, information protection system, quantitative and qualitative assessment.

УДК 004

Юнусова Д.С., Султанов Д.Ж.
Уфимский университет науки и технологий, Уфа

НЕЙРОСЕТЕВОЙ АНАЛИЗ URL-АДРЕСОВ ДЛЯ ВЫЯВЛЕНИЯ ФИШИНГОВЫХ АТАК

Аннотация. Фишинговые URL продолжают быть одним из наиболее частых инструментов в арсенале киберпреступников. В данной статье рассматривается нейросетевая модель для распознавания фишинговых URL-адресов, сотоящая из CNN части для обработки символьных

последовательностей домена и полносвязной части для обработки структурированных признаков.

Ключевые слова: фишинг, URL-адрес, нейронная сеть.

В эпоху цифровизации, когда интернет стал неотъемлемой составляющей повседневной жизни, возросло и количество киберугроз, в том числе фишинговых URL-адресов, представляющих серьезную угрозу для пользователей.

Фишинговые URL-адреса представляют собой специально сконструированные веб-ссылки, которые визуально имитируют адреса легитимных сайтов, но ведут на веб-ресурсы злоумышленников.

Использование черных списков становится малоэффективным, так как злоумышленники быстро создают новые адреса. В связи с этим сегодня востребованы системы обнаружения фишинга на основе нейронных сетей. Во время обучения нейронные сети могут распознавать такие особенности URL-адреса, как длина, спецсимволы и структура домена.

Для анализа и обучения нейросетевой модели был выбран набор данных «Malicious URLs dataset» с платформы Kaggle, включающий 651 191 URL-адрес. В данном датасете содержится 428 103 безопасных URL-адреса, 96 457 испорченных, 94 111 фишинговых и 32 520 URL-адреса, содержащего вредоносное ПО. Данные были собраны из пяти разнообразных источников, что позволяет обеспечить широкий спектр примеров. Это является ключевым аспектом при подготовке данных для проектов машинного обучения.

Для оптимизации работы на локальной машине и ускорения процесса обучения датасет был сокращен до 195 120 строк с равномерным распределением по всем классам.

Для векторизации URL-адресов использовался комбинированный подход, включающий следующие методы:

1. TF-IDF по символьным n-граммам (1–3).
2. OneHotEncoder (OHE) для доменных суффиксов.
3. Статистические признаки URL (длина, спецсимволы и др.).
4. Энтропия Шеннона для пути URL;
5. Символьные индексы домена (для анализа данных CNN).

Для решения задачи применялась нейросетевая модель, состоящая из нескольких компонентов:

1. CNN часть для обработки символьных последовательностей домена:
- слой эмбеддинга (размерность 32);
- два сверточных слоя (64 и 128 фильтров соответственно);
- Global Max Pooling для извлечения наиболее важных признаков.

2. Полносвязная часть для обработки структурированных признаков:
- отдельные полносвязные слои;
- слой объединения всех признаков из обоих ветвей;
- выходной полносвязный слой для финальной классификации;

3. В качестве функции активации выбрана функция ReLu.

4. В архитектуре модели используется функция dropout(0.3), которая случайным образом отключает 30 % нейронов на каждой итерации, тем самым снижая зависимость между нейронами.

Применение такой комбинированной архитектуры позволило достичь высокой точности классификации, так как сверточная часть эффективно выявляет паттерны в символьных последовательностях, а полносвязная часть обрабатывает статистические характеристики URL. Схема работы модели и графики процесса обучения представлены на рис. 1 и 2.

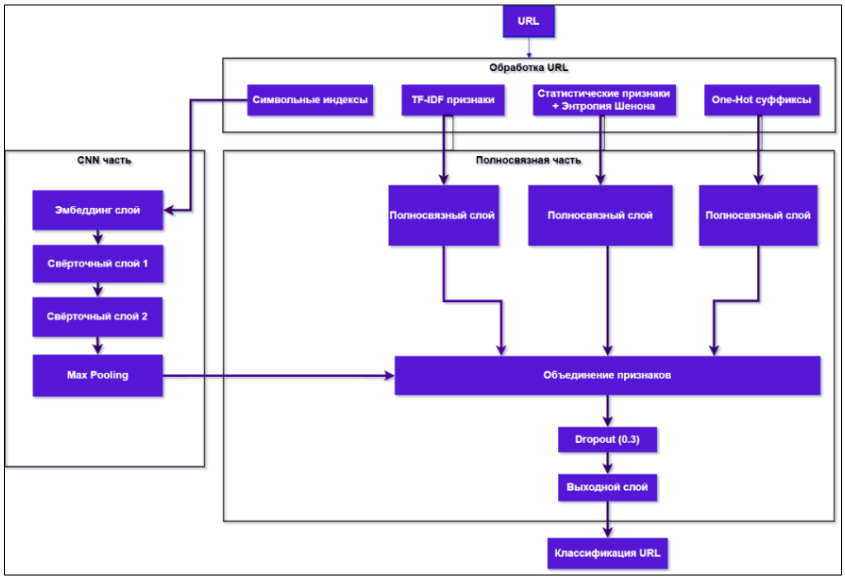

Рис. 1. Схема работы нейросетевой модели

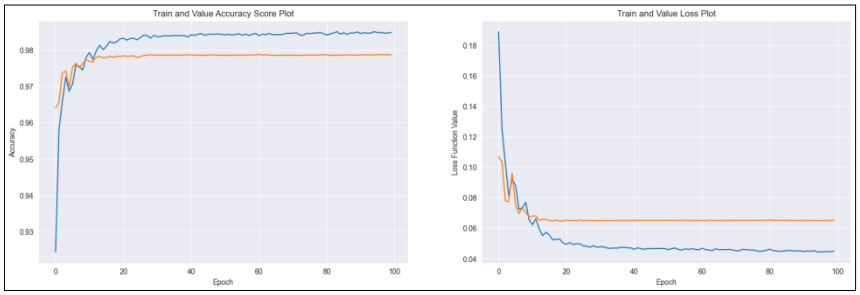

Рис. 2. График процесса обучения

Из графика видим, что на тренировочных данных точность обучения растет от 92,44 % до 98,48 %, а на валидационных – от 96,41 % до 97,87 %.

Разница между точностью на тестировочных и валидационных данных меньше 1 %, что указывает на отсутствие переобучения.

Значение функции потерь во время обучения на тренировочных данных падает от 0,1889 до 0,0449, а на валидационных – от 0,1068 до 0,0652. Функция потерь на валидационных данных не растет, а колеблется около 0.065, что также указывает на отсутствие переобучения.

Таким образом, модель демонстрирует стабильное обучение и хорошую обобщающую способность, успешно классифицируя URL-адреса.

Список использованных источников:

1. Тарасова Ю.А. Анализ проблемы фишинга в цифровом пространстве // Международный журнал прикладных и фундаментальных исследований. 2023. № 11. С. 56–60. URL: https://applied-research.ru/ru/article/view?id=13594 (дата обращения: 30.04.2025).
2. Механизм распознавания фишинговых сайтов по косвенным признакам // Молодой ученый. URL: https://moluch.ru/archive/318/72550/.
3. Mohammed Nazim Feroz, Susan Mengel Phishing URL detection using URL Ranking // Texas Tech University: 2015.
4. Корнюхина С.П., Лапонина О.Р. Исследование возможностей алгоритмов глубокого обучения для защиты от фишинговых атак. 2023.
5. Phishing URL Detection Using CNN-LSTM and Random Forest Classifier // Research Square. URL: https://www.researchsquare.com/article/rs-2043842/v1.

Yunusova D.S., Sutlanov D.Zh.
Ufa University of Science and Technology, Ufa

NEURAL NETWORK ANALYSIS OF URLS TO DETECT PHISHING ATTACKS

Abstract. Phishing URLs continue to be one of the most common tools in the cybercriminals' arsenal. This paper discusses a neural network model for recognizing phishing URLs, consisting of a CNN part for processing domain character sequences and a fully connected part for processing structured features.

Keywords: phishing, URL, neural network.

УДК 343.346.8:004.738.5(082.24)

Яковец Е.Н.
Российская таможенная академия, Люберцы

НЕКОТОРЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ НОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ

Аннотация. В статье рассматриваются вопросы информационно-аналитического обеспечения с использованием автоматизированных логико-аналитических систем в ходе противодействия терроризму и экстремизму. Анализируются проблемы, связанные с созданием интегрированного банка данных антитеррористического назначения и организацией межведомственного информационного взаимодействия в ходе борьбы с терроризмом и экстремизмом.

Ключевые слова: терроризм, экстремизм, автоматизированные логико-аналитические системы; искусственный интеллект; интегрированный банк данных антитеррористического назначения, межведомственное информационное взаимодействие.

Терроризм в наши дни продолжает оставаться общественно-политической проблемой номер один. Он создает проблемы безопасности для всего мира, детерминируя угрозы не только военного, но также экономического, политического и психологического свойства. Размах терроризма в современных условиях настолько широк, что для него не существует государственных границ. Террористы вооружены сегодня передовыми техническими средствами, многие из них в совершенстве владеют современными информационными технологиями. Так, по оценкам специалистов, технологическая вооруженность киберпреступников к 2026 г. позволит им осуществлять целенаправленные атаки на различные объекты критической информационной инфраструктуры с целью выведения их из строя и убийства людей. Как прогнозируют сотрудники исследовательской компании Gartner, использование боевых операционных технологий и других IT-систем только с учетом причинения смерти потерпевшим может нанести всем странам мира ущерб в размере более $50 млрд [1]. В связи с этим возникают вопросы: насколько эффективно Российская Федерация способна противодействовать данному вселенскому злу и что необходимо предпринять для повышения эффективности антитеррористической деятельности?

Российские спецслужбы и правоохранительные органы в борьбе с проявлениями терроризма должны эффективно использовать все имеющиеся организационно-тактические формы антитеррористической деятельности. Последствия любого проявления терроризма следует оперативно минимизировать и устранять. Для этого необходимо своевременно устанавливать организаторов и исполнителей терактов; незамедлительно предупреждать или пресекать их действия, а лиц, причастных к террористической деятельности, привлекать к строгой юридической ответственности. Силы и средства, предназначенные для этого, должны поддерживаться в постоянной оперативной готовности к их применению. Поэтому в местах массового скопления людей, нахождения важных объектов жизнеобеспечения, транспортных магистралей, пунктов пропуска через государственную границу, таможенных постов, также объектов оборонной и гражданской инфраструктуры и др. – должно быть организовано непрерывное наблюдение, сопряженное с оперативным распознанием физических лиц, причастных к террористическим актам, орудий и средств совершения преступлений, предметов двойного назначения, а также признаков самих преступных деяний.

Как известно, био- и нанотехнологии, квантовые вычисления, искусственный интеллект и прочие технологические новации используются

сегодня не только силовыми структурами, но и преступными элементами, в том числе и террористами. Этим самым последние нередко лишают правоохранителей их традиционных преимуществ. Американцы, например, вынуждены были приспосабливаться к этим тенденциям, поскольку так и не смогли победить исламских террористов не только в Афганистане и на Ближнем Востоке, но и в виртуальном пространстве [2, с. 19]. Возможно поэтому перед американскими силовыми структурами в свое время была поставлена глобальная задача – заполучить персональные биометрические данные, включая геномную информацию, всего населения Земного шара [3]. Правда, основные цели подобных шагов американцев до конца пока неясны и к проблемам противодействия терроризму они могут иметь лишь косвенное отношение. Тем не менее, если указанные данные будут использованы для обеспечения контроля за потенциальными террористами, то, безусловно, эти меры внесут существенный вклад в борьбу с данным серьезнейшим видом транснациональной преступности.

Однако в рассматриваемом нами контексте важны не только персональные биометрические данные физических лиц, имеющих причастность к терроризму и экстремизму, но и прочие сведения, имеющие прямое или косвенное отношение к этим людям. Речь в данном случае идет о так называемых «больших данных», накапливаемых в различных информационных массивах. Однако ограничиваться одним лишь накоплением подобных сведений нельзя, в противном случае они не принесут никакой пользы. Необходим их эффективный, тщательный анализ, осуществляемый в режиме реального времени. Единственным инструментарием, способным осуществлять анализ «больших данных», являются автоматизированные логико-аналитические системы (АЛАС), основанные на использовании искусственного интеллекта. Подобные системы уже давно и весьма эффективно применяются силовыми структурами как на Западе, так и на Востоке. Ю.Н. Жданов и В.С. Овчинский справедливо отмечают в этой связи, что искусственный интеллект (ИИ) создает принципиально новые возможности для правоохранительной деятельности и что особенно важно, – для обеспечения национальной безопасности государства. В настоящее время полиция ряда государств широко использует ИИ для сбора, классификации и анализа информации. Причем, при обработке сведений на первый план выходят принципиально новые, ранее не применявшиеся методы распознавания различных криминальных событий, и ближайшие годы станут временем тотальной экспансии методов применения ИИ в полицейской практике [4, с. 42].

В последнее время АЛАС, основанные на использовании ИИ, стали появляться и в России. Национальная стратегия развития искусственного интеллекта определяет ИИ как комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как мини-

мум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений, реализующих возможности ИИ, включает в себя информационно-коммуникационную инфраструктуру и программное обеспечение. К технологиям ИИ данная Стратегия относит в частности «компьютерное зрение», «обработку естественного языка», «распознавание и синтез речи», «интеллектуальную поддержку принятия решений» и «перспективные методы искусственного интеллекта» [5]. Без сомнения, АЛАС позволяют не только осуществлять анализ потокового видеоизображения в местах возможного появления террористов с целью оперативного распознания и отождествления последних, но и обрабатывать имеющие к ним отношение структурированные, неструктурированные и полуструктурированные данные, получаемые из самых различных источников. Что самое важное, отечественным специалистам, посвященным в данные проблемы, об этом было известно уже достаточно давно [6, с. 180–184].

Наряду с этим в рассматриваемом аспекте необходимо реализовать и другие организационные меры. В частности, большое значение для осуществления антитеррористических мер имеет создание в каждом ведомстве, прямо или косвенно вовлеченном в противоборство с терроризмом и экстремизмом, *интегрированного банка данных (ИБД) антитеррористического назначения,* призванного консолидировать различные сведения персонального и событийного характера. Зададимся вопросом: что должен представлять из себя подобный ИБД?

Под интеграцией при создании ИБД антитеррористического назначения следует понимать не простое механическое слияние множества малых учетов в один большой, а прежде всего, – создание единой информационной инфраструктуры, предназначенной для анализа сведений, обладателями которых являются различные субъекты информационного обмена соответствующих ведомств. В качестве приоритетной формы такого обмена, безусловно, должен рассматриваться удаленный доступ с использованием АЛАС.

Таким образом, следует создавать единую информационную инфраструктуру всех силовых ведомств, прямо или косвенно противодействующих терроризму и экстремизму. Для этого необходим *единый межведомственный интегрированный банк данных антитеррористического назначения.* Структурно он должен состоять из объединенных ИБД различных ведомств. Для того чтобы реализовать эту идею на практике, следует обратиться к опыту деятельности специального органа, функционирующего в каждом государстве Европейского Союза (ЕС), – Национального департамента по оперативным данным (НДОД) [7, с. 48–49.].

Список использованных источников:

1. Киберпреступники к 2025 г вооружатся технологиями для убийства людей // Securitylab.ru. 2021. 26 июля // URL: https://www.securitylab.ru/news/522696.php (дата обращения: 30.03.2025).

2. Кондрашов А. В виртуальной паутине. Как террористы и спецслужбы используют социальные сети // Аргументы недели. 2019. 16 мая. № 18(662). С. 19.

3. Рябова В. Дональд Трамп поручил ускорить внедрение биометрической системы на границах США. URL: d-russia.ru/donald-tramp-poruchil-uskorit-vnedrenie-biometricheskoj-sistemy-na-granitsah-ssha.html (дата обращения: 20.04.2025).

4. Жданов Ю.Н., Овчинский В.С. Киберполиция XXI века. Международный опыт / под ред. С.К. Кузнецова. М.: Международные отношения, 2020. 285 с.

5. Национальная стратегия развития искусственного интеллекта на период до 2030 г.: утв. Указом Президента РФ от 10 октября 2019 г. № 490. П. 5, подп. «а», «б» // URL: http://static.kremlin.ru/media/events/files/ru/AH4x6HgKWANwVtMOfPDhcbRpvd1HCCsv.pdf (дата обращения: 20.04.2025).

6. Яковец Е.Н., Журавленко Н.И. Искусственный интеллект в информационно-аналитической работе // Математические методы и информационно-технические средства [Электронный ресурс]: материалы XVIII Междунар. науч.-практ. конф. (17 июня 2022 г.) / редкол.: И.Н. Старостенко, Е.В. Михайленко, А.В. Еськов и др. Электрон. дан. Краснодар: Краснодарский университет МВД России, 2022. С. 180–184.

7. OSCE Guidebookon Intelligence-Ledpolicing. [Руководство ОБСЕ по полицейской деятельности на основе оперативных данных и информации] // Серия публикаций ДТНУ/ОСВПД. Вена, 2017. Т. 13. 106 с.

Yakovets E.N.
Russian Customs Academy, Lyubertsy

SOME ISSUES OF THE APPLICATION OF NEW INFORMATION TECHNOLOGIES IN THE FIELD OF COUNTERING TERRORISM

Abstract. The article discusses the issues of information and analytical support using automated logical and analytical systems in the course of countering terrorism and extremism. The problems associated with the creation of an integrated anti-terrorist database and the organization of interdepartmental information interaction in the fight against terrorism and extremism are analyzed.

Keywords: terrorism, extremism, automated logical and analytical systems; artificial intelligence; integrated anti-terrorist database, interdepartmental information interaction.

УДК 004

Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНИЗАЦИИ

Аннотация. Статья посвящена сравнительному анализу функций Security Operation Center (SOC) и их использованию в современных организациях. Рассматриваются основные аспекты создания и управления SOC, включая процессы мониторинга, обнаружения и реагирования на киберугрозы. В рамках статьи, также обсуждают технологические инструменты и методы анализа данных, необходимые для обеспечения безопасности информационных систем. В статье представлены практические рекомендации по оптимизации работы SOC и повышению эффективности защиты от кибератак.

Ключевые слова: Security Operation Center (SOC), информационная безопасность, процессы, мониторинг, реагирование, инциденты.

Совершенствование системы защиты информации в организации нуждается в модернизации. Одним из перспективных направлений этой работы является использовании достижений науки и техники. Сравнительно новым в этой связи является создание специализированных структур обеспечения информационной безопасности. Такой структурой может стать Security Operations Center (SOC) – центр обеспечения информационной безопасности, структурное подразделение организации, отвечающее за контроль IT-среды и предотвращение киберинцидентов. SOC – это самостоятельное подразделение, обеспечивающее мониторинг, обнаружение, анализ, реагирование и управление информационной безопасностью в организации. SOC используется для защиты от киберугроз и инцидентов информационной безопасности. Основные функции SOC включают в себя наблюдение за событиями в реальном времени, анализ аномальных активностей, обнаружение инцидентов информационной безопасности, реагирование на угрозы, сбор данных о безопасности, управление уязвимостями и инцидентами, а также обеспечение объекта на соответствие требованиям по безопасности информации. SOC обычно сочетает в себе технологии, процессы и высококвалифицированный персонал для обеспечения надежной защиты от киберугроз. Основная триада SOC – это процессы, люди и инструменты, то есть благодаря этим элементам функционирует любой SOC. Если убрать хоть один из элементов, то есть людей, процессы или инструменты, то SOC работать не будет.

SOC включает в себя ряд процессов, направленных на обеспечение безопасности информационных систем [1]. Вот некоторые из них:

1. Мониторинг и анализ: SOC проводит непрерывный мониторинг информационной инфраструктуры с использованием специализированных инструментов и технологий. Аналитики SOC анализируют данные, чтобы выявлять подозрительную активность и потенциальные угрозы.

2. Обнаружение инцидентов: SOC занимается обнаружением инцидентов безопасности, таких как вторжения, вредоносные программы и несанкционированный доступ к данным. Это включает в себя идентификацию аномальных событий и поведения в сети.

3. Реагирование на инциденты: При обнаружении инцидентов SOC принимает меры по реагированию, в том числе изоляции уязвимых узлов, блокированию угроз и восстановлению системной безопасности.

4. Управление уязвимостями: SOC отслеживает уязвимости в информационной инфраструктуре и занимается их решением, чтобы предотвратить возможные атаки.

5. Исправление инцидентов и улучшение процессов: SOC анализирует каждый инцидент, чтобы предотвратить его повторение в будущем, и внедряет улучшения в процессы и системы безопасности.

Перечисленные процессы работают в совокупности, они взаимно дополняют друг друга, и обеспечивают надежную защиту информационных ресурсов организации. При этом SOC использует различные инструменты автоматизации этих процессов для обеспечения более эффективной работы в борьбе с киберугрозами [2]. Некоторые из ключевых инструментов включают в себя:

1. SIEM (Security Information and Event Management): SIEM-системы предоставляют возможность собирать, анализировать и отображать данные о безопасности из различных источников. Они способны обнаруживать аномальное поведение и предупреждать об угрозах.

2. IDS/IPS (Intrusion Detection System/Intrusion Prevention System): Системы обнаружения и предотвращения вторжений позволяют идентифицировать атаки и предотвращать их до того, как они нанесут урон системе.

3. Автоматизированные инструменты анализа угроз: Эти инструменты помогают SOC быстро обрабатывать и анализировать большие объемы данных, выявлять угрозы и классифицировать их по степени угроз безопасности.

4. Автоматизированные системы управления уязвимостями: Эти системы сканируют сети и приложения на наличие уязвимостей, устанавливают патчи и обеспечивают обновления безопасности.

5. SOAR (Security Orchestration, Automation and Response): Технология SOAR используется для автоматизации рутинных задач безопасности, ускорения реагирования на угрозы и упрощения согласования действий между различными системами безопасности.

Названные инструменты способствуют автоматизации многих операций SOC, повышению эффективности и улучшению способности защиты от киберугроз [3].

Другой важной задачей функционирования SOC является комплектование высококвалифицированными кадрами. В SOC требуются специалисты с профессиональными навыками и компетенциями для обеспечения надежной защиты информационной безопасности. Так, большинство обеспечивающих фугкций в SOC выполняют:

– аналитики безопасности (Security Analysts): Они отвечают за мониторинг и анализ данных безопасности для выявления аномальной активности и угроз;

– инцидент-менеджеры (Incident Managers): Эти специалисты занимаются реагированием на инциденты безопасности, осуществляют координацию действий и управление инцидентами;

– инженеры безопасности (Security Engineers): Они работают над проектированием, развертыванием и обслуживанием систем безопасности, а также проводят технические расследования инцидентов;

– специалисты по управлению уязвимостями (Vulnerability Management Specialists): Эти специалисты отвечают за идентификацию, классификацию и устранение уязвимостей в информационной инфраструктуре;

– аналитики угроз (Threat Intelligence Analysts): Они отслеживают и анализируют современные киберугрозы, оценивают потенциальные риски и предоставляют контекст для событий безопасности.

Кроме того, в SOC необходим дополнительный персонал по управлению проектами, командный состав и руководители с высокой степенью ответственности за проделанную работу. Персональную ответственность за обеспечение эффективного управления и координации работ несет руководитель SOC (SOC Manager) или директор-администратор информационной безопасности (Chief Information Security Officer).

В отличие от MSSP (Managed Security Service Provider), где совсем по-другому организована защита информации, SOC подходит для крупных организаций с достаточными ресурсами для создания выделенной инфраструктуры. MSSP больше подходит для малого и среднего бизнеса, у которого нет ресурсов для поддержания внутреннего SOC. Вот некоторые принципиальные отличия SOC (Security Operations Center) от MSSP (Managed Security Service Provider):

1. Собственность и управление. SOC – внутренняя функция, которая напрямую управляется компанией. MSSP – сторонний поставщик услуг безопасности, компании обращаются к нему для аутсорсинга некоторых или всех функций безопасности.

2. Сфера услуг. SOC в основном фокусируется на непрерывном мониторинге, обнаружении угроз и реагировании на инциденты. MSSP предлагает широкий спектр услуг, включая управление брандмауэрами,

обнаружение вторжений, управление уязвимостями и мониторинг событий безопасности.

3. Настройка. SOC обеспечивает индивидуальную защиту с учетом конкретных рисков организации. MSSP использует стандартизированные протоколы для управления общими рисками среди клиентов.

4. Затраты. SOC требует значительных первоначальных инвестиций в инфраструктуру, передовые технологии и квалифицированный персонал. MSSP работает по модели регулярных платежей, предлагая более доступное начальное решение с предсказуемыми затратами со временем.

5. Человеческие ресурсы и экспертиза. SOC включает высокоспециализированные внутренние команды, которые глубоко понимают конкретный контекст организации. MSSP полагается на экспертов с навыками работы в разных секторах, которые работают с несколькими клиентами и отраслями.

6. Подход к работе. SOC функционирует внутри инфраструктуры компании, что позволяет быстро реагировать и тесно сотрудничать с внутренними ИТ-командами. MSSP работает удаленно с использованием безопасных инструментов управления.

Таким образом, Security Operations Center (SOC) представляет собой важное подразделение в организации, ответственное за обеспечение безопасности информационных систем. Через сочетание высокотехнологичных инструментов и компетентного персонала SOC обеспечивает обнаружение, реагирование и предотвращение киберугроз. Ключевые процессы в SOC включают мониторинг и анализ, обнаружение инцидентов, управление уязвимостями и улучшение процессов обеспечения информационной безопасности. Для эффективного функционирования SOC требуется команда специалистов с различными навыками в области информационной безопасности. Автоматизированные инструменты играют важную роль в повышении эффективности работы SOC и борьбы с киберугрозами. В целом, SOC является неотъемлемым компонентом в обеспечении безопасности информационных активов и защите от современных киберугроз.

Список использованных источников:

1. Белоус А.И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения: учебник / А.И. Белоус. М.: Техносфера, 2021. 483 с. ISBN 978-5-94836-612-8.

2. Гришина Н.В. Информационная безопасность предприятия: учебное пособие / Н.В. Гришина. М.: Форум: ИНФРА-М, 2018. 238 с. ISBN 978-5-00091-545-5.

3. Заботина Н.Н. Проектирование информационных систем: учебное пособие. М.: ИНФРА-М, 2020. 331 с. ISBN 978-5-16-104187-1.

Yapparov R.M.
Ufa University of Science and Technology, Ufa

ON THE ISSUE OF IMPROVING THE INFORMATION SECURITY SYSTEM IN THE ORGANIZATION

Abstract. The article is devoted to a comparative analysis of Security Operation Center (SOC) functions and their use in modern organizations. The main aspects of SOC creation and management, including the processes of monitoring, detecting and responding to cyber threats, are considered. The article also discusses the technological tools and data analysis methods necessary to ensure the security of information systems. The article provides practical recommendations for optimizing the operation of SOC and improving the effectiveness of protection against cyber attacks.

Keywords: Security Operation Center (SOC), information security, processes, monitoring, response, incidents.

СЕКЦИЯ 1. МАТЕМАТИЧЕСКИЕ МОДЕЛИ И МЕТОДЫ ЗАЩИТЫ, ПРЕОБРАЗОВАНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ

УДК 004

Аетбаева Р.Г., Файзуллина А.С.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Юнусова Д.С.
Уфимский университет науки и технологий, Уфа

ОБНАРУЖЕНИЕ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Аннотация. Данная статья рассматривает применение методов машинного обучения для выявления финансового мошенничества. Рассматриваются современные способы реализации угроз и роль искусственного интеллекта для борьбы с такими угрозами в банковской сфере.

Ключевые слова: искусственный интеллект, машинное обучение, финансовое мошенничество, мошеннические операции.

Угрозы мошенничества в банковской системе в современном мире неуклонно растут, становясь все более изощренными и сложными, тогда как традиционные методы обнаружения мошеннических операций часто оказываются неэффективными. Развитие банковских технологий, таких как онлайн-банкинг, мобильные платежи и криптовалюты, значительно упростило жизнь клиентов, но одновременно создало новые возможности для мошенников, использующих фишинговые атаки, социальную инженерию, кражу личных данных и изощренные приемы обмана банков и их клиентов. Традиционные методы выявления мошенничества, основанные на ручных проверках и простых правилах, не справляются с современными угрозами, часто приводят к ложным срабатываниям и не способны выявить сложные мошеннические схемы, требующие анализа больших объемов данных, что делает использование ИИ не просто желательным, а необходимым условием обеспечения финансовой безопасности, предоставляя банкам широкий спектр инструментов для борьбы с преступлениями на различных этапах финансовых операций.

Банки применяют ИИ для выявления мошеннических кредитных заявок. Данные, указанные в кредитной заявке, и информация из внешних источников анализируются, чтобы оценить риск мошенничества. Он также помогает банкам соблюдать требования законодательства по борьбе с незаконным оборотом денежных средств путем анализа транзакций, выявления подозрительных операций и оценки рисков. Большую роль

искусственный интеллект играет и в борьбе с кибератаками на банковские системы.

Рассмотрим конкретный пример анализа транзакций на наличие мошеннических операций, используя модель RandomForestClassifier, которая является основой большинства систем обнаружения мошенничества на основе ИИ. Алгоритмы МО обучаются на исторических данных о мошеннических и немошеннических операциях, чтобы выявлять закономерности и аномалии.

Для обучения был использован датасет, содержащий 6 362620 данных о смоделированных банковских транзакциях, на основе историй реальных операций. Датасет содержит следующие данные: тип транзакции, шаг (1 шаг равен 1 часу), код отправителя транзакции, идентификатор получателя транзакции, сумма транзакции, баланс до и после транзакции отправителя и получателя, является ли транзакция мошенничеством.

Транзакции разделены на 5 типов: вывод наличных, платеж, ввод наличных, перевод, дебет. Распределение транзакций по типам приведено на рис. 1.

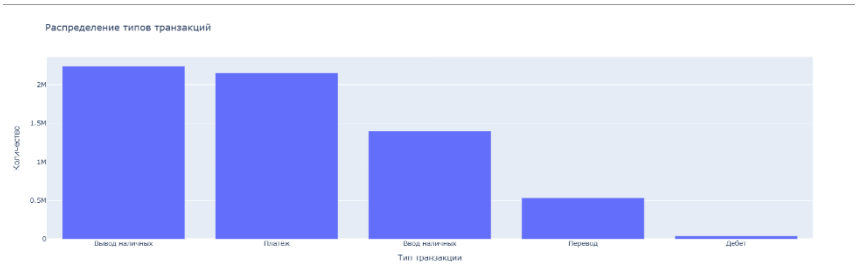

Рис. 1. Распределение типов транзакций

На основании результатов анализа корреляции между различными числовыми переменными и целевой переменной «Является_мошенничеством» составлена табл. 1.

Таблица 1

Корреляция

Сумма	0.076688
Шаг	0.031578
Старый_баланс_отправителя	0.010154
Новый_баланс_получателя	0.000535
Старый_баланс_получателя	-0.005885
Новый_баланс_отправителя	-0.008148

Анализ корреляции помогает выявить признаки, наиболее сильно связанные с мошенническими операциями. Таким образом, можем выявить, что сумма транзакции, шаг и старый баланс отправителя являются признаками, относительно которых можно определить является ли транзакция мошеннической.

Данные разделяются на обучающую и тестовую выборки. Для обучения используется модель Random Forest Classifier. Рассчитываются метрики качествамодели, такие как точность (accuracy), матрица ошибок (confusionmatrix) и отчет о классификации (classificationreport). Полученные значения приведены на рис. 2.

Рис. 2. Метрики качества модели

Этот пример демонстрирует, что искусственный интеллект может быть использован для обнаружения и предотвращения мошеннических транзакций. Так, с помощью модели RandomForestClassifier выявляются подозрительные операции на основе анализа различных признаков транзакции. Также такой метод помогает в анализе поведения клиентов. Анализ корреляции может показать, какие признаки поведения клиентов (например, изменение баланса, сумма транзакции) наиболее сильно связаны с мошенничеством.

Несмотря на огромный потенциал ИИ в борьбе с мошенничеством, существуют и определенные проблемы, и вызовы при его внедрении в банковский сектор:

- качество данных: в примере кода использовался готовый набор данных, реальных условиях необходимо обеспечить высокое качество данных, которые используются для обучения модели;
- интерпретируемость: важно понимать, почему модель приняла то или иное решение, RandomForest - относительно интерпретируемая модель, но более сложные модели (например, нейронные сети) могут быть «черными ящиками»;
- адаптация: мошенники постоянно разрабатывают новые методы, поэтому модель необходимо регулярно переобучать на новых данных.

Таким образом, банки, которые успешно внедрят ИИ, смогут значительно повысить свою безопасность, снизить финансовые потери и защитить своих клиентов от мошеннических действий. Дальнейшее развитие и распространение ИИ в банковском секторе несомненно приведет к появлению новых и более эффективных методов борьбы с мошенничеством, делая финансовую систему более безопасной и устойчивой.

Рассмотренный пример демонстрирует, как ИИ может быть применен для решения конкретной задачи в банковской сфере – выявлении мошеннических транзакций.

Список использованных источников:

1. Искусственный интеллект в банках. URL: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_в_банках (дата обращения: 15.04.2025).

2. Применение искусственного интеллекта на финансовом рынке России. URL: https://elibrary.ru/item.asp?id=54013778 (дата обращения: 16.04.2025).

Aetbaeva R.G., Fayzullina A.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yunusova D.S.
Ufa University of Science and Technology, Ufa

DETECTING FRAUDULENT TRANSACTIONS USING MACHINE LEARNING METHODS

Abstract. This article discusses the application of machine learning methods for detecting financial fraud. It examines modern ways that threats are executed and the role of artificial intelligence in combating such threats in the banking sector.

Keywords: artificial intelligence, machine learning, financial fraud, fraudulent activities.

УДК 004.056

Аминев Б.Р., Бурангулов Д.Б.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Фатхелисламов А.Ф.
Уфимский университет науки и технологий, Уфа

ВЫЯВЛЕНИЕ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ СБОРА ИНФОРМАЦИИ В ОПЕРАЦИОННОЙ СИСТЕМЕ КОМПЬЮТЕРА

Аннотация. В статье рассмотрено программное обеспечение LanAgent, представляющее собой кейлоггер, и его анализ с помощью Wireshark.

Исследованы методы выявления и удаления подобных программ, а также их влияние на локальную сеть. Особое внимание уделено скрытности работы кейлоггеров и способам защиты от них.

Ключевые слова: кейлоггер, сетевой трафик, шпионское ПО, информационная безопасность, анализ данных.

В наше время киберугрозы становятся все более распространенными и могут причинить серьезный вред как индивидуальным пользователям, так и компаниям. Одна из таких киберугроз это кейлоггеры.

Кейлоггеры – это программное или аппаратное средство, предназначенное для фиксации и сохранения всех нажатий клавиш на клавиатуре компьютера или другого устройства. Это может включать пароли, логины, личные сообщения, тексты документов и другие данные, которые пользователь вводит с клавиатуры.

Программы такого типа могут использоваться как в рамках закона, например, в корпоративной среде для мониторинга сотрудников, так и с нарушением законодательства, когда они используются для кражи личной информации. В данной научной статье рассматривается программное обеспечение для мониторинга за сотрудниками и то, как это программное обеспечение может использоваться злоумышленниками.

LanAgent – это программное обеспечение, предназначенное для скрытого мониторинга работы сотрудников внутри организаций. Он предназначен для отслеживания действий пользователей в сети, анализа их активности и обеспечения контроля над рабочими процессами. Программа часто используется администраторами и руководителями для повышения производительности труда сотрудников и оптимизации трудовых ресурсов.

Чтобы провести анализ работы кейлоггеров была скачена и установлена программа LanAgent на два ноутбука подключенные к локальной сети. Один из них был ноутбук простого пользователя. Второй ноутбук был администратора, который следил за пользователем. Предварительно на ноутбук пользователя был установлен анализатор сетевого трафика Wireshark и пользовательская версия программы LanAgent. Первое что бросается в глаза это то, что после установки пользовательской версии LanAgent нет никаких ярлыков приложения, создается только папка в каталоге C:\Windows\SysWOW64\LASys. На первый взгляд нет никаких отклонений в работе операционной системы, все работает так же, как и работало до этого. На устройство администратора была установлена административная версия программного обеспечения LanAgent. После установки программы на рабочем столе появилась не посредственно сама программа. LanAgent простейшее программное обеспечение, открыв программу можно легко добавить нового пользователя по его локальному IP адресу и сразу же начать отслеживать его действия. В программе можно применить настройки для

каждого пользователя отдельно. К примеру, у одного пользователя периодичность снимка экрана будет 5 минут, а у другого минута.

На ноутбуке пользователя это никак уведомлений о том, что за ним следят не будет. На работу операционной системы так же ничего не влияет, все работает в штатном режиме. Однако действия администратора в приложение можно отследить с помощью анализатора трафика Wireshark. Wireshark – это мощное и широко используемое программное обеспечение предназначенное для анализа сетевого трафика. Он позволяет изучать детали передачи данных в реальном времени. Данная программа может использоваться для анализа как проводных, так и беспроводных сетей. Это позволяет применять его в самых разных областях: от локальных офисных сетей до глобальных подключений через интернет.

При каждом изменение настроек или запрашивание «логов» со стороны администратора отслеживается подозрительная активность сетевого трафика. На работу это никак не влияет, но с помощью Wireshark можно заметить отравление и получение множества пакетов со стороны администратора пользователю и от пользователя администратору. С использованием анализатора сетевого трафика было установлено, что все собранные данные, включая текстовую информацию и снимки экрана, сохраняются локально на устройстве пользователя. Так информация на ноутбук администратора поступала не постоянно, он ее получал при обновление «логов» и сразу же после этого начинается отправка пакетов на ноутбук администратора.

Исходя из работы с Wireshark было установлено, что наличие кейлоггера можно выявить по следующим причинам: большие объемы исходящего трафика, подозрительные пакеты, отправляемые на неизвестные IP-адреса, используемые протоколы. Кейлоггер использовал такие протоколы, как HTTP/HTTPS (для отправки данных на удаленные серверы), TCP/UDP (для связи), FTP/SFTP (для загрузки файлов), SMTP (для отправки данных на электронную почту).

Другим способом выявления LanAgent является анализ всех активных приложений и системных процессов на пользовательском ноутбуке. Обычно такие процессы имеют необычные названия или не являются стандартными для операционной системы. При их анализе стоит обращать внимание на расположение исполняемого файла, его версию и информацию о разработчике. К тому же нужно учитывать показатели использования центрального процессор, памяти и сетевой активности. При обнаружении подозрительного процесса, выполнить поиск в интернете по его имени, чтобы проверить является ли он вредоносным ПО.

На ряду с этим для выявления кейлоггера можно использовать специальные утилиты для дополнительного поиска шпионского ПО. Использование обычных антивирусных программ может не дать желаемого результата, так как LanAgent будет рассматриваться ими как обычное приложение, не являющееся вредоносным ПО.

Избавиться от кейлоггера в нашем случае можно через пакет установщика. Проводится вся таже процедура с установкой, но только при повторном открытие установщика программа сама предлагает удалить себя. В случае, когда нет доступа к пакету установщика стоит открыть диспетчер задач и в фоновых задачах искать подозрительные задачи. У нас эта задача system.exe (32 bit). Проведен анализ информации о данном процессе с использованием интернет-ресурсов, в результате которого был сделан вывод о его принадлежности к категории вредоносного программного обеспечения. Затем перешли в расположение папки, завершили задачу процесса и в безопасности папки выдали полный доступ пользователю. Впоследствии нам удалось удалить папку с кейлоггером.

В рамках проведенного исследования мы детально изучили функционал программы LanAgent, которая представляет собой кейлоггер. Особое внимание уделялось ее влиянию на локальную сеть и взаимодействию между устройствами пользователей и администраторов. Анализ показал, что данное программное обеспечение обладает высокой степенью скрытности: оно не отображается в списке активных приложений, не создает уведомлений для пользователя и работает в фоновом режиме, не оказывая заметного влияния на производительность системы.

Кроме того, исследование позволило определить способы обнаружения и удаления кейлоггеров. Один из подходов заключается в анализе процессов операционной системы, где ключевыми признаками являются нестандартные названия исполняемых файлов, их расположение и аномальная нагрузка на системные ресурсы. К тому же было установлено, что использование специализированных утилит для поиска шпионского ПО может быть более результативным, чем применение классических антивирусных решений, которые зачастую не распознают подобные программы как угрозу.

Список использованных источников:

1. Баланов А.Н. Кибербезопасность: учебное пособие для вузов. 2-е изд., стер. М.: Издательство «Лань», 2025. 680 с. ISBN 978-5-507-52709-0.

2. Голубцов И.С., Голубцова Е.С. Кейлоггеры: Электрон. версия. М.: Общество с ограниченной ответственностью «Интернаука», 2021. Студенческий вестник. № 17-6 (162). С. 56–57. URL: https://www.elibrary.ru/item.asp?id=45795122 (дата обращения: 05.04.2025)

3. Давидюк Н.В., Космачева И.М. Мониторинг безопасности информационных систем: практикум для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» и направлений 10.03.01 «Информационная безопасность», 10.04.01 «Информационная безопасность». М.: ИЦ Интермедия, 2020. 116 с.

4. Николаева М.О. Информационная безопасность: современная картина проблемы информационной безопасности и защиты информации: Электрон. версия. Челябинск: Челябинский институт развития

профессионального образования, 2023. Т. 1, № 1. С. 51–57. URL: https://www.elibrary.ru/item.asp?id=54211958 (дата обращения: 06.04.2025).

5. Wireshark – подробное руководство по началу использования. URL: https://habr.com/ru/articles/735866/ (дата обращения: 10.04.2025).

6. Руководство пользователя LanAgent Terminal. URL: https://lanagent.ru/documents/manual_terminal.pdf (дата обращения: 04.04.2025).

7. Бабанов Н.Ю., Евстифеев А.А., Мартынов А.П., Николаев Д.Б., Фомченко В.Н. Основы защиты информации в современных информационных системах: учебное пособие. М.: Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики, 2022. 175 с.

8. Крыгин Н.Д. Шпионское программное обеспечение // Донской государственный технический университет, 2022. Столыпинский вестник. Т. 4, № 4. Порядковый номер 11. URL: https://www.elibrary.ru/item.asp?id=49403090 (дата обращения: 05.04.2025).

Aminev B.R., Burangulov D.B.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhelislamov A.F.
Ufa University of Science and Technology, Ufa

IDENTIFICATION OF MALICIOUS SOFTWARE FOR COLLECTING INFORMATION IN THE COMPUTER'S OPERATING SYSTEM

Abstract. The article discusses LanAgent software, which is a keylogger, and its analysis using Wireshark. The methods of detecting and removing such programs, as well as their impact on the local network, are investigated. Special attention is paid to the secrecy of keyloggers and ways to protect against them.

Keywords: keylogger, network traffic, spyware, information security, data analysis.

УДК 004.056

Аникин С.А.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

Научный руководитель:
Козырева Н.И.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

ПРИМЕНЕНИЕ МЕТОДА ХОЛЬТА-ВИНТЕРСА ДЛЯ ПРОГНОЗИРОВАНИЯ КОЛИЧЕСТВА СЕТЕВЫХ АТАК

Аннотация. В работе рассматривается применение метода Холта-Винтерса для прогнозирования кибератак. Исследуются аддитивная и мультипликативная модели, позволяющие учитывать тренд и сезонность в данных о киберугрозах. Приведены основные формулы метода, а также проведен анализ их применимости для задач информационной безопасности.

Ключевые слова: прогнозирование кибератак, метод Холта-Винтерса, аддитивная модель, мультипликативная модель, временные ряды, информационная безопасность.

Прогнозирование сетевых атак с помощью статических методов – это одна из ключевых техник в области информационной безопасности. Статические методы, в отличие от динамических, не требуют анализа поведения системы в реальном времени. Вместо этого они основаны на предварительном анализе данных, которые не изменяются во времени, и использованию различных алгоритмов для выявления уязвимостей и угроз.

Современные киберугрозы обладают выраженной временной динамикой и сезонными паттернами, что делает методы анализа временных рядов, в частности подход Хольта-Винтерса, перспективным инструментом для прогнозирования атак на основе исторических данных, выявления аномальной активности в сетевом трафике и эффективного использования ресурсов систем защиты. Практическая реализация может достигаться путем сбора исторических данных об атаках, выявления сезонности.

Вопрос выбора модели метода Хольта-Винтерса зависит от характера анализируемых данных и типа угроз. Мультипликативная модель будет применяться при:

- растущей амплитуде колебаний (например, объем DDoS-атак, который увеличивается пропорционально общему трафику);
- при анализе интенсивности атак, где сезонные всплески усиливаются с ростом базового уровня угроз;

• для финансовых показателей киберпреступности (объемы украденных средств).

Пример использования: прогнозирование пиков фишинговых атак в предпраздничные периоды, когда их количество растет в процентном соотношении к базовому уровню.

Аддитивная модель:

• для показателей с постоянной амплитудой колебаний (например, количество попыток сканирования портов);

• при мониторинге рутинных угроз с устойчивыми сезонными паттернами;

• для показателей, где сезонные колебания не зависят от базового уровня.

Пример: прогнозирование суточной активности бот-сетей, где ночные атаки всегда превышают дневные на примерно постоянную величину.

Было рассмотрено две модели посредствам языка программирования python3, с целью изучения и прогнозирования возможных атак. Исходные данные были взяты из отчетов компании ddos-guard [3]. Поскольку в рассматриваемом случае не наблюдается постоянной амплитуды колебаний, то аддитивную модель можно не рассматривать.

Математическая форма аддитивной модели записи имеет вид [2]:

$$L_t = \alpha \cdot (Y_t - S_{t-s}) + (1 - \alpha) \cdot (L_{t-1} + T_{t-1}), \quad (1)$$

$$T_t = \beta \cdot (L_t - L_{t-1}) + (1 - \beta) \cdot T_{t-1}, \quad (2)$$

$$S_t = \gamma \cdot (Y_t - L_t) + (1 - \gamma) \cdot S_{t-m}, \quad (3)$$

$$\acute{Y}_{t+h} = L_t + h \cdot T_t + S_{s+t-m}\ , \quad (4)$$

где Y_t – фактическое значение в момент времени t; L_t – уровень в момент времени t; T_t – тренд в момент времени; S_t – сезонность в момент времени t; $\alpha,\ \beta, \gamma$ – параметры сглаживания, которые определяют вес каждого компонента; h – это количество периодов вперед, на которые нужно сделать прогноз; m – длина сезонного периода.

Математическая запись мультипликативной модели имеет следующий вид и описывается формулами 5–8 [1].

$$L_t = \alpha \cdot \frac{Y_t}{S_{t-s}} + (1 - \alpha) \cdot (L_{t-1} + T_{t-1}), \quad (5)$$

$$T_t = \beta \cdot (L_t - L_{t-1}) + (1 - \beta) \cdot T_{t-1}, \quad (6)$$

$$S_t = \gamma \cdot \frac{Y_t}{L_t} + (1 - \gamma) \cdot S_{t-m}, \quad (7)$$

$$\acute{Y}_{t+h} = (L_t + h \cdot T_t) + S_{s+t-m}\ , \quad (8)$$

где Y_t – фактическое значение в момент времени t; L_t – уровень в момент времени t; T_t – тренд в момент времени; S_t – сезонность в момент времени t; $\alpha,\ \beta, \gamma$ – параметры сглаживания, которые определяют вес каждого компонента; h – это количество периодов вперед, на которые нужно сделать прогноз; m – длина сезонного периода.

Проведенное исследование выявило ключевые ограничения классических методов прогнозирования временных рядов, в частности модели Хольта-Винтерса, для задач информационной безопасности.

В качестве перспективы можно выделить разработку гибридных систем, учитывающие тренд аномалии и внешние факторы, а также модели способные адаптироваться к новым угрозам.

Список использованных источников:

1. А. С. Поздняков. Применение метода Хольта-Винтерса при анализе и прогнозировании динамики временных рядов. URL: https://masters.donntu.ru/2017/fknt/vudvud/library/article6.pdf (дата обращения 10.01.2025).

2. Прогноз по методу экспоненциального сглаживания с трендом и сезонностью (Хольта-Винтерса) // 4Analytics: [сайт]. URL: https://4analytics.ru/prognozirovanie/prognoz-po-metodu-eksponencialnogo-sglajivaniya-s-trendom-i-sezonnostyu-xolta-vintersa.html (дата обращения: 10.01.2025).

3. Статистика DDoS-атак: [ежеквартальные отчеты] / DDoS-Guard. URL: https://ddos-guard.ru/reports (дата обращения: 09.01.2025).

Anikin S.A.
Volga Region State University of Telecommunications and Informatics, Samara

Scientific supervisor:
Kozyreva N.I.
Volga Region State University of Telecommunications and Informatics, Samara

INVESTIGATION OF THE HOLT-WINTERS METHOD FOR PREDICTING THE NUMBER OF NETWORK ATTACKS

Abstract. This paper explores the application of the Holt-Winters method for forecasting cyberattacks. The additive and multiplicative models are examined, enabling the analysis of trends and seasonality in cyber threat data. Key formulas of the method are presented, along with an evaluation of their applicability in cybersecurity tasks. The study demonstrates the effectiveness of this approach for short- and medium-term attack prediction, which can support the development of proactive defense measures.

Keywords: cyberattack forecasting, Holt-Winters method, additive model, multiplicative model, time series analysis, cybersecurity.

УДК 004

Гаврилова А.А., Мусина К.Ш.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Юнусова Д.С.
Уфимский университет науки и технологий, Уфа

ОПРЕДЕЛЕНИЕ И ОБНАРУЖЕНИЕ DDoS-АТАК С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Аннотация. В статье представлено исследование применения различных методов машинного обучения для обнаружения DDoS-атак на основе анализа сетевого трафика. Проводится сравнительный анализ производительности моделей Random Forest, Bagging, AdaBoost, XGBoost, LightGBM, CatBoost с использованием метрик Accuracy, Precision, Recall, F1 и ROC-AUC. Целью работы является определение наиболее эффективного метода для раннего обнаружения и предотвращения DDoS-атак.

Ключевые слова: DDoS-атаки, кибербезопасность, машинное обучение, анализ сетевого трафика, предотвращение атак, Accuracy, Precision, Recall, F1, ROC-AUC.

Обеспечение надежной защиты сетевой инфраструктуры критически важно для предприятий различного масштаба ввиду возрастающего риска возникновения DDoS-атак. Классические способы противодействия данным угрозам зачастую недостаточно эффективны, что обусловлено постоянным усложнением и увеличением объемов атак. Один из перспективных путей улучшения ситуационной осведомленности и раннего реагирования на подобные инциденты заключается в применении методов машинного обучения, обладающих возможностью автоматически анализировать сетевой трафик и выделять характерные паттерны поведения, присущие DDoS-атаке.

Статья направлена на решение задачи определения и выявления DDoS-атак с использованием методов машинного обучения. Основой исследования послужил открытый набор данных, состоящий из записей сетевого трафика, собранных в процессе наблюдения за деятельностью злоумышленников. Общий объем набора составляет 1048444 записей, каждая из которых описывает отдельные события сетевого взаимодействия, включая протоколы верхних уровней и транспортных слоев, IP-адреса отправителей и получателей, порты соединений, размеры передаваемых пакетов и интервал времени между передачами.

Предварительно была проведена обработка данных. Реализована процедура исключения полей с IP-адресами отправителя и получателя, поскольку эти данные не оказывают прямого влияния на природу сетевого

трафика и способствуют увеличению вычислительной нагрузки без увеличения информативности. Отсутствующие значения были заполнены средним значением соответствующего столбца, используя метод mean imputation. Средняя величина дает нейтральную оценку отсутствующему значению, минимизируя возможные смещения в дальнейшей оценке.

Категориальные признаки, такие как протоколы высших и нижних уровней, были переведены в числовую форму с помощью OneHotEncode. Данная техника преобразования позволила сохранить всю необходимую информацию о категориях и подготовить данные для ввода в модели машинного обучения.

Выбор конкретных методов объясняется их популярностью и доказанной эффективностью в аналогичных задачах. Были использованы следующие алгоритмы:

– Random forest: базируется на создании ансамбля решающих деревьев, способных одновременно решать задачи классификации и регрессии, устойчив к переобучению и работает быстро даже с большими объемами данных;

– Bagging classifier: является простым и эффективным способом повышения точности за счет уменьшения вариативности базовой модели;

– Adaboost: алгоритм адаптивного бустинга, последовательно улучшая точность за счет коррекции ошибок предыдущих итераций;

– Xgboost: оптимизированная реализация градиентного бустинга, популярная в соревнованиях по анализу данных благодаря высокой скорости и качеству работы;

– Lightgbm: еще одна версия градиентного бустинга, известная своим быстрым временем обучения и низкими требованиями к ресурсам;

– CatBoost: выделяется высоким качеством работы с категориальными признаками и отсутствием необходимости специальной предобработки данных.

Данные были разделены на обучающую (70 %) и тестовую (30 %) выборки с использованием параметра stratify=y в функции train_test_split(). Данный параметр гарантирует сохранение первоначального распределения классов в обеих выборках, что предотвращает смещение результатов. Такое разделение оптимально, так как оно обеспечивает достаточную долю данных для качественного обучения модели и позволяет провести независимую проверку ее способностей к обобщению на незнакомые образцы. Модели были обучены на обучающей выборке, а их производительность оценивалась с использованием метрик точности (accuracy), точности позитивных предсказаний (precision), чувствительности (recall), меры F1 и показателя ROC-AUC.

В табл. 1 представлены результаты оценки производительности методов машинного обучения при обнаружении DDoS-атак на основе анализа сетевого трафика, где сравнивались значения Accuracy, Precision, Recall, F1 и ROC-AUC.

Таблица 1

Оценка производительности методов машинного обучения

	Accuracy	Precision	Recall	F1	ROC-AUC
CatBoost	0,998073	0,999101	0,996765	0,997932	0,999993
XGBoost	0,998022	0,998548	0,997209	0,997878	0,999993
LightGBM	0,998006	0,999051	0,996673	0,997860	0,999993
Bagging Classifier	0,998026	0,998624	0,997142	0,997882	0,999993
Random Forest	0,998026	0,998624	0,997142	0,997882	0,999993
AdaBoost	0,994781	0,988944	0,999992	0,994437	0,999956

По итогам проведенного исследования выяснилось, что лучшие результаты обеспечивали ансамблевые методы CatBoost и XGBoost, стабильно демонстрируя самую высокую общую точность и лучшую обобщающую способность. Оба метода достигли показателя точности более 99 %, что фактически соответствует уровню практической полезности для реальных систем мониторинга и защиты. Менее выраженные различия наблюдались между другими моделями, такими как Random Forest, Bagging Classifier и LightGBM, которые также дали хорошие результаты, но незначительно уступали двум лидирующим моделям.

Важно подчеркнуть, что такая высокая точность достигается благодаря уникальной архитектуре и оптимизации данных моделей, что позволяет учитывать широкий спектр признаков и успешно выявлять даже небольшие отклонения в поведении сетевого трафика, ассоциированные с DDoS-атаками.

Анализируя результаты моделей, можно выделить несколько ключевых признаков, которые могут указывать на наличие DDoS-атаки:

– частота пакетов (Packets/Time): в случае DDoS-атаки наблюдается резкое увеличение количества пакетов в единицу времени, что создает аномальную нагрузку на сеть;

– протоколы (Highest Layer, Transport Layer): использование специфичных протоколов, таких как ARP или ICMP, может свидетельствовать о попытках перегрузки сети;

– длина пакета (Packet Length): необычные размеры пакетов, особенно если они значительно отличаются от типичного сетевого трафика, могут сигнализировать о подозрительной активности.

Эти признаки играют ключевую роль в определении наличия DDoS-атаки, позволяя моделям машинного обучения эффективно распознавать аномалии в сетевом трафике.

Таким образом, данная работа иллюстрирует успешность применения методов машинного обучения для разработки эффективных систем выявления DDoS-атак. Рассмотренный подход открывает перспективы для

интеграции интеллектуальных аналитических модулей в корпоративные системы безопасности, повышая устойчивость и защищенность инфраструктуры от растущих угроз.

Список использованных источников:

1. Иванникова В.П. Бинарная классификация компьютерных атак на примере базы данных UNSW-NB15 / В.П. Иванникова, О.И. Шелухин // Телекоммуникации и информационные технологии. 2020. Т. 7, № 1. С. 10–18.

2. Колосов И.А. Классический подход решения задачи бинарной классификации / И.А. Колосов, К.Т. Джахангирова // Научный аспект. 2024. Т. 3, № 6. С. 278–283.

Gavrilova A.A., Musina K.S.
Ufa University of Science and Technology, Ufa, Russia

Scientific supervisor:
Yunusova D.S.
Ufa University of Science and Technology, Ufa, Russia

IDENTIFICATION AND DETECTION OF DDoS ATTACKS USING MACHINE LEARNING METHODS

Abstract. The article presents a study of the use of various machine learning methods for detecting DDoS attacks based on network traffic analysis. A comparative analysis of the performance of the Random Forest, Bagging, AdaBoost, XGBoost, LightGBM, and CatBoost models is carried out using Accuracy, Precision, Recall, F1, and ROC-AUC metrics. The aim of the work is to determine the most effective method for early detection and prevention of DDoS attacks.

Keywords: DDoS attacks, cybersecurity, Machine learning, network traffic analysis, attack prevention, Accuracy, Precision, Recall, F1, ROC-AUC.

УДК 004.056

Галимова А.Р., Домрачева В.Е.,
Шарафутдинов Б.И., Ямилова А.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Валеев С.С.
Уфимский университет науки и технологий, Уфа

ОСОБЕННОСТИ КВАНТОВЫХ МЕТОДОВ КРИПТОГРАФИИ: ПРИНЦИПЫ, РЕАЛИЗАЦИЯ И ПЕРСПЕКТИВЫ

Аннотация. В статье рассматриваются особенности квантовой криптографии и протокола BB84, а также их отличие от традиционных методов. Анализируются принципы квантовой механики, лежащие в основе распределения ключей (КРК), такие как принцип Гейзенберга и квантовая суперпозиция. Описаны существующие системы КРК, их плюсы и минусы. Обсуждаются перспективы развития квантовой криптографии и ее роль в защите информации будущего.

Ключевые слова: квантовая криптография, квантовое распределение ключей (КРК), протокол BB84, квантовая суперпозиция, принцип неопределенности, кубиты, безопасность информации.

В условиях усиления угроз кибербезопасности, обусловленных развитием вычислительной техники, в том числе квантовых компьютеров, традиционные криптографические методы становятся все более уязвимыми. Квантовая криптография, использующая законы квантовой механики для защиты передаваемой информации [1]. Основным направлением является квантовое распределение ключей (КРК), позволяющее двум сторонам установить общий секретный ключ, устойчивый к перехвату [2–4]. КРК основывается на двух принципах квантовой механики: квантовой суперпозиции: кубит (наименьшая единица в информации) может одновременно представлять значения 0 и 1, описывается вектором состояния

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{ где } |\alpha|^2 + |\beta|^2 = 1,$$

и принципе неопределенности Гейзенберга. Измерение кубита изменяет его состояние, что позволяет обнаружить любые попытки взлома сообщения.

Протокол BB84. Протокол квантового распределения ключей в котором используется для кодирования информации четыре квантовых состояния двухуровневой системы, формирующие два сопряженных базиса. Носителями информации являются 2-уровневые системы, называемые кубитами (квантовыми битами). Протокол включает следующие этапы:

– подготовка и передача кубитов: например, Алиса генерирует случайные биты, кодирует их в кубиты с использованием двух базисов и отправляет Бобу;

– измерение кубитов: например, Боб измеряет кубиты, выбирая один из базисов;

– объявление базисов: например, Алиса и Боб обмениваются информацией о использованных базисах, сохраняя только согласованные биты;

– оценка ошибок: например, Алиса и Боб сравнивают часть согласованных битов для выявления ошибок;

– исправление ошибок: например, если уровень ошибок приемлем, применяются протоколы исправления.

– усиление приватности: например, Алиса и Боб используют методы для получения абсолютно секретного ключа.

Рассмотрим далее основные методы реализации протокола КРК.

Существуют разные реализации КРК систем, каждая из которых имеет свои плюсы и минусы:

– волоконно-оптические системы: передают фотоны по оптическому волокну, но ограничены расстоянием из-за потерь;

– спутниковые системы: используют спутники для передачи на большие расстояния, нуждаются в специальном оборудовании и подвержены атмосферным влияниям;

– системы свободного пространства: передают фотоны с помощью лазерных лучей в атмосфере, требуют прямой видимости и также подвержены влиянию погоды.

Рассмотрим далее основные преимущества и недостатки методов квантовой криптографии. Преимущества этого метода:

– высокий уровень защиты передаваемых сообщений: КРК гарантирует безопасность, опираясь на фундаментальные принципы физики, а не на вычислительную сложность математических алгоритмов;

– устойчивость к взлому алгоритмов: QKD не зависит от криптографических алгоритмов, потенциально уязвимых в будущем.

Основные недостатки метода:

– ограничения дистанции передачи сообщений: потери в квантовой среде ограничивают дальность передачи ключей, что требует применения квантовых ретрансляторов;

– техническая сложность реализации: развертывание КРК-систем требует использования специализированного и дорогостоящего оборудования;

– совместимость: КРК-системы требуют специальной инфраструктуры и не совместимы с существующими классическими сетями связи.

Квантовая криптография обладает значительным потенциалом для защиты информации. Ожидается дальнейшее развитие QKD-систем,

включая увеличение дальности, скорости генерации ключей и снижение стоимости. Она может защитить важные объекты инфраструктуры, банковские системы и государственные сети.

Квантовая криптография – это революционный подход к информационной безопасности, основанный на квантовой механике. Протокол BB84 лежит в основе современных QKD-систем. Несмотря на ограничения, квантовая криптография может сыграть важную роль в защите информации, особенно в условиях угроз со стороны квантовых компьютеров.

Список использованных источников:

1. Bennett C.H., & Brassard G. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984. P. 175–179.

2. Scarani V., Bechmann-Pasquinucci H., Cerf N.J., Dušek M., Lütkenhaus N., & Peev, M., 2009. The security of practical quantum key distribution. Reviews of Modern Physics, 81(3), 1301.

3. Gisin N., Ribordy, G., Tittel, W., & Zbinden H. Quantum cryptography. Reviews of Modern Physics, 2002, 74 (1), 145.

4. Lütkenhaus N. (2018). Quantum key distribution. Nature Physics, × 14 × (12), 1168–1170. URL: https://arxiv.org/pdf/1905.09197v2.

Domracheva V.E., Galimova A.R.,
Sharafutdinov B.I., Iamilova A.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Valeev S.S.
Ufa University of Science and Technology, Ufa

FEATURES OF QUANTUM CRYPTOGRAPHY METHODS: PRINCIPLES, IMPLEMENTATION, AND PROSPECTS

Abstract. The article discusses the features of quantum cryptography and the BB84 protocol, as well as their differences from traditional methods. The principles of quantum mechanics underlying key distribution (QKD), such as the Heisenberg principle and quantum superposition, are analyzed. The existing QKD systems, their pros and cons are described. The prospects for the development of quantum cryptography and its role in protecting the information of the future are discussed.

Keywords: quantum cryptography, quantum key distribution (QKD), BB84 protocol, quantum superposition, uncertainty principle, qubits, information security.

УДК 004.4: 519.7

Галиуллин Р.Р., Кулдавлетов А.И.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Валеев С.С.
Уфимский университет науки и технологий, Уфа

РАЗРЕЖЕННОСТЬ ДАННЫХ И СЖАТИЕ РАЗМЕРНОСТИ

Аннотация. Статья посвящена анализу разреженности данных как важного аспекта в современных задачах машинного обучения. Рассматриваются причины разреженности, ее влияние на качество моделей и методы эффективной обработки, включая сокращение размерности с использованием PCA. Подчеркивается двойственный характер разреженности как проблемы и источника структурной информации.

Ключевые слова: разреженность данных, PCA, сокращение размерности, машинное обучение, регуляризация, высокоразмерные данные, интерпретируемость моделей.

Большие данные редко бывают полными и равномерно распределенными: зачастую они содержат значительное количество нулевых, отсутствующих или малозначимых значений. Такая неоднородность структуры приводит к явлению, которое называют разреженность данных, т.е. значительная часть информации фактически не несет полезной нагрузки или просто отсутствует.

Разреженность данных является одной из ключевых проблем современной аналитики и машинного обучения. Она напрямую влияет на качество и скорость работы алгоритмов, а также на объем ресурсов, необходимых для хранения и обработки информации. Однако сама по себе разреженность не всегда негативное явление: в ряде случаев она может быть использована в качестве источника структурных признаков, отражающих скрытую закономерность в данных. Поэтому важно не только уметь определять степень разреженности, но и грамотно работать с такими структурами.

Актуальность темы обусловлена тем, что современные интеллектуальные системы – от рекомендательных алгоритмов до нейросетей – часто работают с разреженными данными. Понимание природы разреженности, ее последствий и методов обработки необходимо для разработки устойчивых, производительных и интерпретируемых моделей. Важно учитывать не только форму, но и причины ее возникновения.

Разреженность – это свойство данных, при котором большинство элементов являются нулями, пропущенными или неинформативными значениями. Такая структура характерна для анализа больших данных и

проявляется по-разному: от отсутствующих значений до неравномерного распределения признаков. Осознание причин позволяет лучше понять влияние разреженности на обучение моделей и качество анализа.

Характерный пример – матрицы взаимодействия в рекомендательных системах, где пользователи взаимодействуют лишь с небольшой частью объектов, оставляя большинство ячеек пустыми. Аналогично, в задачах обработки текста модель «мешка слов» создает векторы, заполненные нулями, так как каждый документ содержит лишь малую долю слов из общего словаря. То же наблюдается в высокоразмерных данных, где большинство признаков неактивны для конкретного объекта. Однако разреженность – это не только вызов, но и источник ценной информации. Перейдем к ее положительным аспектам.

Причинами разреженности часто становятся как природа самих данных, так и особенности способов их представления. Например, в пользовательском поведении отсутствует физическая возможность охватить все варианты выбора, а в текстах – естественное ограничение на объем и тематику. Кроме того, разреженность может возникать искусственно, в результате использования обобщенных моделей и признакового кодирования.

Разреженность данных может восприниматься как нежелательное явление, однако ее влияние на анализ и обучение моделей носит двойственный характер. С одной стороны, высокая доля нулевых или пропущенных значений может существенно затруднить извлечение закономерностей. Алгоритмы машинного обучения, сталкиваясь с неполными или нерепрезентативными признаками, подвержены переобучению, особенно в условиях ограниченного объема выборки. Кроме того, обработка разреженных структур требует увеличенных вычислительных ресурсов при использовании стандартных представлений, так как даже пустые элементы необходимо учитывать в памяти и при выполнении операций. Одним из таких методов является сокращение размерности, для чего часто используют метод главных компонент.

С другой стороны, разреженность может быть интерпретирована как форма упорядоченности. В ряде задач она помогает акцентировать внимание на наиболее значимых признаках, отбрасывая избыточные данные. При кооректной реализации, например, с использованием специализированных форматов хранения или методов отбора признаков, разреженные данные позволяют существенно сократить объем памяти и ускорить вычисления. Более того, такие структуры оказываются особенно полезными при построении интерпретируемых моделей, где важны именно редкие, но информативные признаки.

Эффективная работа с разреженными данными требует применения специализированных методов, направленных на уменьшение избыточности и повышение информативности признаков. Одним из базовых подходов является удаление нерелевантных или слабо

вариативных признаков, которые не вносят значимого вклада в обучение модели. Это позволяет сократить размерность пространства и снизить риск переобучения. В случае наличия пропущенных значений возможны различные стратегии их обработки: от простых методов заполнения средними значениями до использования моделей, прогнозирующих недостающие данные на основе имеющихся.

Важным инструментом является регуляризация, особенно в задачах с большим количеством признаков. Методы L1-регуляризации, например, не только уменьшают переобучение, но и способствуют автоматическому отбору наиболее значимых переменных, обнуляя коэффициенты малозначимых. Кроме того, при работе с разреженными структурами необходимо учитывать особенности хранения данных. Применение специализированных форматов, таких как разреженные матрицы, позволяет существенно снизить объем используемой памяти и ускорить выполнение линейной алгебры и других операций. Эти подходы особенно актуальны при построении масштабируемых моделей, работающих с большими и высокоразмерными наборами данных.

Метод главных компонент (PCA) является одним из наиболее распространенных подходов к снижению размерности и сжатию информации в задачах анализа данных. Его основная цель заключается в поиске новых ортогональных признаков – главных компонент – которые максимизируют дисперсию исходных данных. Эти компоненты представляют собой линейные комбинации исходных признаков и позволяют сосредоточить основную информацию в меньшем числе измерений. Такой подход особенно полезен при наличии разреженности, поскольку позволяет отсеять признаки, не вносящие существенного вклада в структуру данных.

В контексте разреженных матриц PCA способствует выявлению скрытых зависимостей между признаками, что позволяет заменить исходное высокоразмерное пространство более компактным и информативным представлением. Это особенно актуально для задач машинного обучения, где избыточная размерность может не только замедлять обучение, но и ухудшать обобщающую способность модели. Применение PCA снижает вычислительные затраты и способствует повышению устойчивости алгоритмов к шуму.

Сокращение объема данных за счет уменьшения размерности признакового пространства играет важную роль в построении эффективных моделей машинного обучения. Высокая размерность приводит к проклятию размерности: расстояния между объектами теряют информативность, выборка становится разреженной, ухудшается обобщающая способность и возрастает риск переобучения. Сокращение числа признаков до информативного минимума повышает устойчивость модели к шуму, улучшает интерпретируемость.

Дополнительно уменьшение числа признаков ускоряет обучение: снижается вычислительная сложность, объем памяти и время настройки параметров. Это особенно важно при использовании ресурсоемких методов, таких как нейронные сети, где обучение на сжатом наборе может быть существенно быстрее. Таким образом, сокращение объема данных повышает качество модели и делает обучение более практичным и масштабируемым.

Разреженность данных, характерная для многих современных наборов, существенно влияет на эффективность аналитических моделей. При правильной обработке она становится источником структурной информации, позволяющей сжимать данные без потери информативности. Методы, такие как PCA и регуляризация, повышают скорость и устойчивость обучения. Эффективная работа с разреженными структурами – ключевой элемент построения масштабируемых и надежных интеллектуальных систем.

Список использованных источников:

1. Паттерсон Д. Глубокое обучение с точки зрения практика / Д. Паттерсон, А. Гибсон. М.: ДМК Пресс, 2018. 418 с. ISBN 978-5-97060-481-6 // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/116122 (дата обращения: 13.04.2025). URL: для авториз. пользователей.

2. Разреженный файл // Википедия. [2023]. Дата обновления: 02.12.2023. URL: https://ru.wikipedia.org/?curid=471221&oldid=134609381 (дата обращения: 13.04.2025).

3. Шалев-Шварц Ш. Идеи машинного обучения: учебное пособие / Ш. Шалев-Шварц, Ш. Бен-Давид; перевод с англ. А.А. Слинкина. М.: ДМК Пресс, 2019. 436 с. ISBN 978-5-97060-673-5 // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/131686 (дата обращения: 13.04.2025). URL: для авториз. пользователей.

Galiullin R.R., Kuldavletov A.I.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Valeev S.S.
Ufa University of Science and Technology, Ufa

DATA SPARSITY AND DIMENSIONALITY REDUCTION

Abstract. The article is devoted to the analysis of sparsity of data as an important aspect in modern machine learning tasks. The reasons for sparsity, its impact on the quality of models, and effective processing methods, including

dimensionality reduction using PCA, are considered. The dual nature of sparsity as a problem and a source of structural information is emphasized.

Keywords: sparsity of data, PCA, dimension reduction, machine learning, regularization, high-dimensional data, interpretability of models.

УДК 004.056

Ганиев М.Р., Ефимов И.О., Каримуллин Т.Ф.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Валеев С.С.
Уфимский университет науки и технологий, Уфа

СОВРЕМЕННЫЕ МЕТОДЫ СОВЕРШЕНСТВОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Современные методы повышения уровня информационной безопасности играют важную роль в обеспечении защиты данных и ресурсов на всех уровнях информационной системы. В статье рассматриваются актуальные подходы и технологии, используемые для защиты информации в условиях постоянно растущих угроз и уязвимостей.

Ключевые слова: управление доступом, системы обнаружения и предотвращения вторжений, облачные вычисления, искусственный интеллект и машинное обучение.

Информационная безопасность (ИБ) одна важнейшей составляющей функционирования организаций, различных государственных структур и отдельных пользователей. Сложность современных информационных систем с требует применения новых методов и технологий для защиты от разнообразных угроз. Эти угрозы могут исходить как от внешних злоумышленников, так и от внутренних нарушителей безопасности [1]. Рассмотрим далее комплексный обзор современных подходов, используемых в ИБ. Как известно, основные задачи ИБ – это обеспечение защиты данных и ресурсов от различных угроз, включая внешние и внутренние, которые базируются на базовых элементах: конфиденциальности, т.е. защите информации от несанкционированного доступа; обеспечение целостности, т.е. обеспечение неизменности и сохранности даны; обеспечение доступности, т.е. обеспечение доступа к информации и ресурсам.

Рассмотрим далее основные методы ИБ.

Криптография. Используется для защиты данных с помощью шифрования данных, цифровых подписей и хеширования.

Управление доступом. Контролирует доступ к информации на основе принятых в организации политик безопасности, включая мандатное, дискреционное и ролевое управление.

Системы обнаружения и предотвращения вторжений. Мониторинг и блокировка угроз в режиме реального времени.

Безопасность в облачных вычислениях. Защита данных в облаке с помощью шифрования и методов многофакторной аутентификации.

Искусственный интеллект и машинное обучение. Используются для обнаружения аномалий, прогнозирования атак и автоматического реагирования на различные угрозы.

Системы обнаружения и предотвращения вторжений являются важнейшими инструментами для мониторинга и защиты информационных систем от внешних и внутренних угроз и включают следующие подсистемы:

– система обнаружения вторжений анализирует сетевой трафик и действия пользователей, чтобы выявить подозрительную активность;

– система предотвращения вторжений не только обнаруживают угрозы, но и может предпринимать активные действия для их блокировки, например блокировать атакующие IP-адреса или прерывать подозрительные соединения.

Эти системы являются важными элементами комплексной системы защиты и используются в режиме реального времени для предотвращения кибератак.

С переходом многих компаний и организаций на использование облачных сервисов возникает необходимость защиты данных в облаке. Современные методы обеспечения безопасности в облачных вычислениях включают:

– шифрование данных: защита данных как при хранении в облаке, так и при их передаче;

– многофакторная аутентификация: для повышения уровня защиты от несанкционированного доступа;

– контроль доступа и управление пользователями: использование ролевого и многоуровневого контроля для минимизации рисков.

Современные методы защиты информации активно используют технологии искусственного интеллекта (ИИ) и машинного обучения (МО) [2]. Эти технологии помогают:

– обнаружение аномалий: анализируя большие объемы данных, системы могут выявить необычное поведение, которое может указывать на угрозу;

– прогнозирование атак: используя алгоритмы МО, системы могут предсказывать возможные атаки на основе предыдущих инцидентов;

– автоматическое реагирование на угрозы: ИИ может автоматически принимать меры для предотвращения атак, например блокировать подозрительные IP-адреса или отключать вредоносный трафик.

Рассмотрим далее пути совершенствования методов ИБ. Современные методы обеспечения ИБ требуют комплексного подхода, включающего обновление и адаптацию стратегий защиты [3]. Важна интеграция

различных методов, таких как многофакторная аутентификация, блокчейн-технологии, машинное обучение и искусственный интеллект для обнаружения аномалий и предотвращения атак. Кроме того, важным элементом обеспечения ИБ является обучение и повышение осведомленности пользователей о потенциальных угрозах, что помогает снизить риски, связанные с человеческим фактором. В условиях растущей зависимости от облачных вычислений и мобильных устройств особое внимание следует уделять защите данных в распределенных системах и обеспечению конфиденциальности пользователей [4].

Таким образом, успешная реализация стратегии информационной безопасности требует взаимодействия технологий, процессов и людей, а также постоянного мониторинга и улучшения защиты на всех уровнях.

Список использованных источников:

1. Валеев С.С., Кондратьева Н.В., Гузаиров М.Б., Мельников А.В. Этапы реинжиниринга информационной системы предприятия в рамках технологии нулевого доверия // vestnik-rosnou.ru – 2023. URL: https://vestnik-rosnou.ru/sites/default/files/136_Сложные %20системы %20№ %203 %20ПРОСМОТРОВЫЙ.pdf (дата обращения: 30.04.2025).

2. Исмагилова А.С. Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей / А.С. Исмагилова, Н.Д. Лушников // Инженерный вестник Дона. 2024. № 1(109). С. 178–188.

3. Валеев С.С., Кондратьева Н.В. Особенности проектирования систем безопасности на базе архитектуры нулевого доверия // ivdon.ru – 2023. URL: http://www.ivdon.ru/uploads/article/pdf/IVD_68__8_valeev_kondratyeva_v2.pdf_72458b243f.pdf (дата обращения: 30.04.2025).

4. Валеев С.С., Кондратьева Н.В., Мельников А.В. Архитектура предприятия и архитектура нулевого доверия. // info-secur.ru – 2023. URL: https://www.info-secur.ru/index.php/ojs/article/download/413/371/ (дата обращения: 30.04.2025).

Ganiev M.R., Karimullin T.F., Efimov I.O.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Valeev S.S.
Ufa University of Science and Technology, Ufa

MODERN METHODS OF IMPROVING INFORMATION SECURITY

Abstract. Modern methods of increasing the level of information security play an important role in ensuring the protection of data and resources at all

levels of the information system. The article discusses current approaches and technologies used to protect information in the face of ever-growing threats and vulnerabilities.

Keywords: access control, intrusion detection and prevention systems, cloud computing, artificial intelligence and machine learning.

УДК 004

Драгунский Н.С., Хусамов Р.Р., Ганиев Ш.И., Шилин С.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Валеев С.С.
Уфимский университет науки и технологий, Уфа

АНАЛИЗ ЭМОЦИОНАЛЬНОЙ ОКРАСКИ ТЕКСТА С ИСПОЛЬЗОВАНИЕМ МОДЕЛИ DISTILBERT

Аннотация. В статье рассматривается задача анализа эмоциональной окраски текста с использованием модели DistilBERT, являющейся облегченным вариантом BERT. Приведены основные этапы подготовки данных, методология обучения модели, а также результаты экспериментов на различных корпусах. Обоснована применимость модели в прикладных задачах анализа пользовательского контента.

Ключевые слова: анализ тональности, DistilBERT, BERT, трансформеры.

Большие языковые модели – это системы машинного обучения. Они построены на глубоких нейронных сетях и содержат огромное количество параметров, позволяющих эффективно решать разнообразные задачи обработки естественного языка (NLP). Кратко рассмотрим основные характеристики и особенности больших языковых моделей.

Архитектура. Большинство современных крупных языковых моделей основаны на архитектуре трансформеров. Трансформеры используют механизм внимания, позволяющий моделировать зависимости между словами независимо от расстояния между ними в тексте. Это значительно улучшает качество понимания контекста и семантики текста. Основные компоненты архитектуры трансформера:

Encoder – преобразует входной текст в векторное представление, учитывая контекст каждого слова; Decoder – генерирует выходной текст на основе полученных представлений; Attention Mechanism – вычисляет связи между элементами последовательности, позволяя лучше учитывать контекст.

Современные большие языковые модели применяются во множестве различных областей:

– обработка естественного языка: создание диалоговых агентов, чат-ботов, виртуальных помощников;

– автоматическое написание текстов: генерация статей, писем, отчетов, сценариев и другого контента;

– перевод текстов: высококачественный машинный перевод на разные языки;

– анализ настроений и эмоций: выявление положительных/отрицательных отзывов пользователей;

– создание вопросов и ответов: автоматическая генерация FAQ разделов, поддержка клиентов;

– генерация изображений по текстовому описанию: использование совместно с моделями компьютерного зрения позволяет создать мультимедийные продукты.

Вот некоторые известные крупные языковые модели:

– GPT (Generative Pre-trained Transformer) – серия моделей от OpenAI, начиная с GPT-1 и заканчивая актуальной версией GPT-4;

– BERT (Bidirectional Encoder Representations from Transformers) – модель широко используемая для классификации текстов и распознавания сущностей;

– RoBERTa, DistilBERT, XLNet – различные вариации BERT с улучшенными характеристиками;

– YandexGigaChat – российская большая языковая модель от Яндекса, доступная пользователям;

– GigaChat – российская большая языковая модель от Sbera, доступная пользователям.

Эти модели отличаются объемом параметров, количеством слоев и уровнем подготовки, что делает их пригодными для решения конкретных задач.

Преимущества: высокая точность и эффективность в обработке сложных запросов, способность понимать и генерировать осмысленный контент, возможность интеграции в разнообразные приложения и сервисы, универсальность применения в разных областях NLP.

Недостатки: высокие требования к вычислительным ресурсам для тренировки и эксплуатации, возможности возникновения ошибок при недостаточной точности тренировочных данных, риск генерации недостоверной или предвзятой информации, необходимость постоянного обновления и адаптации к новым данным.

Актуальность задачи анализа эмоциональной окраски текстов возрастает с развитием цифровых коммуникаций. Анализ эмоционального состояния позволяет решать широкий спектр задач – от мониторинга социальных настроений до улучшения качества обслуживания клиентов.

Классические методы, такие как словарный анализ, уступают по точности и гибкости современным нейросетевым моделям, основанным на архитектуре трансформеров [1].

Одной из наиболее перспективных моделей является DistilBERT – упрощенная версия BERT, обладающая меньшими требованиями к ресурсам при сохранении высокой точности. DistilBERT обучается на корпусе BERT посредством метода знаний-дистилляции, позволяющего сохранить ключевые языковые закономерности [2–6].

Для проведения исследований была выбрана модель distilbert-base-uncased, предварительно дообученная на задаче классификации эмоциональной окраски текста. В качестве корпуса использовалась размеченная выборка твитов с платформы Kaggle, содержащая тексты, относящиеся к категориям «позитивный», «негативный» и «нейтральный».

Предварительная обработка данных включала: очистку текста от эмодзи, ссылок и HTML-тегов; лемматизацию с использованием библиотеки spaCy; токенизацию средствами HuggingFace Tokenizer.

Далее проводилось дообучение модели на размеченном датасете. Использовался кросс-энтропийный лосс и оптимизатор AdamW. Процесс обучения длился 3 эпохи с батч-сайзом 32. Контроль переобучения осуществлялся через сохранение наилучшей модели по метрике accuracy на валидационной выборке.

Отдельного внимания заслуживает визуализация внимания (attention scores), которая показала, что модель эффективно выделяет маркеры эмоционального окраса – такие как «прекрасный», «ужасно», «ненавижу», и др.

Применение данной модели может быть эффективно в: службах поддержки (автоматическая оценка эмоционального состояния клиента); социальных сетях (мониторинг настроений); образовании (оценка эмоционального восприятия учебных материалов); HR-аналитике (анализ отзывов сотрудников).

Таким образом, модель DistilBERT демонстрирует высокую эффективность при решении задачи анализа эмоциональной окраски текстов и может быть внедрена в прикладные информационные системы без значительных вычислительных затрат.

Таким образом, модель DistilBERT демонстрирует высокую эффективность при решении задачи анализа эмоциональной окраски текстов и может быть внедрена в прикладные информационные системы без значительных вычислительных затрат.

Список использованных источников:

1. Свидетельство о государственной регистрации программы для ЭВМ № 2023617147 Российская Федерация. Программное обеспечение для выявления противоправного контента: № 2023616049: заявл. 28.03.2023: опубл. 05.04.2023 / Р.Ф. Исмагилов, Н.Д. Лушников, А.С. Исмагилова;

заявитель федеральное государственное бюджетное образовательное учреждение высшего образования «Уфимский университет науки и технологий».

2. Vaswani A., et al. Attention is All You Need. Advances in Neural Information Processing Systems. 2017.

3. Sanh V., et al. DistilBERT, a distilled version of BERT: smaller, faster, cheaper and lighter. arXiv preprint arXiv:1910.01108. 2019.

4. Devlin J., et al. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. arXiv:1810.04805. 2018.

5. Wolf T., et al. Transformers: State-of-the-Art Natural Language Processing. EMNLP. 2020.

6. Liu Y., et al. RoBERTa: A Robustly Optimized BERT Pretraining Approach. arXiv:1907.11692. 2019.

Dragunskiy N.S., Khusamov R.R., Ganiev S.I., Shilin S.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Valeev S.S.
Ufa University of Science and Technology, Ufa

TEXT SENTIMENT ANALYSIS USING THE DISTILBERT MODEL

Abstract. The article explores the task of text sentiment analysis using the DistilBERT model, a lightweight version of BERT. The paper outlines data preprocessing, model training methodology, and experiment results on various corpora. The applicability of the model to real-world user-generated content analysis is demonstrated.

Keywords: sentiment analysis, DistilBERT, emotionality, transformers.

УДК 004.056

Иванов И.П., Хасанов Р.Р., Ишмаков Т.М.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Статья посвящена современным технологиям информационной безопасности (ИБ), которые помогают защищать данные

и системы от киберугроз. Рассматриваются системы обнаружения и предотвращения вторжений, анализ больших данных, машинное обучение, блокчейн и квантовая криптография. Особое внимание уделяется их роли в противодействии актуальным угрозам, а также примерам из практики, иллюстрирующим их эффективность и ограничения.

Ключевые слова: информационная безопасность, кибербезопасность, системы обнаружения вторжений, анализ больших данных, машинное обучение, блокчейн, квантовая криптография.

Информационная безопасность (ИБ) – это комплекс мер и технологий, направленных на защиту данных, систем и сетей от несанкционированного доступа, утечек и атак. В условиях цифровизации, когда объемы данных стремительно растут, а киберугрозы становятся все более изощренными, традиционные методы защиты, такие как пароли или антивирусы, теряют свою эффективность. Современные технологии, включая машинное обучение, анализ больших данных, блокчейн и квантовую криптографию, открывают новые горизонты для обеспечения ИБ. Эта статья раскрывает суть этих технологий, их преимущества и вызовы, а также демонстрирует, как они применяются для защиты информации.

Системы обнаружения и предотвращения вторжений (IDS/IPS) – это ключевые инструменты для защиты сетей. Они отслеживают сетевой трафик и выявляют подозрительную активность. Традиционные системы опираются на сигнатурный анализ, сравнивая данные с известными шаблонами атак. Однако такие методы не справляются с новыми или сложными угрозами, такими как целевые атаки (APT).

Современные системы, или NGIPS (Next-Generation IPS), используют более продвинутые подходы. Они анализируют поведение пользователей и устройств, выявляя аномалии с помощью машинного обучения. Например, российская компания Positive Technologies разработала PT Network Attack Discovery (PT NAD). Эта система анализирует сетевой трафик в реальном времени, обнаруживает скрытые угрозы и автоматически блокирует подозрительные действия, минимизируя ущерб. Такие решения особенно важны, учитывая, что большинство атак начинается с кражи учетных данных.

IDS/IPS нового поколения демонстрируют, как ИБ переходит от реактивной защиты к проактивной, способной предугадывать и предотвращать угрозы до их реализации.

Большие данные – это огромные объемы информации, генерируемые сетями, устройствами и пользователями. В контексте ИБ они становятся ценным ресурсом для выявления угроз. Технологии анализа больших данных позволяют обрабатывать логи, трафик и другие данные в реальном времени, находя скрытые закономерности и аномалии.

Примером является платформа InfoWatch Traffic Monitor от российской компании InfoWatch. Она собирает данные с серверов, рабочих станций и

сетевых устройств, анализируя поведение пользователей и приложений. Это помогает выявить подозрительные действия, такие как несанкционированный доступ, и предсказать возможные атаки. Гибкость платформы позволяет настраивать алгоритмы под конкретные угрозы, что делает ее эффективной против новых видов атак.

Машинное обучение – это технология, которая позволяет системам обучаться на данных и улучшать свои способности без явного программирования. В ИБ машинное обучение используется для выявления аномалий, предсказания атак и автоматизации реагирования.

Российская компания Group-IB создала систему Threat Intelligence & Attribution, которая применяет машинное обучение и глубокое обучение для анализа киберугроз. Система распознает паттерны, характерные для атак, включая угрозы нулевого дня, которые неизвестны традиционным антивирусам. Она адаптируется к новым видам атак, обеспечивая защиту в реальном времени. Например, система может автоматически изолировать зараженное устройство, предотвращая распространение угрозы.

Машинное обучение делает ИБ более интеллектуальной, позволяя системам не только реагировать на известные угрозы, но и предвидеть новые, что особенно важно в условиях стремительно эволюционирующих кибератак.

Блокчейн – это технология, основанная на децентрализованной базе данных, где информация хранится в виде цепочки блоков, защищенных криптографией. В ИБ блокчейн применяется для обеспечения целостности данных, управления идентификацией и защиты транзакций.

Российская платформа Waves Enterprise использует блокчейн для защиты данных от изменений и утечек. Каждый блок содержит информацию о предыдущем, а криптографические подписи гарантируют неизменность записей. Это делает технологию идеальной для управления цепочками поставок, финансовых транзакций или персональных данных. Например, блокчейн может создать систему, где пользователи сами контролируют доступ к своим данным, снижая риск компрометации.

Блокчейн повышает доверие к системам, устраняя необходимость в посредниках и обеспечивая прозрачность, что делает его перспективным инструментом ИБ.

Квантовая криптография использует законы квантовой физики для создания сверхнадежных систем шифрования. Основной метод – квантовое распределение ключей (QKD), которое позволяет двум сторонам безопасно обмениваться ключами. Любая попытка перехвата ключа нарушает квантовое состояние, что мгновенно обнаруживается.

В России компания QRate разрабатывают компактные QKD-системы, которые можно интегрировать с традиционными методами шифрования. Такие решения устойчивы даже к атакам с использованием квантовых компьютеров, которые могут взломать классические алгоритмы. Исследователи также работают над увеличением дальности передачи

данных и снижением помех, чтобы сделать технологию доступной для массового использования.

Квантовая криптография представляет собой будущее ИБ, обещающее беспрецедентный уровень защиты данных в эпоху квантовых технологий.

Несмотря на прогресс, технологии ИБ сталкиваются с рядом трудностей:

- нехватка специалистов: квалифицированных экспертов по кибербезопасности недостаточно для удовлетворения спроса;
- сложность интеграции: новые технологии требуют адаптации к существующим системам, что может быть дорого и трудоемко;
- эволюция угроз: киберпреступники постоянно разрабатывают новые методы атак, требующие регулярного обновления защитных систем;
- высокая стоимость: внедрение передовых решений, таких как QKD, требует значительных инвестиций.

Эти вызовы подчеркивают необходимость комплексного подхода, сочетающего технологии, обучение персонала и организационные меры.

Информационная безопасность – это не просто набор технологий, а динамично развивающаяся область, требующая постоянной адаптации к новым вызовам. Системы IDS/IPS, анализ больших данных, машинное обучение, блокчейн и квантовая криптография формируют современный арсенал защиты данных и систем. Они позволяют не только реагировать на угрозы, но и предвидеть их, минимизируя риски. Однако ни одна технология не может обеспечить абсолютную безопасность в одиночку. Эффективная защита требует сочетания инноваций, квалифицированных специалистов и осведомленности пользователей. В эпоху цифровизации ИБ становится основой устойчивого развития организаций и общества в целом.

Список использованных источников:

1. Positive Technologies. PT Network Attack Discovery. URL: https://www.ptsecurity.com/ru-ru/products/network-attack-discovery/ (дата обращения 10.04.2025).

2. InfoWatch. InfoWatch Traffic Monitor. URL: https://www.infowatch.ru/products/dlp-sistema-traffic-monitor (дата обращения 10.04.2025).

3. Group-IB. Threat Intelligence & Attribution. URL: https://www.group-ib.com/products/threat-intelligence/ (дата обращения 10.04.2025).

4. Waves Enterprise. URL: https://doc.web3tech.ru/ru/latest/index.html (дата обращения 10.04.2025).

5. QRate. Аппаратно-программный комплекс квантового распределения ключей (КРК). URL: https://goqrate.com/projects/qrate_qkd312/S (дата обращения 10.04.2025).

Ivanov I. P., Khasanov R. R., Ishmakov T. M.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

INFORMATION SECURITY TECHNOLOGIES

Abstract. The article is devoted to modern information security (IS) technologies that help protect data and systems from cyber threats. Intrusion detection and prevention systems, big data analysis, machine learning, blockchain and quantum cryptography are considered. Special attention is paid to their role in countering current threats, as well as practical examples illustrating their effectiveness and limitations.

Keywords: information security, cybersecurity, intrusion detection systems, big data analysis, machine learning, blockchain, quantum cryptography.

УДК 681.31

Ишбаева А.Э., Мансурова А.Р., Сысоева А.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЭПОХУ БОЛЬШИХ ДАННЫХ

Аннотация. Статья рассматривает проблемы защиты персональных данных в эпоху больших данных. Анализируется совместимость технологий больших данных с российским законодательством о персональных данных, а также обсуждаются риски для конфиденциальности и предлагаются технологические решения для их минимизации.

Ключевые слова: большие данные, персональные данные, защита, законодательство, конфиденциальность.

В современном мире, характеризующемся линейным ростом объемов данных, концепция больших данных (Big Data) стала неотъемлемой частью многих отраслей. Анализ больших данных позволяет организациям извлекать ценные знания, оптимизировать процессы и принимать обоснованные решения. Однако, вместе с преимуществами, использование больших данных сопряжено с серьезными проблемами в области защиты

персональных данных. В данной статье мы рассмотрим ключевые проблемы, возникающие при обработке больших данных в контексте защиты персональных данных, а также предложим возможные пути их решения.

Идентификация и реидентификация. Идентификация и реидентификация представляют собой две взаимосвязанные угрозы, способные нарушить конфиденциальность пользователей даже после применения мер по обезличиванию данных.

Идентификация – это процесс определения конкретной личности на основании прямого или косвенного набора данных. Хотя при обработке данных часто используются методы удаления явных идентификаторов (таких как имена, адреса, номера телефонов), оставшиеся данные все равно могут содержать уникальные комбинации признаков, достаточные для точной идентификации субъекта.

Реидентификация – это процесс восстановления исходных данных или привязки обезличенных данных обратно к конкретной личности. Благодаря развитию технологий анализа данных, в частности методов машинного обучения, становится возможным восстановить персональные данные путем объединения нескольких наборов данных, содержащих различные фрагменты информации о субъекте.

Методы анализа больших данных, такие как машинное обучение, позволяют выявлять закономерности и связи, которые могут привести к раскрытию личности, даже если прямые идентификаторы были удалены. Реидентификация становится особенно опасной при объединении различных наборов данных, когда комбинация атрибутов позволяет однозначно идентифицировать человека [2].

Вывод информации. Анализ больших данных может позволить сделать выводы о личной информации, которая не была предоставлена непосредственно. Например, на основе анализа покупательского поведения можно сделать выводы о состоянии здоровья, политических взглядах или религиозных убеждениях человека. Такие выводы могут быть неточными, предвзятыми или дискриминационными, что нарушает права на неприкосновенность частной жизни [4].

Сбор и обработка избыточных данных. Организации зачастую стремятся собрать максимальное количество данных, полагая, что это улучшит точность прогнозирования и качество аналитики. Однако избыток данных существенно повышает вероятность нарушений конфиденциальности.

Причины заключаются в следующем:

– чем больше данных собирается, тем сложнее обеспечить их надлежащую защиту и соответствие принципам минимально необходимого сбора данных (data minimization);

– избыточная информация увеличивает поверхность атаки для злоумышленников, которые могут использовать дополнительные точки

входа для компрометации системы и извлечения конфиденциальных сведений;

– обработка ненужных данных снижает эффективность операций и может привести к непредвиденным последствиям, таким как ошибки классификации или злоупотребления данными.

Кроме того, хранение большого объема необработанных данных затрудняет соблюдение принципов уничтожения данных после истечения срока их полезности, что ведет к дополнительным рискам длительного хранения потенциально уязвимых данных [5].

Далее рассмотрим юридические и этические аспекты.

Обработка больших данных должна соответствовать действующему законодательству о защите персональных данных. В России основным нормативным актом, регулирующим обработку персональных данных, является Федеральный закон № 152-ФЗ «О персональных данных». Этот закон устанавливает требования к сбору, хранению, использованию и передаче персональных данных, а также предусматривает меры защиты прав субъектов данных.

Кроме того, важно учитывать следующие российские законодательные акты:

– Конституция Российской Федерации – гарантирует право каждого гражданина на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (статья 23);

– Гражданский кодекс Российской Федерации – регулирует отношения, возникающие в связи с обработкой персональных данных, включая защиту личных неимущественных прав граждан (например, статья 150 ГК РФ о защите чести, достоинства и деловой репутации);

– Трудовой кодекс Российской Федерации – содержит нормы, касающиеся обработки персональных данных работников, включая гарантии конфиденциальности и защиту от неправомерного использования этой информации (глава 14 ТК РФ).

Также стоит отметить, что обработка больших данных может затрагивать вопросы безопасности информации, регулируемые Федеральным законом №149-ФЗ «Об информации, информационных технологиях и о защите информации», который устанавливает общие правила оборота информации и защиты конфиденциальной информации.

Применение существующих правовых рамок к большим данным может быть сложным, поскольку многие положения были разработаны для традиционных методов обработки данных. Важно адаптировать существующие правовые рамки к специфике больших данных, чтобы эффективно защищать права субъектов данных в условиях современных технологий [1–3].

Помимо юридических требований, необходимо учитывать этические аспекты использования больших данных. Анализ больших данных может приводить к дискриминации, предвзятости и несправедливому отношению

к определенным группам населения. Необходимо разрабатывать этические кодексы и стандарты, которые регулируют использование больших данных и обеспечивают соблюдение принципов справедливости, равенства и уважения прав человека [7].

Рассмотрим далее решения для защиты персональных данных.

Методы анонимизации и псевдонимизации**.** Для снижения риска идентификации необходимо использовать эффективные методы анонимизации и псевдонимизации данных. Однако, необходимо учитывать, что многие традиционные методы анонимизации могут быть недостаточно эффективными для защиты от современных методов анализа больших данных [5].

Контроль доступа и шифрование. Для обеспечения безопасности данных необходимо внедрять комплексные меры контроля доступа и шифрования. Это включает в себя использование многоуровневой аутентификации (например, двухфакторной), управление правами доступа на основе ролей и задач сотрудников, а также внедрение политик минимизации привилегий [6].

Технологии повышения конфиденциальности (PETs)**.** Технологии повышения конфиденциальности (Privacy Enhancing Technologies, PETs) позволяют обрабатывать данные, не раскрывая их содержание. К таким технологиям относятся дифференциальная конфиденциальность, гомоморфное шифрование и безопасные многосторонние вычисления [7].

Использование больших данных предоставляет огромные возможности для развития науки, экономики и общества. Однако, необходимо осознавать и эффективно управлять рисками для защиты персональных данных. Для этого необходимо совершенствовать законодательство, разрабатывать этические стандарты и применять современные технологические решения. Только при таком подходе можно обеспечить баланс между использованием больших данных и защитой прав на неприкосновенность частной жизни.

Список использованных источников:

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2. Амбарцумов Р.А. Правовое регулирование технологии «Big Data» в Российской Федерации // Вопросы Российской Юстиции. 2019. № 4.

3. Петренко В.И. и др. Защита персональных данных в информационных системах: практикум; учебное пособие для вузов.

4. Большие данные в социальных и гуманитарных науках (в частности, разделы о правовых и этических аспектах больших данных): сборник статей.

5. Угрозы конфиденциальности в цифровую эпоху / И.Н. Петров. М.: Издательство «Информационная безопасность», 2022.

6. Большие данные и безопасность: вызовы и решения / С.А. Смирнов. СПб.: Научное издательство, 2023.

7. Защита персональных данных: регуляторные требования и практические аспекты / О.В. Кузьмина. Екатеринбург: Издательство «Право и данные», 2021.

Ishbaeva A.E., Mansurova A.R., Sysoeva A.V.
Ufa University of Science and Technology, Ufa

Science supervisor:
Shagapov I.A.,
Ufa University of Science and Technology, Ufa

PROBLEMS OF PERSONAL DATA PROTECTION IN THE ERA OF BIG DATA

Abstract. This article examines the issues of personal data protection in the era of big data. It analyzes the compatibility of big data technologies with Russian legislation on personal data, discusses the risks to privacy, and proposes technological solutions to minimize these risks.

Keywords: big data, personal data, protection, legislation, privacy.

УДК 004

Ишмухаметов И.Р., Чернышев К.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Юнусова Д.С.
Уфимский университет науки и технологий, Уфа

ОБНАРУЖЕНИЕ ТРОЯНСКИХ ПРОГРАММ

Аннотация. Статья посвящена исследованию применения различных моделей машинного обучения для выявления троянских программ. Выполнен сравнительный анализ эффективности моделей Decision Tree, Random Forest, K Nearest Neighbors и Stacked Classifier с использованием метрик Accuracy, Precision, Recall, F1 Score и AUC-ROC. Основной задачей работы является определение наиболее точного и надежного метода для своевременного обнаружения и противодействия троянским программам.

Ключевые слова: троянская программа, машинное обучение, классификация, Decision Tree, Random Forest, K Nearest Neighbors, Stacked Classifier, Accuracy, Precision, Recall, F1 Score, AUC-ROC.

Троянские программы представляют собой вредоносное программное обеспечение, которое маскируется под легитимные приложения, предоставляя злоумышленникам доступ к персональным данным и ресурсам пользователя. Выявление таких программ важно, так как они представляют собой серьезную угрозу. Могут похищать конфиденциальные данные, такие как пароли и банковские реквизиты, используя для этого различные методы, включая перехват ввода с клавиатуры. Кроме того, они могут вызывать финансовые потери, проводя несанкционированные транзакции или создавая поддельные счета. Не менее опасно то, что некоторые троянские программы имеют способность повреждать систему, удаляя или изменяя файлы и тем самым делая компьютер непригодным для использования. Традиционные методы, основанные на поиске известных сигнатур вирусов, становятся менее эффективными, поскольку современные угрозы постоянно эволюционируют. Именно поэтому актуальным решением стало применение машинного обучения, способного выявлять скрытые паттерны поведения зараженных устройств.

Статья посвящена разработке эффективных методов идентификации троянских программ с использованием методов машинного обучения. Мы рассматривали набор данных, состоящий из 177 482 наблюдений, среди которых 90 683 соответствовали случаям заражения («Trojan») и 86 799 – чистым («Benign»). Данные представляли собой подробное описание технических аспектов сетевого взаимодействия устройств, таких как временные промежутки, объемы передаваемых данных, частоты передачи пакетов и другие статистические параметры.

Методика анализа состояла из нескольких последовательных шагов. Во-первых, произошла очистка данных от пропусков и формирование нового набора признаков, позволяющего точнее определить отличия между поведением зараженного и незараженного устройства. Затем осуществлялось преобразование категорических признаков в числовой формат, балансировка классов с помощью метода SMOTE и стандартизация данных для устранения влияния размаха величин.

Далее выполнялось сравнение нескольких популярных моделей машинного обучения: дерева решений, случайного леса, k ближайших соседей и ансамблевого классификатора. Чтобы выбрать лучшую модель, каждая из них прошла процедуру оптимизации гиперпараметров с целью максимизировать точность классификации.

В табл. 1 представлены итоговые результаты сравнения моделей, оцениваемые по основным показателям качества: точности, полноте, F1-мере и площади под кривой ROC (AUC-ROC).

Таблица 1

Показатели эффективности моделей машинного обучения
при определении троянских программ

Model	Accuracy	Precision	Recall	F1 Score	AUC-ROC
Decision Tree	0,95	0,95	0,95	0,95	0,95
Random Forest	0,95	0,95	0,95	0,95	0,95
K Nearest Neighbors	0,91	0,91	0,89	0,90	0,91
Stacked Classifier	0,95	0,95	0,95	0,95	0,95

Полученные данные показывают значительное преимущество Decision Tree и Random Forest, которые достигли примерно одинаковых высоких уровней точности порядка 95 %, что свидетельствует о стабильной и точной работе этих моделей.

Модель K Nearest Neighbors, несмотря на чуть меньшую общую производительность, остается достаточно конкурентоспособной. Ансамблевый классификатор также подтвердил свою надежность, показав аналогичные результаты с деревьями решений и случайным лесом.

Результаты подчеркивают перспективность применения машинного обучения для детектирования троянских программ на основе анализа сетевого трафика. Новый подход позволил создать высокоэффективные инструменты, способные успешно выявлять угрозы в режиме реального времени, открывая возможности для совершенствования современных защитных механизмов и средств кибербезопасности.

Список использованных источников:

1. Кобяков Н.С. Оценка опасности вредоносных программ классов «Троянские программы» / Н.С. Кобяков // Альманах Пермского военного института войск национальной гвардии. 2023. № 2 (10). С. 31–38.

2. Фадеева М.А. Применение метрик качества моделей бинарной классификации для анализа модели данных / М.А. Фадеева // Инженерные кадры – будущее инновационной экономики России. 2023. № 1. С. 1104–1107.

Ishmukhametov I.R., Chernyshev K.V.
Ufa University of Science and Technology, Ufa, Russia

Scientific supervisor:
Yunusova D.S.
Ufa University of Science and Technology, Ufa, Russia

TROJAN PROGRAM DETECTION

Abstract. The article is devoted to the study of the application of various machine learning models to identify Trojans. A comparative analysis of the effectiveness of the Decision Tree, Random Forest, K Nearest Neighbors, and Stacked Classifier models was performed using Accuracy, Precision, Recall, F1 Score, and AUC-ROC metrics. The main objective of the work is to determine the most accurate and reliable method for timely detection and countering Trojan programs.

Keywords: trojan program, classification, Decision Tree, Random Forest, K Nearest Neighbors, Stacked Classifier, Accuracy, Precision, Recall, F1 Score, AUC-ROC.

УДК 004

Ляпустин Е.М., Ахметзянов Д.И., Баязитов Т.Т.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ И СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. Цифровизация и киберугрозы требуют эффективного управления информационной безопасностью (ИБ). Моделирование процессов ИБ – мощный инструмент анализа, проектирования и оценки защитных механизмов. В статье рассматриваются подходы к моделированию (формальные, имитационные, графические), области применения (анализ рисков, проектирование архитектуры безопасности), вызовы (сложность, нехватка данных) и перспективы (ИИ, гибридные модели, цифровые двойники).

Ключевые слова: информационная безопасность, моделирование, моделирование процессов, анализ рисков, формальные методы, имитационное моделирование.

Современный мир характеризуется беспрецедентным ростом информации и повсеместным внедрением ИТ, что неизбежно усложняет инфраструктуры и умножает количество и изощренность киберугроз. Сложность систем и многообразие задач информационной безопасности (ИБ) делают интуитивные подходы неэффективными, порождая острую потребность в инструментах формализации, анализа и прогнозирования. Ключевым таким инструментом является моделирование – создание абстрактных представлений реальных или гипотетических систем, атак и защит для их изучения. Модели упрощают сложность, выявляют скрытые связи, позволяют проводить анализ «что-если», сравнивать альтернативы и оптимизировать ресурсы, улучшая общее понимание ИБ.

Информационная безопасность определяется как состояние защищенности информации и инфраструктуры от угроз, обеспечивая конфиденциальность, целостность и доступность (CIA). Она поддерживается через взаимосвязанные процессы (управление рисками, инцидентами, уязвимостями) и системы ИБ, включающие организационные меры и программно-технические средства (МЭ, IDS/IPS, политики). Модель ИБ – это абстракция объекта ИБ, отражающая его существенные черты для конкретной цели. Исследования моделирования в ИБ эволюционировали от анализа рисков и политик к более сложным подходам, включая формальные методы, нотации бизнес-процессов (BPMN) и модели атак (деревья/графы атак). Однако проблемы стандартизации и интеграции моделей сохраняются.

Формальные методы, такие как Сети Петри, конечные автоматы и процессные алгебры, применяются для точного математического описания и строгого анализа политик безопасности, протоколов и моделей доступа. Они позволяют верифицировать корректность и выявлять логические уязвимости на этапе проектирования, анализируя потоки работ, жизненные циклы объектов и взаимодействие параллельных процессов.

Имитационное моделирование воспроизводит поведение систем во времени, учитывая случайность и динамику. Дискретно-событийное моделирование (DES) анализирует производительность систем ИБ. Агентное моделирование (ABM) изучает сложные эмерджентные явления, такие как распространение вредоносного ПО или поведение пользователей, через взаимодействие автономных агентов. Системная динамика (SD) исследует долгосрочные эффекты политик ИБ и инвестиций через потоковые диаграммы и петли обратной связи.

Графические модели используют визуальные языки для наглядного представления. BPMN помогает описывать и оптимизировать процессы ИБ. UML применяется для моделирования систем и их компонентов. Деревья и графы атак визуализируют пути компрометации системы, помогая выявить критические точки. Диаграммы потоков данных (DFD) отслеживают движение информации, указывая места, требующие защиты.

Модели на основе знаний, включая онтологии ИБ и экспертные системы, фокусируются на представлении и использовании экспертных знаний. Онтологии стандартизируют терминологию и интегрируют данные, а экспертные системы автоматизируют принятие решений на основе правил «если-то», например, при классификации инцидентов.

Применение моделирования в ИБ сталкивается со значительными вызовами. Сложность, масштаб и динамичность современных систем и угроз затрудняют создание точных, актуальных моделей. Недостаток достоверных данных для калибровки и сложность безопасной валидации на реальных системах являются существенными препятствиями. Точная формализация непредсказуемого человеческого фактора (пользователей и атакующих) остается серьезным ограничением. Интеграция различных типов моделей для комплексного анализа также представляет методологическую и техническую проблему.

Преодоление этих вызовов связано с перспективными направлениями. Важнейшим является интеграция с Искусственным Интеллектом и Машинным Обучением (AI/ML) для автоматизации построения и калибровки моделей, генерации данных для обучения систем защиты и моделирования адаптивного поведения AI-агентов. Развитие гибридных подходов, комбинирующих сильные стороны разных методов, также актуально. Концепция цифровых двойников (Digital Twins) обещает создание динамических моделей ИТ-инфраструктуры для мониторинга и симуляции. Необходимо улучшенное моделирование человеческого фактора с учетом когнитивных и социальных аспектов. Стандартизация языков и форматов моделирования ИБ упростит обмен моделями и интеграцию инструментов. Наконец, требуется адаптация и разработка методов моделирования для новых технологий: Интернета вещей (IoT), облачных вычислений, киберфизических систем.

Таким образом, моделирование – незаменимый инструмент для анализа и управления ИБ в условиях растущих угроз. Несмотря на прогресс, его применение ограничено сложностью среды, нехваткой данных и проблемой учета человеческого фактора. Дальнейшие исследования, особенно в области интеграции с AI/ML, гибридных моделей, цифровых двойников и моделирования поведения человека, критически важны для преодоления этих барьеров и повышения киберустойчивости.

Список использованных источников:

1. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. Введ. 2008-02-01. М.: Стандартинформ, 2008. 16 с.

2. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введ. 2022-04-01. М.: Стандартинформ, 2021. 39 с.

3. Мельников Д.А. Моделирование систем защиты информации: учебное пособие / Д.А. Мельников; Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет). М.: Издательство МГТУ им. Н.Э. Баумана, 2018. 87 с.

4. Баранов А..П. Формальные методы верификации и синтеза протоколов безопасности / А.П. Баранов // Труды Института системного программирования РАН. 2012. Т. 23. С. 319–334.

5. Максимов Д.Ю. Моделирование процессов управления информационной безопасностью организации с использованием BPMN / Д.Ю. Максимов, А.С. Марков // Бизнес-информатика. 2015. № 4 (34). С. 48–57.

6. Моделирование и оценка последствий компьютерных атак на критически важные информационные системы / И.В. Котенко, И.Б. Саенко, О.С. Лаута [и др.] // Информатика и автоматизация. 2019. Т. 18, № 1. С. 137–166.

Lyapustin E.M., Akhmetzyanov D.I., Bayazitov T.T.
Ufa University of Science and Technology, UFA

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

MODELING OF INFORMATION SECURITY PROCESSES AND SYSTEMS

Abstract. Digitalization and cyber threats require effective management of information security (IS). Modeling of IS processes is a powerful tool for analyzing, designing and evaluating defense mechanisms. This article discusses modeling approaches (formal, simulation, graphical), applications (risk analysis, security architecture design), challenges (complexity, data scarcity) and perspectives (AI, hybrid models, digital twins).

Keywords: information security, modeling, process modeling, risk analysis, formal methods, simulation modeling.

УДК 004.89:004.056

Пуйко Д.Д.
Северо-Кавказский федеральный университет, Ставрополь

Научный руководитель:
Петренко В.И.
Северо-Кавказский федеральный университет, Ставрополь

ПРОБЛЕМЫ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ В ДЕЦЕНТРАЛИЗОВАННЫХ КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

Аннотация. Многофакторная аутентификация (MFA) имеет первостепенное значение для обеспечения безопасности киберфизических систем (CPS), особенно в сфере Интернета вещей (IoT), характеризующейся ограниченными ресурсами устройств и критически важными операциями. Обсуждаются возможные стратегии смягчения последствий, включающие легковесную криптографию, вычисления вне цепи, специализированные механизмы консенсуса и надежные протоколы децентрализованного управления. Трудность заключается в обеспечении баланса между надежной безопасностью, удобством использования и производительностью в условиях жестких ограничений этих децентрализованных сред IoT.

Ключевые слова: многофакторная аутентификация (MFA), Интернет вещей (IoT), киберфизические системы (CPS), блокчейн.

Киберфизические системы (CPS) представляют собой тесную интеграцию вычислений, сетей и физических процессов. Интернет вещей (IoT) является ярким проявлением CPS, объединяющим миллиарды устройств – от простых датчиков и исполнительных механизмов до сложных машин и носимых устройств – часто работающих в условиях значительных ограничений ресурсов (вычислительной мощности, памяти, энергии) и взаимодействующих с физическим миром, часто в таких критически важных приложениях, как промышленный контроль (IIoT) или здравоохранение (IoHT). Обеспечение безопасности таких систем имеет огромное значение, поскольку уязвимости могут привести к физическому ущербу, утечке данных или нарушению работы основных служб.

Многофакторная аутентификация (MFA) – это краеугольный камень современной системы безопасности, требующий от пользователей или организаций предоставления нескольких доказательств (факторов) из разных категорий – знания (то, что вы знаете), владения (то, что у вас есть) и принадлежности (то, что вы есть) – для подтверждения их личности. Реализация MFA в IoT крайне важна, но сложна из-за ограничений устройств и масштабов развертывания.

Как отмечается в работе [1], посвященной многофакторной аутентификации в контексте Интернета вещей, для обеспечения безопасности таких систем необходимо решить ряд следующих вопросов:

– как взвесить факторы?

– как адаптировать решения?

– как завоевать доверие пользователей?

– как безопасно получить внешние данные?

Первая проблема при проектировании моделей многофакторной аутентификации заключается в отсутствии общепринятых критериев для ранжирования аутентификационных факторов и выбора метрик их эффективности. Это приводит к необъективности приоритезации факторов и контекстной зависимости.

Вторая проблема уже частично решается системами с использованием статистических моделей, основанных на байесовских сетях [2] или нейронных сетях [3]. Однако в контексте IoT-устройств с низким энергопотреблением она сохраняет актуальность, так как эти методы требуют значительных вычислительных мощностей для обучения и инференса моделей, больших объемов памяти для хранения параметров (например, весов нейросетей), постоянной энергии для обработки данных в реальном времени.

Третья проблема касается необходимости прозрачности модели многофакторной аутентификации. Ключевой вызов – обеспечение доверия к системе через описание ее решений, особенно в сценариях, где факторы аутентификации динамически меняются.

В четвертой проблеме затрагиваются риски взаимодействия между устройствами, создающих уязвимости, связанные с отсутствием гарантий надежности и целостности внешних источников. Это требует внедрения динамических моделей оценки доверия, способных адаптироваться к меняющимся условиям работы устройств в гетерогенных средах, таких как умные города или промышленные IoT.

Также MFA сталкивается с большими проблемами в области криптографии. Криптографические алгоритмы используются для безопасной связи, согласования ключей, проверки факторов и взаимодействия с DHT / блокчейном. Хотя легковесная криптография стремится минимизировать потребление памяти и энергии, ее эффективность остается под вопросом на низкоуровневых микроконтроллерах.

Легкие примитивы: хэш-функции (например, SHA-256), операции XOR и симметричные шифры (например, AES-128, стандарт NIST ASCON, SPECK) обычно считаются выполнимыми. Моделируемые затраты показывают, что операции занимают от микросекунд до миллисекунд на мощных процессорах, но могут быть значительными на низкоуровневых MCU. В работе [4] было приведено моделируемое время:

– хэш: $T_h \approx 0{,}0026$ мс;

– AES-128 Шифрование / Дешифрование $T_{E/D} \approx 0{,}00325$ мс;

– нечеткое извлечение $T_{FE} \approx 1{,}989$ мс (актуально для биометрии).

Криптография эллиптических кривых (ECC) обеспечивает надежную защиту с меньшими ключами, чем RSA, но требует больших вычислительных затрат. В том же исследовании время умножения точек над ECC (T_{ecm}) оценивалось в 1,989 мс, что значительно выше, чем время хэширования или симметричного шифрования.

Билинейные пары, используемые в некоторых продвинутых схемах [5], еще более требовательны. Пригодность ECC для сильно ограниченных устройств остается спорной, что часто приводит к необходимости перекладывать ее на шлюзы [4].

Для защиты от квантовых компьютеров в будущем требуются алгоритмы PQC, которые часто имеют больший размер ключа/подписи и более высокие вычислительные затраты, чем текущая криптография над ECC.

В работе [6] анализируются требования к устройствам IoT, необходимые для работы алгоритмов PQC.

Главными параметрами этих устройств являются: объем доступной оперативной памяти, объем RAM/флэш-памяти/накопителя и тактовая частота.

Причем объем накопителя не так значителен, как объем RAM, поскольку даже в современных устройствах он обычно не превышает 64 кб.

Если сравнить PQC алгоритмы для создания ЭЦП, то Falcon (0,5 кб) выигрывает у Dilithium (40–70 кб), хотя у Dilithium объем кода гораздо меньше.

В качестве алгоритма инкапсуляции ключей предлагают использовать Kyber или Saber, оба имеют достаточные характеристики для работы с IoT.

Тем не менее, большинство стандартов рассматривают модели, сравнимые с ARM Cortex M4. Большое количество моделей на рынке имеют куда более низкие характеристики.

Другой задачей является обеспечение эффективности MFA. Она зависит от политики, определяющей, какие факторы требуются при тех или иных обстоятельствах (например, аутентификация на основе риска). Децентрализация затрудняет управление политиками:

– как определяются и безопасно распространяются политики MFA среди всех соответствующих субъектов (устройств, валидаторов) в киберфизических системах?

– как последовательно обновляются политики в сети, особенно с учетом проблем с соединением и необходимости консенсуса по изменениям? Задержки в завершении работы блокчейна влияют на скорость распространения политик.

Обеспечение правильного и последовательного применения политик потенциально недоверенными или ограниченными в ресурсах сущностями – сложная задача.

Решение этих взаимосвязанных задач требует целостного подхода. Для этого необходимы достижения в области легковесной и постквантовой криптографии, инновационное использование методов вычислений вне

цепочки. В конечном итоге успешное развертывание MFA в этих средах зависит от нахождения правильного баланса между обеспечением надежной многоуровневой безопасности, поддержанием приемлемой производительности и удобства использования в условиях жестких ограничений на время ожидания и соблюдением жестких ограничений на ресурсы в обширном ландшафте IoT. Для полной реализации потенциала безопасного и эффективного MFA в этих многообещающих, но сложных децентрализованных архитектурах все еще требуются значительные исследования и разработки.

Список использованных источников:

1. Ometov A., Petrov V., Bezzateev S., Andreev S., Koucheryavy Y., Gerla M. Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications // IEEE Network. 2019. Т. 33, № 2. С. 82–88.
2. Muncaster J., Turk M. Continuous multimodal authentication using dynamic Bayesian networks // Proc. 2nd Workshop Multimodal User Authentication, Toulouse, France. 2006. С. 1–8.
3. Phiri J., Zhao T.-J., Zhu C. H., and J. M. Using Artificial Intelligence Techniques to Implement a Multifactor Authentication System // International Journal of Computational Intelligence Systems. 2011. Т. 4, № 4. С. 420–430.
4. Vinoth R., Deborah L., Vijayakumar P., Kumar N. Secure Multi-factor Authenticated Key Agreement Scheme for Industrial IoT // IEEE Internet of Things Journal. 2020. Дек. Т. PP.
5. Nikravan M., Reza A. A Multi-factor User Authentication and Key Agreement Protocol Based on Bilinear Pairing for the Internet of Things // Wirel. Pers. Commun. USA, 2020. Март. Т. 111, № 1. С. 463–494. ISSN 0929-6212.
6. Atkins D. Requirements for post-quantum cryptography on embedded devices in the IoT // Third PQC Standardization Conference. 2021.

Puiko D.D.
North Caucasus Federal University, Stavropol

Scientific supervisor:
Petrenko V.I.
North Caucasus Federal University, Stavropol

PROBLEMS OF MULTIFACTOR AUTHENTICATION IN DECENTRALIZED CYBER-PHYSICAL SYSTEMS

Abstract. Multi-factor authentication (MFA) is of paramount importance for securing cyber-physical systems (CPS), especially in the Internet of Things (IoT) domain characterized by limited device resources and mission-critical operations. Possible mitigation strategies including lightweight cryptography,

off-chain computing, specialized consensus mechanisms, and robust decentralized management protocols are discussed. The challenge is to balance robust security, usability and performance under the severe constraints of these decentralized IoT environments.

Keywords: multi-factor authentication (MFA), Internet of Things (IoT), cyber physical systems (CPS), blockchain.

УДК 004.056: 519.2

Резбаев В.М.
Стерлитамакский филиал Уфимского
университета науки и технологий, Стерлитамак

Корнилова А.А.
Уфимский университет науки и технологий, Уфа

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ВРЕМЕННОГО РЯДА ПОХИЩЕННЫХ ЗАПИСЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ В МИРЕ

Аннотация. В работе приведено описание статистических данных утекшим записям персональных данных в мире в период с 2013 по 2024 года. Показано, что с наибольшим коэффициентом корреляции данные описываются экспоненциальной функции. Проведена интерпретация полученных результатов и прогноз количества утечек персональных данных на 2025–2027 гг.

Ключевые слова: математическое моделирование, прогноз, персональные данные, утечка.

В начале 2024 г. в России были приняты законы об административной и уголовной ответственности за действия, повлекшие за собой утечку персональных данных (ПДн). Например, новый законопроект предусматривается введение штрафов за допущение утечек и дополнение Уголовного кодекса Российской Федерации [1] новой статьей 272.1, которая устанавливает ответственность за сбор, использование, передачу и хранение в цифровом виде ПДн, полученных незаконным путем. Несмотря на все действия со стороны руководства станы обезопасить ПДн граждан, в 2024 г. Россия заняла 2-е место во всем мире по количеству утечек ПДн уступая лишь Соединенным Штатам Америки [2]. Для исследования дальнейшей динамики утечек записей ПДн применим математическое моделирование временного ряда [3]. Математические модели применяются во всех сферах деятельности человека для прогноза, определения факторов, влияющих на изучаемы процесс и многое другое [4–7]. В сфере информационной безопасности, юриспруденции все чаще применяются математические методы с целью прогноза преступности [5, 7].

Целью данной работы являлось описание и подбор математической модели для описания течек похищенных ПДн.

Экспертно-аналитическим центром InfoWatch в 2024 г. опубликованы данные о количестве утекших записей ПДн. В 2024 г. их количество возросло до более чем 47,24 млрд, что на 111,5 % больше, чем в 2022 г., тогда утекло 22,34 млрд записей ПДн (рис. 1) [2].

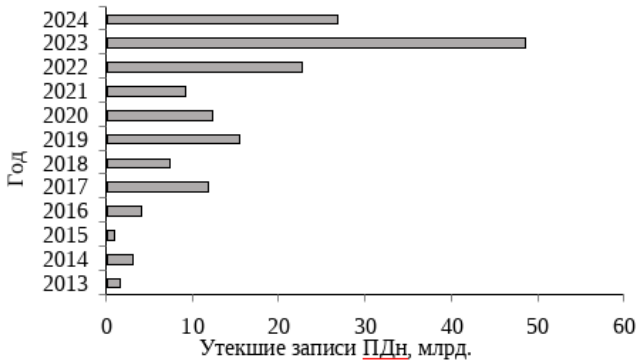

Рис. 1. Утечки записей ПДн в мире в период с 2013–2024 гг.

Наиболее распространенными (простыми) моделями описания статистических данных являются: линейная, экспоненциальная, логарифмическая, полиномиальная, степенная. Все этим модели встроены в MS Excel, результаты расчетов представлены в табл. 1.

Таблица 1

Результаты вычислений

Модель	Уравнение	R^2
Линейная	$y = 3{,}051 \cdot x - 6{,}254$	0,6510
Экспоненциальная	$y = 1{,}196 \cdot exp(0{,}293 \cdot x)$	0,7942
Логарифмическая	$y = 12{,}58 \cdot ln(x) - 7{,}376$	0,4863
Степенная	$y = 0{,}85 \cdot x^{1{,}349}$	0,7389
Полиномиальная (2-я степень)	$y = 0{,}29x^2 - 0{,}72x + 2{,}54$	0,7058
Полиномиальная (3-я степень)	$y = 0{,}006x^3 + 0{,}17x^2 - 0{,}07x + 1{,}69$	0,706
Полиномиальная (4-я степень)	$y = -0{,}018x^4 + 0{,}46x^3 - 3{,}75x^2 + 12{,}38x - 9{,}2493$	0,7201
Полиномиальная (5-я степень)	$y = -0{,}02x^5 + 0{,}56x^4 - 6{,}34x^3 + 31{,}71x^2 - 65{,}09x + 42{,}89$	0,8284
Полиномиальная (6-я степень)	$y = -0{,}007x^6 + 0{,}266x^5 - 3{,}67x^4 + 24{,}62x^3 - 81{,}32x^2 + 122{,}33x - 61{,}09$	0,9498

где x = (год – 2012), то есть номер точки.

Из табл. 1 видно, что наилучший результат получен при описании данных полиномом 6 порядка, однако обычно применяют полиномы 1–3 сте-

пени. Полиномы высоких степеней использовать нецелесообразно для выделения тенденции, так как полученные аппроксимирующие функции будут отражать случайные отклонения [3]. При описании данных полиномом третьего порядка коэффициент нелинейной регрессии равен 0.706 (рис. 2), который меньше коэффициента регрессии полученный при использовании экспоненциальной модели (0,7942).

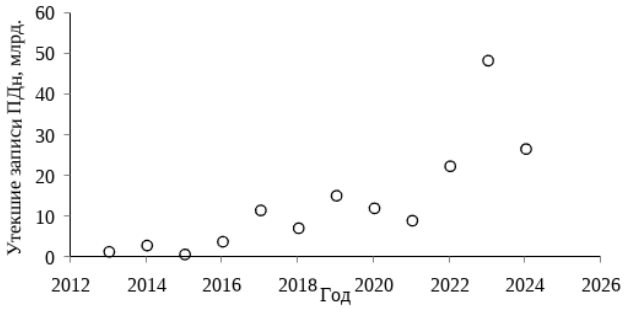

Рис. 2. Описание утечек информации (символ – статистические данные; линия – расчет по экспоненциальной модели; пунктирная линия – полином 6-го порядка)

Если провести аналогию с физической химией [4], где константа скорости реакций описывается уравнением Аррениуса:

$$k = A \cdot exp\left(-\frac{E_a}{R \cdot T}\right),$$

где A – предэкспоненциальный множитель, показывающий общее число столкновений молекул; E_a – энергия активации; R – универсальная газовая постоянная; T – температура процесса [4].

Размерность предэкспоненциального множителя совпадает с размерностью константы скорости реакции, таким образом в нашем случае:

$$y = 1.196 \cdot exp(0.293 \cdot x).$$

x входит в показатель степени, таким образом количество утечек информации (y) очень чувствительна к изменению номера точки (года). С каждым последующим годом количество утечек увеличивается экспоненциально. Обнуление степени экспоненты, количество утечек ПДн (млрд) становится равной 1,196, что показывает частоту числа утечек ПДн в миллиардах.

При подстановке в полученное уравнение точек, соответствующих 2025–2027 гг., получаем, что в 2025 г. число утечек увеличится в 2 раза (54 млрд) во всем мире по сравнению с 2024 г., а в 2027 составит уже 97 млрд.

Такие данные безусловно связаны с напряженной ситуацией во всем мире. В январе и феврале 2025 г. Роскомнадзором уже зафиксировано 19 фактов утечек ПДн, в результате которых в открытом доступе оказались более 24 млн записей российских пользователей [8].

Список использованных источников:

1. Уголовный кодекс Российской Федерации // Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/?ysclid =m9nqa3dtg3694793877 (Дата обращения: 19.04.2025).

2. Утечки информации в мире, 2022–2023 гг. // Экспертно-Аналитический центр InfoWatch. 2024 г. URL: https://www.infowatch.ru/ sites/default/files/ analytics/files /issledovaniye-utechek-informatsii-v-mire-za-2022-2023-gody.pdf?ysclid=m9kwhev8ln20907 4874 (дата обращения: 17.04.2025).

3. Саженкова Т.В., Пономарев И.В., Пронь С.П. Методы анализа временных рядов: учебно-методическое пособие. Барнаул: Изд-во Алт. ун-та. 2020. 60 с.

4. Янборисов В.М., Султанова А.А., Колесов С.В., Фризен А.К., Улитин Н.В. Моделирование механизма полимеризации метилметакрилата в присутствии азобисизобутиронитрила и ферроцена методом Монте-Карло // Вестник технологического университета. 2015. Т. 18. № 18. С. 51–53.

5. Постовалов О.В. Математическое моделирование на основе теории причинности в приложении к криминалистической характеристике и профилактике преступлений // Правовое государство: теория и практика. 2020. С. 152–160.

6. Янборисов В.М., Султанова А.А., Колесов С.В. Модель вещественно-инициированной полимеризации метилметакрилата в массе // Системы управления и информационные технологии. 2015. Т. 62. № 4. С. 24–30.

7. Дианов Д.В. Прикладные статистические исследования экономической безопасности. М.: Русайнс. 2022. 194 с.

8. Роскомнадзор: в сеть утекло 24 млн записей россиян с начала 2025 г. Iaassaaspaas. Обзор ИТ решений для бизнеса и государства. 13.03.2025г. URL: https://iaassaaspaas.ru/news/okolo-milliarda-strok-personalnyh-dannyh-uteklo-v-set-za-polgoda-nikakie-shtrafy-ne-pomogayut (дата обращения: 17.04.2025).

Rezbaev V.M.
Sterlitamak branch of Ufa University
of Science and Technology, terlitamak

Scientific supervisor:
Kornilova A.A.
Ufa University of Science and Technology, Ufa

MATHEMATICAL MODELING OF TIME SERIES OF STOLEN PERSONAL DATA RECORDS WORLDWIDE

Abstract. The paper presents a description of statistical data on leaked records of personal data in the world in the period from 2013 to 2024. It is shown that the data with the highest correlation coefficient are described by an exponential function. The interpretation of the obtained results and a forecast of the number of leaks of personal data for 2025–2027 are carried out.

Keywords: mathematical modeling, forecast, personal data, leak.

УДК 004.056

Шамсутдинов Б.С.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Валеев С.С.
Уфимский университет науки и технологий, Уфа

МЕТОДЫ ЗАЩИТЫ QR-КОДОВ ОТ ПОДДЕЛКИ

Аннотация. Для защиты QR-кодов от подделки важно использовать комплексный подход, основанный на использовании криптографических методов защиты информации, защищенные информационные платформы, двухфакторные аутентификацию. Применение этих методов защиты информации повышает сложность и стоимость использования QR-кодов, однако снижает риски использования их в целях фишинга и кражи данных. В докладе рассматривается пример генерации QR-кода и цифровой подписи.

Ключевые слова: QR-код, методы защиты, цифровая подпись.

Защита QR-кодов от подделки – актуальная задача в условиях активного их использования в системах логистики. Злоумышленники используют технологии копирования и замены QR-кодов для различных схем фишинга и кражи данных. Для защиты от этого можно использовать следующие методы [1–4]:

– использование защищенных цифровых платформ генерации QR-кодов. Для повышения безопасности следует создавать QR-коды с помощью специализированных цифровых сервиов, обеспечивающих дополнительную защиту подлинности QR-кода. Например, шифрование содержимого QR-кода, добавления цифровой подписи или проверки подлинности сканируемого адреса перед переходом по ссылке, полученной из QR-кода;

– шифрование данных. Использование криптографического алгоритма для шифрования информации внутри QR-кода помогает предотвратить несанкционированное чтение данных. Это значительно усложняет процесс подделки, поскольку сначала необходимо расшифровать данные, что требует занаие ключа;

– цифровая подпись. Применение цифровых подписей используется для подтверждения подлинности QR-кода. Когда пользователи сканируют код, специальное приложение проверяет цифровую подпись и подтверждает ее подлинность. Если подпись отсутствует или повреждена, то система предупреждает пользователей о возможной угрозе;

– контроль над распространением кода. Это ограничение распространение QR-кодов только через проверенные каналы распространения. В этом случае необходимо контролировать размещение QR-кода на открытых информационных платформах. Необходимо проводить мониторинг размещенных QR-кодов, чтобы убедиться в отсутствии подделок;

– обучение пользователей и персонала компаний. Необходимо информировать их о потенциальных рисках и правилах безопасного обмена информацией с помощью QR-кодов;

– использование двухфакторной аутентификации. Добавление второго уровня авторизации после сканирования QR-кода, содержащего ссылку на информационный ресурс снижает вероятность взлома злоумышленником аккаунта даже в случае успешной атаки. Пользователю при применении этого кода потребуется ввести дополнительный пароль или одноразовый код, отправленный на зарегистрированный номер телефона или электронную почту.

Пример применения цифровой подписи представлен на рис. 1.

Рис. 1. QR-код и цифровая подпись

Для защиты QR-кодов от подделки важно использовать комплексный подход, основанный на использовании криптографических методов защиты информации, защищенные информационные платформы, двухфакторные аутентификацию. Применение этих методов защиты информации повышает сложность и стоимость использования QR-кодов, однако снижает риски использования их в целях фишинга и кражи данных.

Список использованных источников:

1. Smith J. (2020). *The Security Risks of Barcode Systems. Journal of Information Security, 12(3), 45–58.

2. Jones A., Taylor, R. (2019). Best Practices for Secure Barcode Implementation. International Journal of Technology Management, 15(2), 123–134.

3. SO/IEC 15420:2009. Information technology – Automatic identification and data capture techniques – Bar code print quality test specification*. International Organization for Standardization.

4. National Institute of Standards and Technology (NIST). (2022). Guidelines for Securing Barcode Systems.

Shamsutdinov B.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Valeev S.S.
Ufa University of Science and Technology, Ufa

METHODS OF PROTECTING QR CODES FROM FORGERY

Abstarct: To protect QR codes from forgery, it is important to use an integrated approach based on the use of cryptographic information protection methods, secure information platforms, and two-factor authentication. The use of these information protection methods increases the complexity and cost of using QR codes, but reduces the risks of using them for phishing and data theft. The report examines an example of QR code generation and digital signature.

Keywords: QR code, security methods, digital signature.

СЕКЦИЯ 2. СОВРЕМЕННЫЕ ВЫЗОВЫ В ОБЛАСТИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.49

Агапова В.О.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

Научный руководитель:
Лихачевский Д.В.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

АНАЛИЗ МЕТОДОВ СКРЫТИЯ ВРЕДОНОСНЫХ ПРИЛОЖЕНИЙ

Аннотация. В статье рассматриваются методы, которыми вредоносные приложения стремятся ухитриться и уйти от обнаружения в *sandbox*-средах и антивирусных системах. Приведен анализ основных техник, выявлены их преимущества и ограничения. Рассмотрены возможные подходы к противодействию таким механизмам.

Ключевые слова: вредоносное посещение, *sandbox*, антивирусная защита, эвазия, кибербезопасность.

Введение

Современные атаки на информационные системы зачастую осуществляются через внедрение вредоносных приложений. Для их обнаружения и исследования широко используются *sandbox*-среды и антивирусы. Тем не менее, авторы вредоносных ПО создают техники, позволяющие уклоняться от их обнаружения.

Основная часть

Техники уклонения от *sandbox'ов* и антивирусов можно условно разделить на несколько категорий:

Обнаружение виртуальной среды

Многие *sandbox'ы* используют виртуальные машины (*VM*) для изоляции исполняемого кода. Вредоносные приложения анализируют признаки виртуализации, такие как наличие специфических драйверов (например, *VBoxGuest.sys*, *vmhgfs.sys*), виртуальных сетевых адаптеров (*vmxnet3*, *virtio*) или неестественные конфигурации оборудования (необычно маленький объем памяти, один процессор, отсутствие физических устройств) [5].

Расширенные методы обнаружения *VM* включают:

Определение задержек выполнения инструкций, характерных для виртуализации (например, через *RDTSC*, *RDPMC*, *CPUID*) [3].

Считывание специфических *CPUID*-инструкций (*Hypervisor present bit, hypervisor vendor ID*).

Проверку нестандартных размеров кэш-памяти (*L3 cache*) и особенностей структуры *ACPI*-таблиц.

Сканирование имен *BIOS'ов* и производителей оборудования на наличие упоминаний о виртуализации (например, *VMware, VirtualBox, QEMU*) [5].

Анализ специфических процессов и сервисов, характерных для *VM* (например, *vboxservice.exe, vmtoolsd.exe*).

Новейшие техники:

Использование побочных каналов (*side-channel analysis*) для определения наличия гипервизора [3].

Атаки через чтение аномалий работы *TLB* (*Translation Lookaside Buffer*) и кэш-памяти.

Некоторые вредоносные программы даже динамически меняют свое поведение, например, активируются только в случае отсутствия признаков виртуализации. Более того, в некоторых случаях осуществляется активная имитация нестабильной работы программного обеспечения, чтобы спровоцировать *sandbox* на преждевременное завершение анализа. Часто также применяются техники контроля температуры *CPU* и частоты отклика устройств ввода, поскольку виртуальные среды не всегда корректно эмулируют физические параметры реального оборудования.

Проверка времени выполнения

Sandbox-окружения ограничены по времени анализа (обычно от нескольких секунд до 5 минут), чтобы минимизировать ресурсы.

Классические техники:

Использование задержек (*sleep, NtDelayExecution*), нередко с модификацией параметров таймера для обхода простого пропуска времени анализа (*sleep-patching*) [2].

Измерение реального времени через *RDTSC, GetTickCount*(), *QueryPerformanceCounter*().

Расширенные методы:

Использование техник *sleep obfuscation*: выполнение коротких периодов сна, перемежаемых безвредной активностью [1].

Завуалированные задержки через ресурсоемкие задачи: перебор данных, бесконечные циклы с условием выхода в зависимости от времени.

Environmental Keying: активация вредоносного кода только по достижении определенного времени, даты или события (например, запуск только в пятницу вечером). Дополнительно, некоторые вредоносные программы анализируют изменения системных часов в процессе выполнения, чтобы выявить попытки искусственного ускорения времени *sandbox'ом*. Применяются также таймеры на базе внешних событий, таких как отклик сетевого оборудования или появление новых процессов пользователя, что затрудняет форсированную эмуляцию активности.

Ожидание пользовательского взаимодействия

Sandbox'ы часто не моделируют реальное поведение пользователя.

Традиционные методы:

Проверка наличия движения мыши (*GetCursorPos*, *GetLastInputInfo*) [2].

Ожидание ввода текста или нажатия клавиш (*GetAsyncKeyState*, *SetWindowsHookEx*).

Расширенные техники:

Анализ естественности движений мыши: криволинейность, скорость, ускорение.

Ожидание нескольких разных типов взаимодействия: клик + перетаскивание + прокрутка + закрытие окна.

Проверка фоновых приложений и их активности (проверка наличия популярных приложений: *Chrome, Teams*, *Skype*, антивирусных процессов).

Слежение за состоянием окон: минимизация, разворачивание окон и фокус ввода. Также вредоносные программы могут измерять скорость и ритм набора текста, определяя, являются ли нажатия клавиш результатом реальной деятельности человека или автоматизированного скрипта. В некоторых случаях вредоносный код ожидает многократных взаимодействий с разными окнами, что трудно воспроизвести в *sandbox'ax* за короткий период анализа.

Шифрование, упаковка и полиморфизм

Шифрование частей кода, полиморфизм и метаморфизм позволяют избегать статического анализа.

Методы:

Полиморфизм: изменение структуры кода без изменения функциональности при каждом запуске.

Метаморфизм: полное переписывание кода, создание новых функций с тем же поведением [1].

Упаковка с помощью известных или самописных пакеров (*UPX, Themida*, собственные крипторы).

Использование стеганографии: сокрытие вредоносного кода внутри изображений, документов и других медиафайлов.

Новые тренды:

Fileless Malware: использование легитимных системных инструментов (например, *PowerShell*, *WMI*, *Living-off-the-Land Binaries – LOLBins*) без записи файлов на диск.

Атаки через многослойную упаковку: вредоносный код зашифрован несколько раз с использованием разных алгоритмов и методов упаковки. При этом некоторые современные обфускаторы могут динамически изменять сигнатуры *API*-вызовов и использовать методы шифрования с одноразовыми ключами (OTP), что практически исключает возможность статической декомпиляции. Нередко также применяется внедрение промежуточных виртуальных машин внутри основного кода, усложняющее процесс анализа.

Использование легитимных процессов

Классические методы:

Process Hollowing: создание процесса, замена его кода вредоносным [2].

DLL Injection: внедрение своей библиотеки в адресное пространство другого процесса.

Parent Process Spoofing: подмена родительского процесса для маскировки активности.

Современные методы:

AtomBombing: внедрение кода без изменения памяти процесса напрямую через атомарные таблицы *Windows*.

Process Doppelgänging: создание процесса с использованием *NTFS*-транзакций для запуска вредоносного кода без фактического сохранения исполняемого файла на диск [4].

Heaven's Gate: переход между 32-битным и 64-битным режимами исполнения в *Windows* для обхода системных ограничений.

Callback Injection: использование легитимных функций *Windows* (например, *CreateRemoteThread*, *QueueUserAPC*) для внедрения кода.

Дополнительно:

Инжекция через сетевые стеки (например, внедрение через фильтры сетевого драйвера).

Использование *Trusted Installer* сервисов для запуска вредоносного кода с привилегиями *SYSTEM*. Все чаще встречаются сложные многоступенчатые схемы, где вредоносный код сначала захватывает управление над менее защищенными пользовательскими процессами, а затем через цепочку внедрений переходит к системным службам. Используется также методика внедрения через COM-объекты, когда вредоносный код регистрирует себя как легитимный обработчик событий в системе.

Список использованных источников:

1. You I., Yim K. Malware Obfuscation Techniques: A Brief Survey. – 2010.

2. Egele M., Scholte T., Kirda E., Kruegel C. A Survey on Automated Dynamic Malware-Analysis Techniques and Tools. ACM Computing Surveys, 2012.

3. Dinaburg A., Royal P., Sharif M., Lee W. Ether: Malware Analysis via Hardware Virtualization Extensions. Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS), 2008.

4. Moser A., Kruegel C., Kirda E. Exploring Multiple Execution Paths for Malware Analysis. –Proceedings of the 2007 IEEE Symposium on Security and Privacy.

5. Ugarte-Pedrero X., Santos I., Bringas P.G., Alvarez G. Countering virtualization detection techniques. Computers & Security, 2015.

Agapova V.O.
Belarusian State University of
Informatics and Radioelectronics, Minsk

Scientific supervisor:
Likhachevsky D.V.
Belarusian State University of
Informatics and Radioelectronics, Minsk

ANALYSIS OF METHODS FOR HIDING MALICIOUS APPLICATIONS

Abstract. The article examines the methods by which malicious applications attempt to evade detection in sandbox environments and antivirus systems. An analysis of the main techniques is presented, highlighting their advantages and limitations. Possible approaches to counteracting these mechanisms are considered.

Keywords: malicious application, sandbox, antivirus protection, evasion, cybersecurity.

УДК 004.49

Агапова В.О.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

Научный руководитель:
Лихачевский Д.В.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

ИСПОЛЬЗОВАНИЕ ШИФРОВАНИЯ, ЗАЩИЩЕННОЙ ПАМЯТИ И KEYSTORE API ДЛЯ ЗАЩИТЫ ДАННЫХ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ

Аннотация. В статье рассматриваются современные методы обеспечения безопасности данных в мобильных приложениях на платформе *Android*. Особое внимание уделено использованию шифрования, защищенной памяти устройств и возможностей *KeyStore API* для хранения криптографических ключей. Описаны преимущества каждого из подходов, а также приведены рекомендации по их комбинированному использованию для повышения общей защищенности приложений.

Ключевые слова: мобильная безопасность, шифрование данных, защищенная память, *KeyStore API, Android*.

Введение

Мобильные устройства повсеместно используются для хранения и обработки конфиденциальной информации. В связи с этим возрастает необходимость в надежных механизмах защиты данных как при их хранении, так и при передаче. Платформа *Android* предоставляет разработчикам ряд инструментов для обеспечения безопасности, включая механизмы шифрования, использование защищенных хранилищ и специализированные *API* для управления криптографическими ключами.

Основная часть

Применение шифрования данных

Шифрование позволяет сделать данные нечитаемыми для злоумышленников в случае их перехвата или несанкционированного доступа [1], [2]. В *Android* доступны как стандартные алгоритмы симметричного шифрования (например, *AES*-256 с режимами *GCM* или *CBC*), так и асимметричного (*RSA, ECC*) [3]. Кроме того, активно развивается использование алгоритмов постквантовой криптографии, обеспечивающих защиту от будущих угроз, связанных с появлением квантовых компьютеров [1].

Для повышения безопасности рекомендуется:

- применять современные и проверенные временем криптографические библиотеки (например, *BouncyCastle, Conscrypt*) [1];
- использовать надежные схемы управления ключами, включая генерацию уникальных сессионных ключей [2];
- реализовывать двойное шифрование особо чувствительных данных (двухступенчатую криптографию) [3].

Также важно обеспечивать защиту данных как «на покое» (*data at rest*), так и «в пути» (*data in transit*), применяя защищенные транспортные протоколы, такие как *TLS* 1.3 [2], [5].

Использование защищенной памяти

Современные мобильные устройства оснащаются доверенными средами исполнения (*Trusted Execution Environment, TEE*) или безопасными элементами (*Secure Element, SE*), обеспечивающими физическую и логическую защиту критически важных данных [1].

TEE, реализуемый, например, на базе *ARM TrustZone*, позволяет изолировать выполнение кода безопасности от основной операционной системы, обеспечивая:

- безопасное выполнение криптографических операций [1];
- проверку целостности приложений и среды выполнения [1];
- надежное хранение биометрических данных (отпечатков пальцев, сканов лица) [1].

Secure Elements представляют собой специализированные микросхемы, соответствующие банковским и государственным стандартам безопасности (например, *Common Criteria EAL* 5+), что делает их

оптимальным выбором для хранения особо важных данных, таких как ключи цифровых кошельков или идентификационные токены [2].

В *Android* реализована поддержка *Protected Confirmation API* и *Identity Credential API*, позволяющих использовать возможности защищенной памяти для безопасного подтверждения пользовательских операций и хранения цифровых документов [1].

Использование *KeyStore API*

KeyStore API Android предоставляет разработчикам возможность безопасной генерации, хранения и использования криптографических ключей без прямого доступа к ним со стороны приложения [1].

Особенности *KeyStore API*:

- ключи могут быть помечены как требующие аутентификацию пользователя (например, с помощью отпечатка пальца или распознавания лица) [1];
- возможность установки срока действия ключей и ограничений по числу применений [1];
- использование аппаратных модулей безопасности (*Hardware-Backed Keystore*) для предотвращения атак через извлечение из памяти [1].

Кроме того, в последних версиях Android (начиная с *Android* 9 *Pie*) доступны расширенные функции:

- *StrongBox Keymaster* – модуль, обеспечивающий еще более строгую аппаратную защиту ключей в отдельном чипе [1];
- поддержка безопасной генерации асимметричных пар ключей для подписания данных и аутентификации без передачи закрытого ключа [5].

Преимущества комплексного использования

Комбинирование технологий шифрования, защищенной памяти и *KeyStore API* позволяет достичь максимально возможного уровня защиты данных в мобильных приложениях [1], [2]:

- минимизация риска кражи данных даже при физическом доступе к устройству или взломе операционной системы [1];
- защита ключей и чувствительной информации от утечек через приложения, перехват трафика или эксплойты нулевого дня [1];
- повышение доверия пользователей благодаря соответствию приложения современным требованиям законодательства и стандартов безопасности (*GDPR, HIPAA, PCI DSS*) [4];
- устойчивость к новым угрозам, включая атаки с использованием квантовых вычислений и атаки по сторонним каналам (*side-channel attacks*) [1], [3].

В совокупности эти методы позволяют создать надежную архитектуру защиты мобильных приложений, минимизируя потенциальные риски и обеспечивая долгосрочную безопасность пользовательских данных [1].

Заключение

Обеспечение защиты данных в мобильных приложениях требует применения многоуровневых подходов. Использование шифрования,

защищенной памяти и *KeyStore API* позволяет значительно повысить безопасность пользовательских данных. В условиях растущего числа угроз разработчикам следует учитывать данные методы при проектировании архитектуры приложений и реализации механизмов хранения и обработки чувствительной информации.

Список использованных источников:

1. Stallings W. Cryptography and Network Security: Principles and Practice. 7th ed., Pearson, 2016.
2. Kaufman C., Perlman R., Speciner M. Network Security: Private Communication in a Public World. 2nd ed., Prentice Hall, 2002.
3. Menezes A.J., van Oorschot P.C., Vanstone, S.A. Handbook of Applied Cryptography. CRC Press, 1996.
4. Barkley J. Implementing Role-Based Access Control Using CORBA Security Service. –Proceedings of the Third ACM Workshop on Role-Based Access Control, 1998.
5. Housley R., Polk W., Ford W., Solo D. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. IETF RFC 5280, 2008.

Agapova V.O.
Belarusian State University of
Informatics and Radioelectronics, Minsk

Scientific supervisor:
Likhachevsky D.V.
Belarusian State University of
Informatics and Radioelectronics, Minsk

ANALYSIS OF METHODS FOR HIDING MALICIOUS APPLICATIONS FROM SANDBOXES AND ANTIVIRUS SYSTEMS

Abstract. The article examines modern methods of ensuring data security in mobile applications on the Android platform. Particular attention is paid to the use of encryption, secure device memory, and the capabilities of the KeyStore API for cryptographic key storage. The advantages of each approach are described, along with recommendations for their combined use to enhance the overall security of applications.

Keywords: mobile security, data encryption, secure memory, KeyStore API, Android.

УДК 004.056.53

Алейникова Д.И.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

Научный руководитель:
Белоусова Е.С.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

МЕТОДИКА КОНФИГУРАЦИИ SIEM-СИСТЕМ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛЬНЫХ ДЕЙСТВИЙ В КОРПОРАТИВНОЙ СЕТИ

Аннотация. В статье представлена методика конфигурации SIEM-системы для обнаружения аномальных действий в корпоративной сети. Приведены примеры аномальных действий в корпоративной сети. Рассмотрены отличия сигнатурных правил корреляции от правил, основанных на поведенческом анализе, разработанных на основе данных базы знаний Mitre Att&ck.

Ключевые слова: система мониторинга, SIEM-система, методика конфигурации, корреляция, выявление инцидентов, Mitre Att&ck.

Введение

В настоящее время информационная безопасность является одним из приоритетных направлений для любой организации. Для своевременного выявления угроз и инцидентов применяются системы класса SIEM (Security Information and Event Management). Следует отметить, что эффективность работы SIEM-системы определяется правильностью ее конфигурации с учетом специфики конкретной информационной инфраструктуры.

Основная часть

SIEM-система – ключевой компонент в архитектуре SOC (Security Operational Center), обеспечивающий централизованный сбор событий информационной безопасности, мониторинг, выявление аномальных действий в корпоративной сети и оповещение команды реагирования о выявленных инцидентах [1].

К аномальным действиям могут относиться любые отклонения от штатной работы автоматизированных систем и поведения пользователей. Среди наиболее распространенных примеров таких действий можно выделить:

– попытки авторизации в локальной сети работниками в нерабочее время или из нетипичных геолокация, например, другой страны;

– несанкционированное повышение привилегий пользователем, не имеющим соответствующих полномочий;

– попытки доступа к конфиденциальной информации с устройств, с которых такой доступ не предусмотрен;

– запуск PowerShell или командной строки пользователем, работа которого не подразумевает использование данных инструментов;

– создание и изменение учетных записей без согласования с работниками отдела информационной безопасности и отдела информационных технологий;

– несогласованное с работниками отдела информационной безопасности и отдела информационных технологий изменение конфигураций оборудования.

Для своевременного выявления подобных угроз информационной безопасности можно эффективность конфигурации SIEM путем проведения анализа информационной инфраструктуры организации, определения критически важных активов, использования адаптивных правил корреляции, комбинировании сигнатурных правил корреляции и основанных на поведенческом анализе, а также использования актуальных баз знаний по техникам нарушителей, например, Mitre Att&ck [2].

Mitre Att&ck – это открытая база знаний о моделях поведения нарушителей информационной безопасности, основанная на реальных данных о кибератаках. Также она классифицирует тактики, техники и процедуры, которые применяются при проникновении в информационные системы и развитии кибератаки внутри сети.

Методика конфигурации SIEM-систем включает в себя следующие основные этапы:

1 Анализ информационной инфраструктуры организации. На данном этапе необходимо определить критически важные активы, используемые средства защиты, а также пользователей, обладающих повышенными привилегиями.

2 Подключение источников событий к SIEM-системе. На данном этапе необходимо настроить отправку логов оборудования, систем аутентификации, используемых в организации приложений и средств защиты в SIEM-систему. Следует отметить, что современные SIEM-системы обладают функционалом по нормализации получаемых логов – приведение их к единому формату для дальнейшего анализа.

3 Построение профиля нормального поведения пользователей и работы автоматизированных систем локальной сети. На данном этапе необходимо провести анализ штатной активности автоматизированных систем и пользователей локальной сети.

4 Настройка правил корреляции в SIEM-системе. На данном этапе существует несколько подходов к разработке правил корреляции – сигнатурные и с использованием поведенческого анализа.

Сигнатурные правила корреляции основываются на известных шаблонах событий, которые указывают на конкретные типы кибератак. Такие правила срабатывают при наличии точного совпадения настроенных в правиле параметров с данными из агрегируемых логов, таких как: идентификаторы событий, хэши вредоносных файлов, имена и пути расположения вредоносных процессов, обращения на IP-адреса и доменные имена, связанные с вредоносной активностью, точные команды с определенными параметрами, запускаемые в PowerShell. Преимущество сигнатурных правил: высокая точность при обнаружении уже известных угроз. Недостаток: не позволяют выявлять новые или модифицированные атаки.

Правила, основанные на поведенческом анализе, ориентированы на анализ отклонения от штатной работы систем и пользователей локальной сети, обычно подразумевают реализацию определенных цепочек событий, отражающих логику действий нарушителя информационной безопасности. Для построения таких цепочек событий можно использовать открытую базу знаний Mitre Att&ck. Преимущество правил, основанных на поведенческом анализе: позволяют выявлять новые или модифицированные атаки. Недостаток: большое количество ложных сработок, требующих проведения повторного анализа цепочки событий и правила корреляции, его корректировки.

5 Тестирование и корректировка. На данном этапе происходит тестирование настроенных правил корреляции, анализ ложных срабатываний SIEM-системы, корректировка и доработка созданных правил корреляции. Для снижения количества ложных срабатываний можно воспользоваться списками исключений и подбором более точных условий агрегации событий, доработкой логики работы правила.

6 Непрерывное обновление и обогащение SIEM-системы. Необходимо регулярно пересматривать правила корреляции и актуализировать их для своевременного выявления новых угроз, а также обновлять используемые списки исключений и базы сигнатур. Необходимо на постоянной основе отслеживать наличие логов оборудования, систем аутентификации, используемых в организации приложений и средств защиты в SIEM-системе, по мере увеличения информационной инфраструктуры подключать новые источники.

Следует отметить, что после обнаружения аномальных действий в корпоративной сети важно обеспечить своевременное реагирование. Для этого необходимо разработать сценарии реагирования на инциденты, возможно, настроить интеграцию со специализированными средствами автоматизации для повышения эффективности реагирования.

Заключение

Эффективная конфигурация SIEM-системы – это непрерывный процесс, подразумевающий комплексный подход, учитывающий особенности информационной инфраструктуры организации, модели

поведения нарушителей информационной безопасности и легитимных пользователей локальной сети, а также особенности архитектуры используемой SIEM-системы и ее механизмы сбора, обработки и анализа событий информационной безопасности. Использование базы знаний Mitre Att&ck при конфигурировании SIEM-системы позволяет существенно обогатить логику ее работы, так как в таком случае правила корреляции основаны на логике реализации атаки, ее последовательных этапах, а не только на использовании сигнатур. Дополнение сигнатурных правил корреляции правилами, основанными на поведенческом анализе позволяет выявлять более сложные или неизвестные ранее атаки, что значительно повышает уровень защищенности корпоративной сети.

Список использованных источников:

1. Алейникова Д.И. Системы управления информационной безопасностью и событиями информационной безопасности // Технические средства защиты информации: материалы XXIII Международной научно-технической конференции, Минск, 08 апреля 2025 г. Минск: БГУИР, 2025. С. 51–54.

2. Таблица Attack Mitre. // Mitre: официальный сайт. 2025. URL: https://attack.mitre.org/ (дата обращения: 22.04.2025).

Aleinikova D.I.
Belarusian State University of
Informatics and Radioelectronics, Minsk

Scientific supervisor:
Belousova E.S.
Belarusian State University of
Informatics and Radioelectronics, Minsk

THE METHODOLOGY FOR CONFIGURING SIEM SYSTEMS TO DETECT ABNORMAL ACTIVITY IN A CORPORATE NETWORK

Abstract. The methodology for configuring a SIEM system to detect abnormal activity in a corporate network is considered. Examples of abnormal actions in the corporate network are given. The differences between the signature rules of correlation and the rules based on behavioral analysis, developed on the basis of data from the Mitre Att&ck knowledge base, are considered.

Keywords: monitoring system, SIEM system, configuration methodology, correlation rules, incident detection, Mitre Att&ck.

УДК 004.056

Александрова В.М.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

МЕРЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПРИ ВЗАИМОДЕЙСТВИИ СОТРУДНИКОВ СО СТОРОННИМИ ОРГАНИЗАЦИЯМИ

Аннотация. В статье рассматриваются угрозы информационной безопасности, возникающие при взаимодействии сотрудников организации со сторонними организациями. Особое внимание уделяется обоснованию и этапам разработки мер организационной защиты конфиденциальной информации при взаимодействии сотрудников организации со сторонними организациями.

Ключевые слова: информация, организационная защита информации, риски информационной безопасности, конфиденциальная информация.

Обеспечение безопасности конфиденциальной информации является важным составляющим деятельности для любой организации, особенно это касается вопросов взаимодействия со сторонними организациями. Для эффективной защиты конфиденциальности необходимо разработать комплекс мер организационного характера, направленных на минимизацию рисков утечки и несанкционированного доступа (НСД) к важной информации при взаимодействии со сторонними организациями.

Рассматривая в общем организационные угрозы, по характеру воздействия их можно разделить на:

- угрозы воздействия на персонал заинтересованными лицами;
- действия самого персонала [1].

Воздействие на сотрудников может быть как физическим, так и психологическим. Действия персонала, которые могут создавать угрозы безопасности защищаемой информации, могут быть преднамеренными или непреднамеренными (случайными). Таким образом, организационные угрозы либо направлены против персонала компании, либо реализуется через них, т. е. сами сотрудники компании рассматриваются как источник организационных угроз информационной безопасности.

Воздействие на сотрудников, как отмечалось ранее, может быть двух видов:

1. Физическое. Физическое воздействие на сотрудников заключается в том, что злоумышленник действует на самого сотрудника, чтобы заставить его или косвенно через других людей получить конфиденциальную

информацию или нарушить работу определенных организационных процессов компании. Эти инциденты расследуются службой информационной безопасности организации и правоохранительными органами.

2. Психологическое. При психологическом воздействии на работников можно рассматривать такие распространенные методы влияния в области информационной безопасности, как шантаж, взяточничество, социальная инженерия и многие другие.

Современные организации регулярно взаимодействуют с различными контрагентами – поставщиками, клиентами, подрядчиками и др. При этом происходит постоянный обмен информацией различного уровня секретности. Это взаимодействие несет потенциальные риски ИБ, такие как утечка коммерческих тайн, нарушение законодательства о защите персональных данных, компрометации репутации предприятия и др. Для предотвращения негативных последствий необходимы меры организационно-правового регулирования процессов обмена конфиденциальной информацией между сотрудниками и представителями сторонних организаций.

Основные направления разработки мер организационной защиты:

1. Разработка внутренней политики информационной безопасности. Необходимо создать политику ИБ, регламентирующую правила обращения с конфиденциальной информацией внутри организации и при работе с внешними субъектами. Документально закрепленные положения позволят сотрудникам четко понимать требования и последствия нарушения данных правил обработки информации. Важно включить и задокументировать следующие положения: классификацию уровней секретности документов; порядок допуска сотрудников к закрытой информации; процедуры передачи информации внешним организациям; запрет разглашения конфиденциальной информации третьим лицам без согласования руководства [2].

2. Организация контроля доступа сотрудников к защищаемым данным. Следует внедрить систему ограничения доступа к документам и ресурсам, содержащим коммерческую тайну или персональные данные. Только сотрудники, непосредственно вовлеченные в процесс взаимодействия с партнерами, должны иметь возможность получать доступ к такому виду сведениям. Примерами методов реализации являются: использование паролей и многоуровневой аутентификации пользователей; установка автоматизированных систем мониторинга действий сотрудников с файлами; периодическое обновление инструкций по использованию защищенных каналов связи. Система Аккорд-АМДЗ предназначена для комплексного разграничения доступа сотрудников к защищенной информации на различных уровнях сетевых и аппаратных компонентов организации. Она представляет собой специализированное решение, ориентированное на российские стандарты информационной безопасности и применяемое преимущественно государственными учреждениями и предприятиями оборонно-промышленного комплекса.

3. Регулирование процесса обмена конфиденциальной информацией. Все процессы взаимодействия сотрудников организации со сторонними организациями должны быть строго формализованы. Передача важных сведений должна осуществляться исключительно в рамках установленных процедур и с соблюдением соответствующих требований закона. Меры включают: подписание соглашений о неразглашении (NDA), контроль сроков хранения переданных материалов, применение шифрования электронной почты и иных каналов коммуникации [3].

4. Повышение осведомленности персонала. Сотрудники должны осознавать важность соблюдения норм безопасности информацию и ответственности за возможные негативные последствия несоблюдения регламентов ИБ. Рекомендуется проведение регулярных тренингов и семинаров по вопросам информационной безопасности.

5. Мониторинг эффективности защитных мероприятий. Постоянная оценка качества существующих мер защиты информации позволяет своевременно выявлять слабые места системы защиты и вносить необходимые изменения. Эффективность измеряется показателями, такими как количество случаев попыток взлома, уровень информированности сотрудников, скорость реакции службы информационной безопасности на инциденты [4].

Подводя итог, можно сделать вывод, что организационные уязвимости практически всегда появляются из-за отсутствия или неправильного применения механизмов контроля. Если уменьшить количество организационных уязвимостей, уменьшится и количество организационных угроз и атак. Организационные угрозы либо направлены против персонала компании, либо реализуется через них, поэтому защита от организационных угроз должна быть направлена на обучение сотрудников организации информационной безопасности, определение их ответственности в случае нарушения требований информационной безопасности.

Список использованных источников:

1. Баланов А.Н. Комплексная информационная безопасность: учебное пособие для СПО / А.Н. Баланов. 2-е изд., стер. Санкт-Петербург: Лань, 2025. 284 с. Электрон. версия. // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/463001 (дата обращения: 20.04.2025).

2. Ерохин В.В. Безопасность информационных систем: учебное пособие / В.В. Ерохин, Д.А. Погонышева, И.Г. Степченко. 4-е изд., стер. М.: ФЛИНТА, 2022. 184 с. Электрон. версия. // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/232457 (дата обращения: 19.04.2025).

3. Тимофеева Т.Ф. Защита интеллектуальной собственности и информационная безопасность: учебно-методическое пособие / Т.Ф. Тимофеева. Чебоксары: ЧГУ им. И.Н. Ульянова, 2023. 172 с. Электрон. версия. // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/388823 (дата обращения: 20.04.2025).

4. Шагапов И.А. О некоторых вопросах при работе с персоналом, допущенным к конфиденциальной информации предприятия / И.А. Шагапов // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов V Всероссийской молодежной научно-практической конференции, Уфа, 20–21 мая 2022 г. Уфа: Башкирский государственный университет, 2022. С. 39–41. URL: https://confbsu.bashedu.ru/itokbo-2022-05-20/9/ (дата обращения: 20.04.2025).

Aleksandrova V.M.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

MEASURES TO PROTECT CONFIDENTIAL INFORMATION WHEN EMPLOYEES INTERACT WITH THIRD-PARTY ORGANIZATIONS

Abstract. The article examines the threats to information security that arise when employees of an organization interact with third-party organizations. Special attention is paid to the justification and stages of the development of organizational measures for the protection of confidential information in the interaction of the organization’s employees with third-party organizations.

Keywords: information protection rights, organizational information protection, information security risks, confidential information.

УДК 004.7

Ализода С.С.
Белорусский государственный университет информатики и радиоэлектроники, Минск

Научный руководитель:
Лихачевский Д.В.
Белорусский государственный университет информатики и радиоэлектроники, Минск

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ СЕТЕВОЙ БЕЗОПАСНОСТИ

Аннотация. Использование искусственного интеллекта (ИИ) в сетевой безопасности позволяет эффективно обнаруживать и предотвращать атаки, а также анализировать угрозы в реальном времени. ИИ помогает в

автоматизации процессов защиты и реагировании на инциденты. В работе рассматриваются методы применения ИИ, такие как машинное обучение и анализ больших данных, а также возможные риски.

Ключевые слова: ИИ, сетевая безопасность, искусственный интеллект, машинное обучение, защита от атак, аномалии, автоматизация, прогнозирование угроз, киберзащита, безопасность сетей.

В условиях стремительного роста числа кибератак и усложнения методов вторжения традиционные средства защиты компьютерных сетей оказываются недостаточно эффективными [1]. С увеличением объемов передаваемой информации и масштабом атакующих воздействий возникает необходимость в системах, способных адаптироваться к новым условиям и угрозам. В этом контексте технологии искусственного интеллекта (ИИ) становятся ключевым инструментом в арсенале средств кибербезопасности. Их применение позволяет не только оперативно реагировать на инциденты, но и предотвращать атаки еще до того, как они наносят ущерб. В данной статье рассматриваются основные направления использования ИИ в обеспечении сетевой безопасности, а также оцениваются вызовы и перспективы, связанные с этой технологией.

Ранее системы обеспечения сетевой безопасности были в основном основаны на сигнатурных методах – они эффективно справлялись с известными угрозами [2], но были практически бесполезны против новых, неизвестных атак. Такая модель не позволяла вовремя адаптироваться к стремительно меняющемуся ландшафту угроз. Появление систем, использующих поведенческий анализ, стало первым шагом в сторону интеллектуальной безопасности. Однако настоящим прорывом стало внедрение методов машинного обучения и искусственного интеллекта, которые позволили не только фиксировать уже произошедшие инциденты, но и предсказывать потенциальные угрозы на основе большого количества данных.

ИИ способен анализировать сетевой трафик в реальном времени, выявлять аномалии и подозрительную активность, которая не укладывается в рамки стандартного поведения пользователей или систем [3]. Таким образом, он становится активным элементом защиты, а не просто пассивным наблюдателем.

Одним из ключевых направлений применения ИИ в сетевой безопасности является интеллектуальное обнаружение вторжений. Алгоритмы машинного обучения анализируют поведение пользователей, систем и приложений, выявляя отклонения, которые могут свидетельствовать о попытке взлома, заражении вредоносным ПО [4] или компрометации учетной записи. Такие системы непрерывно обучаются, что позволяет им распознавать все более сложные атаки.

Важно отметить, что искусственный интеллект также активно используется в системах автоматического реагирования на инциденты.

После выявления угрозы соответствующая система может в реальном времени изолировать подозрительное устройство, прекратить определенный сетевой процесс или уведомить администратора. Это позволяет значительно сократить время между атакой и началом контрмер, тем самым снижая возможный ущерб.

Кроме того, ИИ находит применение в прогнозировании угроз – на основе исторических данных и текущих трендов формируются модели, позволяющие предугадывать потенциальные сценарии атак [5] и заранее укреплять защиту.

Использование искусственного интеллекта в кибербезопасности дает значительные преимущества. Это прежде всего скорость обработки данных и реагирования, способность обнаруживать ранее неизвестные атаки, а также снижение зависимости от человеческого фактора [6]. В отличие от специалистов, ИИ не устает, не отвлекается и может обрабатывать огромные объемы данных круглосуточно.

Однако существуют и определенные ограничения. Алгоритмы машинного обучения могут быть подвержены ошибкам – например, выдавать ложные срабатывания или, наоборот, пропускать опасные события. Кроме того, существует риск, что злоумышленники начнут использовать ИИ против самих систем безопасности, создавая вредоносные программы, способные обходить интеллектуальные фильтры. Необходимо также учитывать этические аспекты использования ИИ, в том числе вопросы конфиденциальности данных, возможность предвзятости алгоритмов и ограниченность прозрачности в принятии решений.

В ближайшие годы ИИ, скорее всего, станет неотъемлемой частью всех этапов обеспечения сетевой безопасности – от аутентификации пользователей до анализа логов и автоматизации принятия решений. Особое внимание будет уделяться усиленной интеграции ИИ в существующие архитектуры безопасности и повышению его объяснимости – способности «объяснить», почему система приняла то или иное решение. Ожидается также рост интереса к гибридным моделям, сочетающим ИИ с традиционными методами и экспертными системами. Кроме того, начнется активное развитие технологий защиты самих моделей машинного обучения от манипуляций и атак, направленных на подмену или искажение данных, на которых они обучаются.

Таким образом, искусственный интеллект в ближайшем будущем будет не только усиливать существующие системы, но и формировать новые подходы к безопасности, где превентивный характер защиты выйдет на первый план.

Искусственный интеллект уже сегодня занимает важное место в системе обеспечения сетевой безопасности. Он способен существенно повысить эффективность защиты, снизить риски и ускорить реагирование на инциденты. Однако для полной реализации его потенциала необходимо учитывать технические, этические и организационные аспекты. Только

гармоничное сочетание человеческого опыта и машинной точности позволит создать устойчивую и адаптивную систему кибербезопасности, готовую к вызовам цифровой эпохи.

Список использованных источников:

1. Buczak A.L., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 2016.

2. Sommer R., Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, 2010.

3. Garcia-Teodoro P., Diaz-Verdejo J., Maciá-Fernández G., Vázquez E. Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 2009.

4. Bhuyan M.H., Bhattacharyya D.K., Kalita J.K. Network anomaly detection: Methods, systems and tools. IEEE Communications Surveys & Tutorials, 2014.

5. Chio C., Freeman D. Machine Learning and Security: Protecting Systems with Data and Algorithms. O'Reilly Media, 2018.

6. Shabtai A., Elovici Y., Rokach L. A Survey of Data Leakage Detection and Prevention Solutions. Springer, 2012.

Alizoda S.S.
Belarusian State University of
Informatics and Radioelectronics, Minsk

Scientific supervisor:
Likhachevsky D.V.
Belarusian State University of
Informatics and Radioelectronics, Minsk

THE ROLE OF ARTIFICIAL INTELLIGENCE IN NETWORK SECURITY

Abstract. The use of artificial intelligence (AI) in network security enables efficient detection and prevention of attacks, as well as real-time threat analysis. AI helps automate protection processes and respond to incidents. The paper discusses AI methods like machine learning and big data analysis, as well as potential risks.

Keywords: AI, network security, artificial intelligence, machine learning, attack protection, anomalies, automation, threat forecasting, cybersecurity, network safety.

УДК 004.8

Ализода С.С.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

Научный руководитель:
Лихачевский Д.В.
Белорусский государственный университет
информатики и радиоэлектроники, Минск

ЭВОЛЮЦИЯ КИБЕРУГРОЗ: КАК МЕНЯЮТСЯ МЕТОДЫ АТАК НА КОМПЬЮТЕРНЫЕ СЕТИ

Аннотация. Эволюция киберугроз демонстрирует увеличение сложности и масштабности атак на компьютерные сети. С развитием технологий методы атак также изменяются: от простых вирусов до сложных фишинг-атак и постоянных угроз (*APT*). Работа рассматривает ключевые этапы этой эволюции, классификацию атак и прогнозы для будущего киберугроз.

Ключевые слова: эволюция, киберугрозы, методы атак, компьютерные сети, фишинг, нулевые уязвимости, *APT*, киберпреступность, защита, атаки, уязвимости.

Современный мир все глубже погружается в цифровую реальность, и компьютерные сети стали неотъемлемой частью функционирования не только бизнеса, но и государства, образования, здравоохранения и личной жизни миллионов людей. С увеличением степени цифровизации возрастает и значимость защиты этих сетей от киберугроз, которые за последние десятилетия претерпели колоссальные изменения [1]. От примитивных вирусов и червей прошлого, созданных зачастую ради эксперимента, кибератаки эволюционировали в мощный инструмент шпионажа, саботажа и цифрового вымогательства. В этой статье рассматриваются ключевые этапы трансформации методов атак на компьютерные сети, современные тенденции и наиболее перспективные направления в области защиты.

Кибератаки не всегда были столь сложными и разрушительными, как в наши дни. Их развитие происходило поэтапно, отражая уровень развития цифровых технологий и инфраструктуры. В самом начале основными угрозами были относительно простые вирусы, нередко создававшиеся энтузиастами без злого умысла [2]. Однако уже в начале 2000-х гг. фокус сместился в сторону получения материальной выгоды: появились вредоносные программы, способные красть банковские данные, удаленно управлять устройствами и устанавливать шпионское ПО.

Следующий значительный этап ознаменовался появлением целенаправленных атак, организуемых на основе предварительной разведки и оценки инфраструктуры жертвы. Эти атаки стали основой феномена *APT* (*Advanced Persistent Threat*), где злоумышленники действуют с особой скрытностью, иногда оставаясь в системе в течение месяцев или даже лет, медленно развивая свою атаку [3].

Сегодняшние киберугрозы представляют собой комплексные, многоступенчатые и трудно обнаруживаемые схемы вторжений, часто поддерживаемые на государственном уровне или организованными киберпреступными группами. В частности, заметно усилилось использование методов социальной инженерии [4], при которых злоумышленники манипулируют людьми, чтобы получить доступ к защищенной информации. Эти методы особенно опасны тем, что трудно поддаются техническому контролю и требуют высокого уровня осведомленности со стороны сотрудников организаций.

Все больше атак направлены не на конечного пользователя, а на инфраструктуру, поставщиков и цепочки программного обеспечения [5]. Это позволяет злоумышленникам обойти традиционные средства защиты и получить доступ сразу к множеству целевых систем. Большую угрозу представляют и облачные технологии: ошибки конфигурации, уязвимые *API* и недостаточная изоляция данных становятся уязвимыми точками входа.

В ответ на усложнение атак развиваются и защитные меры, принимающие все более интеллектуальный характер. Одним из наиболее действенных подходов стала архитектура *Zero Trust*, в основе которой лежит отказ от доверия к любым компонентам системы по умолчанию. Такая модель предполагает строгую проверку и верификацию каждого действия, каждого пользователя и каждой машины. Не менее важным элементом современной защиты является поведенческая аналитика, позволяющая не просто выявлять технические сбои, но и анализировать отклонения от нормального поведения пользователей. Это дает возможность обнаруживать внутренние и внешние угрозы на ранних стадиях, до нанесения серьезного ущерба.

Автоматизация реагирования на инциденты также играет ключевую роль в защите. Благодаря системам класса *SOAR* организации могут мгновенно принимать меры по изоляции и нейтрализации угроз без необходимости вмешательства человека. Однако ни одна технология не может быть эффективной без обученного персонала. Образовательные инициативы, направленные на повышение осведомленности сотрудников, становятся таким же важным компонентом киберзащиты, как и технические решения.

Вектор развития киберугроз в будущем, по мнению большинства экспертов, будет направлен в сторону еще более глубокой автоматизации атак, а также их интеграции с информационно-психологическим воздействием [6]. Применение искусственного интеллекта злоумышленниками

позволит проводить высокоточные атаки с учетом поведенческих моделей жертв. Одной из растущих угроз становится распространение синтетических медиа – фальсифицированных изображений, голосов и видеозаписей, которые могут использоваться для компрометации высокопоставленных лиц, шантажа или введения в заблуждение широкой аудитории.

Появление квантовых компьютеров в перспективе может радикально изменить правила игры, разрушив существующие криптографические стандарты. Это требует уже сейчас разработки новых алгоритмов защиты, способных противостоять вычислительным возможностям будущих машин. Также все чаще обсуждаются угрозы, связанные с автономными системами, роботизированными комплексами и цифровыми двойниками, которые при взломе могут стать неконтролируемыми.

Понимание эволюции киберугроз важно не только для специалистов в области информационной безопасности, но и для широкой общественности, поскольку цифровая безопасность – это зона ответственности всех участников цифрового общества. Надежная защита требует не просто технических решений, но и системного подхода к формированию культуры безопасности. Только сочетание технологической, организационной и образовательной составляющих может обеспечить устойчивость к современным и будущим киберугрозам. В условиях непрерывных изменений стратегий атак, единственной стабильной ценностью остается необходимость постоянного развития механизмов защиты.

Список использованных источников:

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.
2. Symantec. Internet Security Threat Report, 2023.
3. FireEye. Threat Intelligence Reports, 2022.
4. Mitnick K. The Art of Deception: Controlling the Human Element of Security. Wiley, 2011.
5. Verizon. Data Breach Investigations Report (DBIR), 2023.
6. Europol. Internet Organised Crime Threat Assessment (IOCTA), 2023.

Alizoda S.S.
Belarusian State University of
Informatics and Radioelectronics, Minsk

Scientific supervisor:
Likhachevsky D.V.
Belarusian State University of
Informatics and Radioelectronics, Minsk

EVOLUTION OF CYBER THREATS: HOW METHODS OF ATTACKING COMPUTER NETWORKS ARE CHANGING

Abstract. The evolution of cyber threats shows an increase in the complexity and scale of attacks on computer networks. As technology develops, attack methods have shifted from simple viruses to complex phishing attacks and advanced persistent threats (APT). The paper explores key stages of this evolution, attack classification, and forecasts for the future of cyber threats.

Keywords: evolution, cyber threats, attack methods, computer networks, phishing, zero-day vulnerabilities, APT, cybercrime, protection, attacks, vulnerabilities.

УДК 004

Ахмадиева Виола Ф., Ахмадиева Вилена Ф.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шафиков М.Р.
Уфимский университет науки и технологий, Уфа

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ АВТОМАТИЗИРОВАННОГО ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ КИБЕРАТАК НА МОБИЛЬНЫЕ УСТРОЙСТВА

Аннотация. Статья посвящена исследованию возможностей искусственного интеллекта (ИИ) в области автоматизированного обнаружения и предотвращения кибератак на мобильные устройства. В рамках исследования был разработан и протестирован прототип системы на основе машинного обучения, способной анализировать поведение приложений и сетевой трафик в реальном времени для выявления аномалий. Эксперимент включает создание модели ИИ, обученной на наборе данных, содержащем как легитимные, так и вредоносные активности, и последующее тестирование ее эффективности на реальных устройствах.

Ключевые слова: искусственный интеллект, машинное обучение, тестирование модели, сбор данных, анализ данных, Random Forest, F1-мера, мобильные устройства.

С развитием мобильных технологий и увеличением числа пользователей смартфонов и планшетов, мобильные устройства стали одной из главных целей для киберпреступников [1]. Зачастую традиционные методы защиты, то есть, системы обнаружения вторжений и антивирусные программы оказывается недостаточно действенными в борьбе с новыми и сложными угрозами. В этой статье исследуется возможность использования искусственного интеллекта для автоматизированного обнаружения и предотвращения кибератак на мобильные устройства [2]. Основная цель – разработать и протестировать прототип системы, способной анализировать поведение приложений и сетевой трафик в реальном времени.

Методология реализации данного исследования включает в себя: сбор и анализ данных, разработку модели машинного обучения, тестирование модели [3].

Для обучения модели использовался набор данных, содержащий примеры нормального и вредоносного сетевого трафика. Данные включали такие признаки, как количество пакетов, размер пакетов, IP-адреса, порты и метки (легитимный/вредоносный).

Для классификации легитимных и вредоносных активностей была выбрана модель Random Forest, которая хорошо справляется с задачами классификации и устойчива к переобучению.

Модель была протестирована на реальных устройствах с использованием симулятора атак. Для оценки эффективности использовались метрики точности, полноты и F1-меры.

Набор данных был создан на основе симуляции нормального и вредоносного трафика. Вредоносные активности включали фишинг, атаки на сетевой трафик и вредоносное ПО. Модель Random Forest была обучена на 80 % данных. Для улучшения качества модели использовались методы балансировки классов (SMOTE) и настройки гиперпараметров (GridSearchCV). Модель была протестирована на оставшихся 20 % данных. Результаты показали высокую точность (99 %) и низкий уровень ложных срабатываний.

В результате нашего исследования мы определили эффективность модели, сравнили ее с традиционными методами и выявили ограничения и пути улучшения работы нашей модели:

– эффективность модели: модель успешно обнаружила 98 % вредоносных активностей, включая новые типы атак, которые традиционные методы не смогли бы обнаружить;

– сравнение с традиционными методами: традиционные методы, такие как антивирусы, показали точность около 85 %, что значительно ниже, чем у модели на основе ИИ;

– ограничения и пути улучшения: основным ограничением модели является зависимость от качества данных. Для повышения точности требуется больше данных и использование более сложных алгоритмов, таких как нейронные сети.

Разработанная система может быть интегрирована в мобильные приложения для защиты пользователей от кибератак. Это особенно важно для приложений, работающих с конфиденциальными данными, таких как банковские приложения и мессенджеры.

Мы провели эксперимент по обнаружению вредоносного ПО на Android-устройствах с использованием модели машинного обучения. Работа нашей модели показала, что:

– ИИ демонстрирует высокую эффективность в обнаружении новых и сложных угроз, которые традиционные методы могут пропустить;

– автоматизированные системы на основе ИИ могут стать ключевым элементом будущих решений в области кибербезопасности;

– для повышения точности и снижения ложных срабатываний требуется дальнейшее обучение моделей на более разнообразных данных.

Использование искусственного интеллекта для автоматизированного обнаружения и предотвращения кибератак на мобильные устройства показало высокую эффективность. Разработанная модель на основе Random Forest успешно справляется с обнаружением новых и сложных угроз, что делает ее перспективным решением для повышения безопасности мобильных устройств. Этот подход позволяет не только изучить теоретические аспекты ИИ, но и получить практический опыт разработки и тестирования систем безопасности, что особенно важно для профессионального роста в области информационной безопасности.

В контексте ужесточения законодательства РФ в области обработки персональных данных, разработка таких систем становится особенно актуальной. Уголовная ответственность (ст. 272.1 УК РФ) за нарушения, связанные с незаконным использованием персональных данных, предусматривает наказания вплоть до лишения свободы на срок до 6 лет и штрафов до 1 млн рублей. Административная ответственность (ст. 13.11 КоАП РФ) включает штрафы для юридических лиц до 15 млн рублей за массовые утечки данных. Эти меры подчеркивают важность внедрения современных технологий, таких как ИИ, для предотвращения кибератак и обеспечения соответствия законодательным требованиям.

Разработанная система на основе ИИ может быть интегрирована в мобильные приложения, особенно для защиты конфиденциальных данных, что делает ее перспективным решением для повышения кибербезопасности и минимизации рисков, связанных с нарушениями законодательства.

Список использованных источников:

1. Худхейр Ауси Р.М., Заргарян Е.В., Заргарян Ю.А. Модели машинного обучения и глубокого обучения для электронной информа-

ционной безопасности в мобильных сетях // Известия ЮФУ. Технические науки. 2022. № 3 (227). URL: https://cyberleninka.ru/article/n/modeli-mashinnogo-obucheniya-i-glubokogo-obucheniya-dlya-elektronnoy-informatsionnoy-bezopasnosti-v-mobilnyh-setyah

2. Намиот Д.Е., Ильюшин Е.А., Чижов И.В. Искусственный интеллект и кибербезопасность // International Journal of Open Information Technologies. 2022. № 9. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-kiberbezopasnost

3. Галимнуров А.А. Применение машинного обучения для определения спреда доходности корпоративных облигаций / А.А. Галимнуров, А.С. Исмагилова // Информационные технологии интеллектуальной поддержки принятия решений (памяти проф. Н.И. Юсуповой) ITIDS'2024: Труды X Международной научной конференции. В 2 томах. Уфа, 12–14 ноября 2024 г. Уфа: Уфимский университет науки и технологий, 2024. С. 36–41.

Akhmadieva Viola F., Akhmadieva Vilena F.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shafikov M.R.
Ufa University of Science and Technology, Ufa

USING ARTIFICIAL INTELLIGENCE FOR AUTOMATED DETECTION AND PREVENTION OF CYBERATTACKS ON MOBILE DEVICES

Abstract. The article is devoted to the study of artificial intelligence (AI) capabilities in the field of automated detection and prevention of cyberattacks on mobile devices. As part of the research, a prototype machine learning-based system capable of analyzing application behavior and network traffic in real time to detect anomalies was developed and tested. The experiment involves building an AI model trained on a dataset containing both legitimate and malicious activity and then testing its effectiveness on real devices.

Keywords: artificial intelligence, machine learning, model testing, data collection, data analysis, Random Forest, F1-measure, mobile devices.

УДК 004

Ахмадиева Виола Ф., Ахмадиева Вилена Ф.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Байрушин Ф.Т.
Уфимский университет науки и технологий, Уфа

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ: АНАЛИЗ УГРОЗ И МЕТОДЫ ЗАЩИТЫ

Аннотация. В статье рассматриваются современные угрозы безопасности мобильных устройств, такие как вредоносное ПО, фишинг, утечки данных и атаки на операционные системы. Проведен анализ существующих методов защиты, включая антивирусы, двухфакторную аутентификацию и шифрование данных. Предложена новая концепция использования блокчейн-технологий для повышения безопасности мобильных устройств, которая обеспечивает децентрализованное хранение данных и защиту от несанкционированного доступа.

Ключевые слова: мобильные устройства, угрозы, фишинг, утечка данных, атака, аутентификация, антивирусное программное обеспечение, блокчейн-технологии, уязвимость, шифрование.

Мобильные устройства стали важной частью нашей повседневной жизни. Мы используем их для работы, общения, проведения финансовых операций и хранения личной информации. Однако их широкое распространение привлекает внимание киберпреступников. С увеличением популярности мобильных гаджетов, таких как смартфоны и планшеты, вопросы безопасности этих устройств становятся все более важными. В этой статье мы обсудим ключевые угрозы, связанные с использованием мобильных устройств, а также способы их защиты и предложим новые стратегии для повышения уровня безопасности, включая современные решения.

Проведя анализ угроз безопасности мобильных устройств, можно сделать вывод, что основными угрозами безопасности мобильных устройств являются:

− вредоносные программы (Malware): представляют собой одну из самых серьезных угроз для мобильных устройств. Они могут быть установлены через зараженные приложения, ссылки или даже при подключении к незащищенным Wi-Fi сетям. Они представляют собой вирусы, трояны, шпионские программы и другие виды вредоносного ПО, которые могут украсть данные или повредить устройство. Примерами таких программ могут служить: приложения, маскирующиеся под легитимные, но содержащие вредоносный код;

– фишинг и социальная инженерия: фишинг представляет собой способ обмана пользователей с целью получения их конфиденциальной информации, такой как пароли и номера кредитных карт. Этот процесс может происходить через электронные письма, текстовые сообщения или поддельные веб-сайты, которые выглядят как настоящие;

– уязвимости в операционных системах: мобильные операционные системы, например, Android и iOS, могут иметь недостатки, которые хакеры могут использовать для получения неразрешенного доступа к устройствам. Часто пользователи не обновляют свои устройства своевременно, что повышает вероятность использования этих уязвимостей.

Утрата или кража гаджета: физическая утрата или кража мобильного устройства может стать серьезной угрозой. Если устройство не защищено надлежащим образом, злоумышленник может получить доступ ко всем хранящимся на нем данным:

– утечки данных: представляют собой несогласованный доступ к конфиденциальной информации, хранящейся на мобильных устройствах или в облачных сервисах. В качестве примера можно привести взломы облачных сервисов. Злоумышленники применяют различные техники, такие как фишинг или атаки методом «грубой силы», чтобы получить доступ к учетным записям пользователей в облачных хранилищах;

– атаки на операционные системы: атаки на операционные системы мобильных устройств связаны с эксплуатацией уязвимостей в ОС для получения несанкционированного контроля над устройством. Такие атаки могут быть направлены на системные компоненты и на пользовательские приложения;

– небезопасные приложения: Небезопасные приложения – это программы, которые требуют слишком много разрешений или имеют уязвимости, что позволяет злоумышленникам получить доступ к личной информации пользователя.

Существующие методы защиты от вышеперечисленных угроз, такие как:

– антивирусное программное обеспечение. Применение антивирусного ПО – это один из ключевых способов защиты мобильных устройств от вредоносных программ. Регулярные обновления баз данных антивирусов помогают обнаруживать новые угрозы;

– двухфакторная аутентификация. Двухфакторная аутентификация (2FA) обеспечивает дополнительную защиту при входе в аккаунты. Даже если хакер узнает пароль, ему все равно понадобится второй элемент (например, код, отправленный по SMS), чтобы получить доступ;

– постоянные обновления. Обновление операционной системы и программного обеспечения способствует устранению известных уязвимостей. Пользователям следует понимать важность регулярного обновления своих устройств;

– шифрование данных. Шифрование информации на мобильных устройствах способствует сохранению конфиденциальных данных в случае утраты или кражи устройства. Большинство актуальных операционных систем имеют встроенные возможности для шифрования;

– применение VPN. Подключение к виртуальным частным сетям (VPN) при работе с общественными Wi-Fi сетями способствует защите информации от возможного перехвата со стороны злоумышленников.

Существующие методы не справляются с современными угрозами, потому что они работают изолированно и зависят от действий пользователя, данные методы защиты не адаптированы к новым технологиям (IoT, 5G). Можно сделать вывод, что для поддержания безопасности требуется интегрированная система с использованием ИИ, блокчейна и автоматического устранения уязвимостей.

Внедрение блокчейн-технологий в системы защиты мобильных устройств позволит создать децентрализованную, прозрачную и устойчивую к взлому инфраструктуру для управления данными, аутентификации и защиты от киберугроз. Блокчейн обеспечивает высокий уровень безопасности за счет своей неизменяемости, распределенности и использования криптографических методов.

Основные компоненты системы:

– децентрализованное хранение данных: данные не хранятся на централизованных серверах, исключая риск массовых утечек. Предлагается хранить пароли, ключи шифрования и другие конфиденциальные данные в распределенной сети блокчейн. Пользователь может получить доступ к своим данным только через приватный ключ, а для хакеров доступ будет затруднителен;

– устойчивость к взлому: блокчейн использует криптографические алгоритмы, которые делают данные практически невозможными для подделки. Если злоумышленник изменит данные в блокчейне, то потребуется изменение всех последующих блоков, что сделает атаку экономически невыгодной;

– прозрачность и аудит: операции записываются в блокчейн, что обеспечивает прозрачность и возможность аудита. Пользователь беспрепятственно отследит, кто и когда пытался получить доступ к его данным;

– защита от фишинга: блокчейн позволяет устанавливать подлинность сайтов и приложений через децентрализованные реестры. Пользователь сможет видеть подтверждение легитимности ресурса перед вводом данных;

– удобная и безопасная аутентификация: использование цифровых подписей и смарт-контрактов для аутентификации пользователя. Предлагается осуществлять вход в приложения без передачи паролей через интернет, вместо традиционных паролей использовать цифровую подпись, которая хранится в блокчейне, что исключит риск перехвата;

– контроль доступа: смарт-контракты управляют доступом к данным на основе предустановленных правил. Можно установить ограничение доступа к данным приложения в зависимости от местоположения устройства.

Внедрение блокчейн-технологий в системы защиты мобильных устройств предлагает инновационный подход к обеспечению безопасности данных. Децентрализованное хранение, прозрачность и удобная аутентификация делают блокчейн идеальным решением для защиты от современных киберугроз. Внедрение данной системы способно существенно улучшить безопасность мобильных устройств и гарантировать защиту пользовательских данных.

Защита мобильных устройств продолжает оставаться важной проблемой на фоне увеличения числа киберугроз. Обеспечение безопасности мобильных устройств представляет собой многогранную задачу, требующую усилий как от пользователей, так и от создателей программного обеспечения. Несмотря на имеющиеся риски, использование современных защитных методов и внедрение новых технологий способны существенно улучшить уровень безопасности мобильных устройств. Предложенная концепция использования блокчейн-технологий предлагает инновационный подход к защите данных, обеспечивая децентрализованное хранение, прозрачность и контроль доступа. Необходимо учитывать, что безопасность – это не конечная цель, а непрерывный процесс, который требует регулярного обновления знаний и инструментов.

Список использованных источников:

1. Кузьминых Е.С., Маслова М.А. Анализ основных мобильных угроз и способы защиты от вирусов // Научный результат. Информационные технологии. 2022. № 2. URL: https://cyberleninka.ru/article/n/analiz-osnovnyh-mobilnyh-ugroz-i-sposoby-zaschity-ot-virusov

2. Аннамухаммедова О., Атаев Я., Бегмырадов Д. Безопасность мобильных приложений: лучшие практики защиты личной информации // Вестник науки. 2024. № 10 (79). URL: https://cyberleninka.ru/ article/n/bezopasnost-mobilnyh-prilozheniy-luchshie-praktiki-zaschity-lichnoy-informatsii

Akhmadieva Viola F., Akhmadieva Vilena F.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Bayrushin F.T.
Ufa University of Science and Technology, Ufa

MOBILE DEVICE SECURITY: THREAT ANALYSIS AND PROTECTION TECHNIQUES

Abstract. This article discusses current security threats to mobile devices, such as malware, phishing, data breaches and attacks on operating systems. It analyzes existing protection methods, including antivirus, two-factor authentication and data encryption. A new concept of using blockchain technology to improve the security of mobile devices is proposed, which provides decentralized data storage and protection from unauthorized access.

Keywords: mobile devices, threats, phishing, data leakage, attack, authentication, anti-virus software, blockchain technology, vulnerability, encryption.

УДК 004

Ахмадуллин Р.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Байрушин Ф.Т.
Уфимский университет науки и технологий, Уфа

ИСПОЛЬЗОВАНИЕ НЕЙРОСЕТЕЙ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

Аннотация. В данной статье рассматривается применение нейросетевых технологий в сфере нейронных сетей для повышения уровня информационной безопасности предприятий. Выражается необходимость внедрения новых методов анализа сетевого трафика, выявления ошибок и угроз предприятию. Рассматриваются эффективность, достоинства и недостатки нейросетей для при внедрении нейросетей в организацию работы предприятия, даются примеры компаний внедривших нейросети в компании для повышения уровня безопасности.

Ключевые слова: безопасность, кибератака, защита, угроза, нейросеть.

Информационная безопасность является одним из важнейших аспектов деятельности любого современного предприятия, особенно в условиях

стремительного роста числа кибератак и иных угроз. Старые способы защиты без использования продвинутого искусственного интеллекта – антивирусы, которыек сожалению, уже не такие эффективные. Именно здесь на помощь приходят технологии искусственного интеллекта и нейросети, способные анализировать огромные объемы данных и выявлять потенциальные угрозы в режиме реального времени.

Нейросети являются хорошим механизмом для защиты предприятий и иных организаций. Преимущества нейросетевых технологий таковы:

1. Автоматизация. Внедрив в нейросеть способность распознавать и ликвидировать угрозы без постоянного присутствия человека позволит, таким образом, распределить трудовые ресурсы по другим направлениям. Это позволит компаниям грамотно реорганизовывать рабочий процесс, добиваясь большей эффективности, что в свою очередь двигает компанию вперед.

2. Адаптация защиты. Одна из крайне положительных способностей нейросетей – это самообучение. Благодаря самообучению, нейросеть может приспосабливаться на опыте защиты ПО к новым технологическим ухищрениям хакеров и их вирусам, способных выкрасть, испортить или исказить информацию поступающею из предприятия в предприятие и внутри предприятия. Это позволит сделать защиту гибкой без необходимости своевременно писать коды для защиты ПО, с этим справится машина самостоятельно, главное лишь следить, чтобы она это делала правильно.

3. BigData или масштабируемость. В условиях цифрового общества своевременная и правильно структурированная информация делается необходимостью. Развитие нейросетей дала возможность сделать нейросети более продвинутыми, внедрив в них технологию BigData, что позволило компаниям, обладающих огромным размером информационной структуры, быстро обрабатывать огромные потоки информации, позволяя принимать правильные и своевременные решения. Технология нейросетей имеет довольно большой спектр возможного применения в сфере защиты информации. Например, распознавание лиц. Нейросеть запоминает лица сотрудников производства, что позволяет защищать аппаратуру и иное имущество компании от чужаков.

4. Cafee – пространство для точного обучения, является опенсорсом. Выполняет упорядочивание картинок и иных изображений с использованием нейросетей.

5. Анализ поведения пользователей и сотрудников. Каждая компания желает сохранить свое существование на рынке. И чтобы сохранить себя на рынке она будет отслеживать поведение пользователей и сотрудников. Нейросети, участвуя в этом процессе, позволяют максимизировать полезность в данной сфере. Через голос и биометрию нейросеть может обнаружить чужака в компании, посланного для шпионажа, диверсии и прочих пакостей.

6. Мониторинг сетевого трафика. Мониторинг сетевого трафика является крайне важным процессом в отношении защиты информационной безопасности. Нейросети необходимо провести анализ информации, идущей через адаптеры WIFI роутеры и прочие способы передачи информации для обнаружения в ней вредоносной для компании информации.

7. Управление идентификацией и аутентификацией. Биометрия является сейчас довольно популярной технологией для защиты общественных мест. Например, аэропорта как место сосредоточения пассажиров. Вся биометрия (отпечатки пальцев, глаза, голос), которую можно проверить на отличительные свойства, используется для проведения и идентификации и аутентификации личности сугубо в защитных интересах. Но, несмотря на наличие бесспорных плюсов, нейросети обладает рядом недостатков и издержек.

Издержки и недостатки:

1. Отсутствие квалифицированных специалистов: для предприятий и, в особенности для России, насущна проблема нехватки программистов, способных обеспечивать качественную работу нейронных сетей. Проблема нехватки кадров не позволяет популяризовать использование нейросетей в России ровно до тех пор, пока не будет доступного количества специалистов.

2. Необходимость большого объема качественных данных и добросовестного ведения отчетности: для эффективной работы необходим большой набор данных, которые нейросеть сможет обрабатывать, и учится, совершенствуя свои навыки. Небольшие компании не смогут предоставить достаточного количества данных для качественного приспособления нейросети под специфику работу своей компании, что приведет к некачественной работе нейросети.

3. Высокая стоимость внедрения: малая доступность также обуславливается высокой стоимостью работы нейросети. На данный момент технология не является доступной и требует большого количества высококвалифицированных специалистов, что, следовательно, затребует большое количество финансов на оплату услуг таких специалистов. У небольших компаний таких денег нет и им приходится работать по-старому, или полагаться на специалистов качеством ниже.

4. Уязвимость самих нейросетей: несмотря на продвинутость технологии, де-факто дарующая бесконечно оптимистичные перспективы на данный момент нейросети не идеальны. Уязвимость заключается в качестве даваемых ему на обработку данных. Неправильная, то есть ошибочная информация, крайне вредоносна в перспективе для обучения нейросети, которая может делать неправильные выводы, что будет приводить к статистическим ошибкам и потерям компаний.

Разобрав все достоинства и недостатки, следует рассмотреть примеры использование нейросетей: авангардом использования нейросетей выступают передовые компании мира: Google, использующие машинное

обучение и нейронные сети для повышения безопасности, Microsoft в рамках Microsoft 365 и Azure используют машинное обучение для анализа поведенческих паттернов пользователей и обнаружения потенциально опасных действий и IBM использует нейронные сети и другие методы машинного обучения для защиты данных и документооборота.

Нейросети являются очень важной составляющей современной информационной безопасности. Их использование и внедрение во все большее количество предприятий является важной с точки зрения и практической, и теоретической. Технология расширяет возможности обеспечения информационной безопасности. Нейросети за годы существования были достаточно доработаны, чтобы повысить уровень защищенности архитектуры ПО и минимизировать риски вреда для ПО. Успех работы нейросети зависит от профессионализма сотрудников. Исследования в области нейросетей должны быть направлены на увеличение защищенности к внешним воздействиям, самостоятельности в сфере обучения и совершенствования BigData.

Список использованных источников:

1. Резник Д.В. Искусственные нейросети. Анализ возможностей использования в целях обеспечения информационной безопасности // The Scientific Heritage 2021. С. 50–51. URL: https://cyberleninka.ru/article/n/iskusstvennye-neyroseti-analiz-vozmozhnostey-ispolzovaniya-v-tselyah-obespecheniya-informatsionnoy-bezopasnosti.

2. Прохоров А.С. Применение нейронных сетей для обеспечения безопасности человека в жилых и промышленных помещениях // Символ науки. 2021. С. 25–29. URL: https://cyberleninka.ru/article/n/primenenie-neyronnyh-setey-dlya-obespecheniya-bezopasnosti-cheloveka-v-zhilyh-i-promyshlennyh-pomescheniyah.

3. Тихолаз Р.В. Обеспечение информационной безопасности документооборота с использованием нейронных сетей // Документ в современном обществе. 2024. С. 584–586. URL: https://elar.urfu.ru/bitstream/10995/140754/1/978-5-7996-3940-2_2024_135.pdf.

Akhmadullin R.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Bayrushin F.T.
Ufa University of Science and Technology, Ufa

USING NEURAL NETWORKS TO ENSURE INFORMATION SECURITY AT THE ENTERPRISE

Abstract. This article discusses the application of neural network technologies in the field of neural networks to enhance the information security of enterprises. It emphasizes the need to implement new methods for analyzing network traffic, detecting errors and threats within organizations. The effectiveness, advantages, and disadvantages of neural networks for enterprise integration are examined, along with examples of companies that have implemented neural networks to improve security levels.

Keywords: security, cyberattack, protection, threat, neural network.

УДК:004.056

Белов И.А.
Поволжский государственный университет телекоммуникаций и информатики, Самара

Научный руководитель:
Новикова Д.Д.
Поволжский государственный университет телекоммуникаций и информатики, Самара

ПОЛИТИКА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ, США, КИТАЕ И ЕС

Аннотация. Статья посвящена анализу политики в сфере информационной безопасности в России, США, Китайской Народной Республике и Европейском Союзе. В работе рассматриваются различные подходы этих стран к обеспечению кибербезопасности, а также выявляются как положительные, так и отрицательные аспекты их политик. В результате проведенного анализа сделан вывод о том, что эффективная стратегия в области информационной безопасности должна находить оптимальный баланс между обеспечением безопасности и развитием международного сотрудничества.

Ключевые слова: информационная безопасность, информационная политика, Интернет, киберпространство.

Одна из притч мудрого царя Соломона звучит так: «Благоразумный видит беду, и укрывается; а неопытные идут вперед, и наказываются». В век информационных технологий эта притча очень актуальна.

Современные угрозы в цифровом пространстве становятся сложными и разнообразными, что требует значительных усилий для поддержания кибербезопасности.

В разных странах мира их собственные стратегии создаются для формирования информационной безопасности [2]. Рассмотрим примеры такой политики в России, Китае, США и Европейском союзе.

Наша страна нацелена на формирование национальной цифровой среды, включая свои системы поиска, социальные сети и услуги обмена сообщениями. К 2021 г. введен в действие Закон «суверенного Интернета», содержащий положения создать национальную систему управления интернет-трафиками, регулируя ключевые информационные ресурсы. Указ Президента Российской Федерации от 1 мая 2022 г. № 250 определил список предметов квот и установил требования для их защиты. Недавний Указ 13 июня 2024 г. № 500 обновил ряд положений. Согласно новому правилу, в 2025 г. государственным структурам и предприятиям запрещено использовать инструменты защиты информации, разработанные компаниями из стран в состоянии недружелюбных связей. Федеральной службе безопасности в России теперь назначено право определять условия работы с центрами, включенными в систему защиты [1]. План стратегического развития для российской ИТ промышленности за период с 2024 по 2030 г. сконцентрирован на поддержание технологической независимости цифровой техники. Сформирован Национальный координационный центр компьютерных мероприятий (NKSKI). С 2019 г. «Цифровой диктант» организуется регулярно Российской Ассоциацией электронных коммуникаций (РАЭК). Данный диктант состоит из тестирований, которое разработано с учетом разных возрастных категорий: для детей (7–13 лет), подростков (14–17 лет), взрослых (18–59 лет). Онлайн-платформа «Цифровой гражданин», дейст-вующая с 2018 г., предлагает учебные ресурсы и проводит сертификацию сотрудников в государственных и торговых организациях. 30 ноября 2024 г. Президент Российской Федерации подписал законнодательные действия, направленные на привлечение как к административной, так и уголовной ответственности за нарушение Российского Законодательства по личным сведениям [6]. Федеральный закон № 420, который меняет Кодекс административных преступлений, был принят 3 ноября 2024 г. Федеральный закон № 421 от 30 ноября 2024 г. вводит специальный корпус Delicti в Уголовный кодекс Российской Федерации по контрактам на личную информацию, имеет силу с 11 декабря 2024 г. [5].

Среди компаний, сосредотачивающих свою деятельность на кибербезопасности, «Лаборатория Касперского», конечно, занимает лидирующие положения в России. Softline, московская компания,

находится на «ступеньке ниже» по объему выручки и предоставляет просторный спектр ИТ-сервисов, включая решения для киберзащиты. Вслед за ними идут такие компании, как BI.Zone Cybersecurity, GIS, Solar и Positron. С целью улучшения уровня защиты от киберугроз, я думаю, необходимо сотрудничество между СМИ, государственными органами и бизнесом. Минцифры разрабатывает платформу «ТелекомЦерт». Старт этой разработки намечен на конец 2026 г. [5].

Квантовые компьютеры, действительно, представляют собой потенциальную угрозу безопасности информации. В России ведутся экспериментальные разработки по внедрению постквантового шифрования, осуществляемые структурным подразделением «Российского квантового центра» [4].

Безопасность информации в США ориентирована, в первую очередь, на независимость всемирной сети и небольшое государственное вмешательство. Отражено это в законодательстве, включая CLOUD Act (2018). В 2019 г. был введен запрет на применение федеральных средств с целью закупки оборудования и услугу Huawei и ZTE. США заставляют союзников отказываться от оборудования в сетях 5G. Изданный Указ президента США № 14028 «Об усилении кибербезопасности страны» (2021) содержит 74 директивы, устанавливающие общие правила взаимодействия с кибератаками между федеральными агентствами и коммерческими организациями. Незащищенности в программном обеспечении Microsoft и Atlassian использовались, чтобы похитить сети. AWS занимает лидирующие положения в США и союзных государствах в плане сохранности и обработки секретной информации.

Китайская политика, в первую очередь, базируется на концепции и киберсуверенитета, подразумевающей надзор государства над глобальной сетью. Китай активно контролирует интернет, сдерживая иностранные ресурсы, и развивает свои компьютерные методики, такие как Baidu и WeChat, для уменьшения подчиненности от западных технологий. Вопреки всему, Китай не стремится к изоляции. Взгляды Российской Федерации и Китая на кибербезопасность в большинстве вопросов совпадают.

Европейский союз (ЕС) стремится к защите цифровых прав граждан, а также уменьшению влияния китайских технологий. Цифровой суверенитет в ЕС связан с защитой персональных данных, а отражено это в Общем регламенте по защите данных (GDPR), устанавливающем высокие стандарты защиты данных. ЕС также достигает совершенства своей цифровой инфраструктуры в рамках стратегии «Формирование цифрового будущего Европы», включая создание облачного хранилища Gaia-X. Главной частью системы кибербезопасности ЕС является Вторая директива о сетях и информационных системах (NIS2), обязывающая государства разрабатывать стратегии кибербезопасности.

Таблица 1

Преимущества и недостатки в деятельности политики ИБ

Страны	Преимущества	Недостатки
Россия	Независимость от западных технологий и устойчивость к атакам	Ограничение конкуренции
США	Собственное технологическое развитие и отстаивание национальных интересов	Высокая стоимость разработки и внедрения
Китай	Быстрое развитие собственных цифровых технологий и платформ	Высокие барьеры для выхода иностранных компаний на китайский рынок
ЕС	Высокий уровень защиты персональных данных граждан и мотивация усовершенствования европейской цифровой инфраструктуры	Немалая цена соблюдения GDPR для предпринима-тельства, а также ограничен-ность резервов и власти Европейского агентства по кибербезопасности

Таким образом, анализируя данные, пришли к следующим выводам:

1. Если ограничить системы телекоммуникаций стран, то при создании сетей будет иметь меньший результат по сравнению с обменом информации для усиления мер защиты.

2. Геополитическое соперничество имеет отношение и к гиперпространству.

3. Эффективная стратегия должна балансировать между безопасностью и сотрудничеством между странами.

Список использованных источников:

1. Указ Президента РФ от 13.06.2024 № 500 «О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"». URL: https://www.consultant.ru/law/hotdocs/85170.html.

2. Информационная безопасность. URL: https://ru.wikipedia.org/wiki.

3. На платформу становись. Минцифры поднимает отрасли на борьбу с киберугрозами. URL: https://www.kommersant.ru/doc/6905615, 21.08.2024.

4. НСПК и QApp реализовали пилот по защите данных на основе постквантовых алгоритмов шифрования. URL: https://safe.cnews.ru/news/line/2023-11-10_nspk_i_qapp_realizovali_pilot.

5. Степанова Г.А. Основные изменения в правовом обеспечении защиты информации, персональных данных и функционирования ИС в РФ в 2025 г. // Корпоративные информационные системы. 2024. № 4 (28). С. 1–9. URL: https://corpinfosys.ru/archive/2024/issue-28/259-2024-28-itlawschangesin2025.

6. Цифровой суверенитет как залог глобальной безопасности. URL: https://roscongress.org/materials/tsifrovoy-suverenitet-kak-zalog-globalnoy-bezopasnosti/.

Belov I.A.
Volga Region State University of
Telecommunications and Informatics, Samara

Scientific supervisor:
Novikova D.D.
Volga Region State University of
Telecommunications and Informatics, Samara

INFORMATION SECURITY POLICYIN RUSSIA, THE USA, CHINA A ND THE EU

Abstract. The article analyzes the policies in the field of information security in Russia, the United States, the People's Republic of China and the European Union. The work examines the various approaches of these countries to ensuring cybersecurity, and identifies both positive and negative aspects of their policies. As a result of the analysis, it is concluded that an effective strategy in the field of information security should find an optimal balance between ensuring security and developing international cooperation.

Keywords: information security, information policy, Internet, cyberspa.

УДК 004

Галяутдинов Р.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

СПОСОБЫ УПРАВЛЕНИЯ РИСКАМИ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. В статье раскрыты особенности управления рисками информационной безопасности с помощью искусственного интеллекта. Особое внимание уделяется проблемам защиты информации и мерам безопасности при использовании искусственного интеллекта в работе с информационными рисками.

Ключевые слова: информация, информационная безопасности, риски, риски информационной безопасности, искусственный интеллект.

Внедрение искусственного интеллекта (ИИ) становится все более распространенным явлением в разнообразных сферах в современных реалиях. Компании непрерывно ищут инновационные способы интеграции ИИ в свои бизнес-процессы, стремясь к оптимизации и повышению производительности благодаря возможностям искусственного интеллекта.

Развитие ИИ охватывает множество областей. В каждой из этих областей существуют различные подходы, которые можно использовать как по отдельности, так и в комбинации для управления рисками. Это направлено на увеличение эффективности работы и достижение ключевых целей компаний. В настоящее время использование алгоритмов искусственного интеллекта с целью оценки вероятности наступления рисков получило широкое распространение в ряде областей:

– финансовый сектор: анализ финансовых операций для обнаружения признаков мошенничества и определения уровня риска для страховых компаний;

– здравоохранение: прогнозирование возможности наступления риска появления или усиления характера заболеваний, снижение нагрузки на систему здравоохранения;

– государственный сектор: анализ рисков государственных контрактов, предназначенный для улучшения результативности госзакупок и рационализации использования бюджетных средств;

– обеспечение информационной безопасности (ИБ): система управления рисками информационной безопасности направлена на обеспечение защиты информации организации, предотвращение финансовых потерь из-за инцидентов и поддержание прибыльности.

Традиционные подходы к управлению информационными рисками зачастую оказываются неэффективными в условиях динамичного развития информационных технологий. Возможности искусственного интеллекта по оперативной обработке больших массивов информации, выявлению взаимосвязей и прогнозированию потенциальных рисков делают его ключевым инструментом для современного бизнеса. Искусственный интеллект предлагает организациям средства для анализа рисков ИБ в режиме реального времени, автоматизации процессов принятия. Рассматривая применение ИИ при управлении рисками, потенциал особенно заметен в следующих областях: прогнозирование рисков путем анализа предыдущих периодов и выявления новых вероятных угроз ИБ, анализе рисков с помощью продвинутой аналитики, снижении рисков путем оптимизации ресурсов и превентивных мер защиты информации [1, с. 12–13].

Наиболее распространенными методами управления рисками информационной безопасностью с помощью искусственного интеллекта являются: искусственные нейронные сети, машинное обучение и глубокое обучение, обработка естественного языка.

Стоит отметить, что технологии обработки естественного языка (NLP) позволяют анализировать масштабные текстовые массивы, включая

публикации в соцсетях, статьи новостей и отзывы потребителей. Цель анализа – выявление признаков мошенничества на основе определенных ключевых слов, например, связанных с безопасностью крупного банка. В корпоративной среде для обнаружения мошеннических действий применяются программные решения, основанные на искусственном интеллекте, такие как Caseware, Feedzai и SAS [2, с. 44].

Реализация ИИ в управлении рисками и обнаружении мошенничества предоставляет организациям мощные инструменты для повышения безопасности и защиты активов. Однако, успешное внедрение требует комплексного подхода, учитывающего не только технические аспекты, но и вопросы этики, конфиденциальности и экономической целесообразности. Технологии ИИ применяются в нескольких областях управления рисками, например:

1. Выявление потенциальных рисков: ИИ применятся для изучения значительных объемов данных, чтобы находить отклонения, указывающие на вероятные риски.

2. Прогнозное моделирование: ИИ применяется построения для аналитических моделей, способных предвидеть возможность наступления тех или иных рисковых событий в перспективе.

3. Оценка рисков: ИИ помогает оценивать возможные последствия рисков и разрабатывать стратегии по их смягчению.

4. Выявление мошеннических схем: В сфере финансов ИИ идентифицирует махинации, анализируя структуру финансовых транзакций и выделяя нестандартные или вызывающие сомнения действия.

5. Автоматизация риск-комплаенса: ИИ автоматизирует процессы соответствия законодательным требованиям и профессиональным стандартам, таким образом, уменьшая риски, связанные с несоблюдением [3, с. 46].

Стоит отметить, что на рынке есть уже готовые решения для управления и анализа рисков для бизнеса с применением искусственного интеллекта:

– RiskVision от SAP: предлагает инструменты предиктивной аналитики и интеллектуального мониторинга бизнес-процессов, помогающие выявлять потенциальные угрозы;

– Oracle Risk Management Cloud: интегрированная платформа для комплексного управления корпоративными рисками с поддержкой машинного обучения;

– Qlik Risk Analytics: платформа визуализации и анализа больших объемов данных, позволяющая эффективно анализировать риски с помощью аналитического инструментария на основе AI.

В целом, внедрение ИИ в управление рисками приводит к повышению эффективности, снижению затрат и улучшению принятия решений. Однако важно помнить, что ИИ не является панацеей. Для успешного применения ИИ необходимо наличие качественных данных, опытных специалистов и четко определенных целей. Кроме того, важно учитывать

этические аспекты использования ИИ, чтобы избежать предвзятости и обеспечить прозрачность алгоритмов. Не следует забывать и о расходах на развертывание AI-решений, которые, учитывая современный дефицит и высокую цену опытных специалистов в сфере информационных технологий, могут оказаться чрезвычайно большими [4, с. 88].

Искусственный интеллект (ИИ) предоставляет компаниям множество способов для управления рисками. Он помогает быстро находить возможные проблемы, оценивать их серьезность и разрабатывать планы по смягчению последствий. Использование ИИ позволяет уменьшить непредсказуемость и сделать бизнес более устойчивым к внешним воздействиям. Чем больше компания использует современные технологии, тем лучше она сможет контролировать риски и достигать своих целей.

Список использованных источников:

1. Бессмертный И.А. Искусственный интеллект: учебное пособие / И.А. Бессмертный. СПб.: НИУ ИТМО, 2010. 132 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/43663 (дата обращения: 16.04.2025).

2. Бондаренко И.С. Информационная безопасность: учебник / И.С. Бондаренко. М.: МИСИС, 2023. 254 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/360344 (дата обращения: 13.04.2025).

3. Жданов А.А. Автономный искусственный интеллект: учебное пособие / А.А. Жданов. 5-е изд. (эл.). М.: Лаборатория знаний, 2024. 362 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/387629 (дата обращения: 16.04.2025).

4. Кацов И. Искусственный интеллект на предприятии: руководство / И. Кацов; перевод с англ. В. С. Яценкова. М.: ДМК Пресс, 2024. 710 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/456725 (дата обращения: 16.04.2025).

Galyautdinov R.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

RISK MANAGEMENT CAPABILITIES WITH ARTIFICIAL INTELLIGENCE

Abstract. The article reveals the features of information security risk management using artificial intelligence. Special attention is paid to the

problems of information protection and security measures when using artificial intelligence in dealing with information risks.

Keywords: information protection rights, information security, risks, information security risks, artificial intelligence.

УДК 004

Давлетшин Б.М.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Салов И.В.
Уфимский университет науки и технологий, Уфа

МЕТОД НУЛЕВОГО ДОВЕРИЯ (ZERO TRUST) МЕЖДУ ЛЮДЬМИ КАК ОТВЕТНАЯ МЕРА НА РАСПРОСТРАНЕНИЕ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Аннотация. В статье рассматривается применение концепции Zero Trust и перенос принципов кибербезопасности на уровень межличностного общения в контексте голосовых коммуникаций.

Ключевые слова: нулевое доверие, телефонное мошенничество, социальная инженерия, поведенческая аутентификация, цифровая безопасность.

Современные цифровые технологии, с одной стороны, упрощают повседневную коммуникацию и обеспечивают удобство взаимодействия, а с другой – создают широкие возможности для злоумышленников. В последние годы наблюдается рост количества телефонных мошенничеств, особенно с использованием подмены номеров, социальных манипуляций и технологий искусственного интеллекта (ИИ), таких как генерация голоса.

Традиционные средства защиты, основанные на доверии к идентификатору звонящего, становятся недостаточными. В этих условиях возрастает потребность в применении более строгих и универсальных моделей безопасности. Одной из таких моделей является концепция Zero Trust Security (модель нулевого доверия), которая предполагает отсутствие автоматического доверия к любому субъекту взаимодействия без предварительной проверки его подлинности [1].

Актуальность исследования обусловлена необходимостью адаптации принципов Zero Trust к голосовой коммуникации, как в личной, так и в деловой среде. В условиях постоянного роста количества и сложности мошеннических схем важно сформировать устойчивые поведенческие паттерны защиты от угроз [2].

Метод Zero Trust был изначально разработан для защиты цифровой инфраструктуры и ИТ-систем, где каждый пользователь и устройство проходят обязательную аутентификацию и проверку доступа. Однако его применение к сфере голосовых коммуникаций между людьми ранее не рассматривалось системно. Новизна заключается в переносе принципов цифровой безопасности на уровень обычной телефонной беседы.

Ключевые аспекты новизны [3]:

– формирование концепции «не доверяй – проверяй» в бытовом телефонном общении;

– внедрение поведенческой и голосовой аутентификации при голосовых вызовах;

– объединение технологических инструментов (антиспам-фильтров, распознавания речи) с социально-психологическими механизмами (обучение, кодовые слова, критическое мышление);

– учет возможности фальсификации голоса с помощью ИИ как нового фактора риска.

Данная адаптация делает подход Zero Trust универсальным инструментом противодействия мошенничеству как в цифровой, так и в человеческой плоскости коммуникаций.

Актуальные угрозы телефонных коммуникаций можно классифицировать по нескольким направлениям:

1. Подмена номера (Caller ID Spoofing): Используя технологии VoIP и специальное программное обеспечение, мошенники могут звонить с номеров, визуально совпадающих с номерами банков, госучреждений, родственников или коллег. Это создает иллюзию легитимности и повышает вероятность доверия со стороны жертвы.

2. Голосовые подделки (Deepfake Voice): Развитие ИИ позволило создавать фальсификации голосов, практически неотличимые от оригинальных. Это используется для атак в бизнес-среде (например, фальшивый звонок от «директора» с просьбой перевести деньги) или в частной жизни (имитация голоса ребенка с просьбой о помощи).

3. Социальная инженерия: Используется для создания чувства срочности, паники, доверия или страха. Примеры включают звонки от «службы безопасности банка», «следователя», «медработника» или «внука» с мольбами о срочной помощи. Часто используется сценарий, в котором жертва должна действовать немедленно, не раздумывая.

4. Фишинг по телефону (Vishing): Выманивание паролей, одноразовых кодов и других данных. Отличие от традиционного фишинга заключается в том, что атака происходит в реальном времени и часто подкреплена манипулятивной речью и подменой номера.

5. Технические уязвимости: Использование уязвимостей в системах VoIP, недостаточной защиты приложений, отсутствие защиты SIM-карт и уязвимости в прошивке телефонов также могут использоваться злоумышленниками для компрометации связи.

Для применения модели нулевого доверия в голосовых коммуникациях необходимо формировать устойчивые принципы взаимодействия, основанные на проверке, а не на доверии. Предлагаются следующие рекомендации:

1. Недоверие к внешним признакам достоверности: Не следует полагаться на номер, отображаемый на экране телефона, голос собеседника или даже содержание разговора. Всегда необходима проверка источника информации.
2. Использование вторичных каналов проверки: При сомнениях следует завершить разговор и связаться с предполагаемым собеседником через альтернативный канал связи – мессенджер, электронную почту, личную встречу.
3. Введение кодовых слов: В кругу семьи или в организации можно договориться об использовании заранее определенных кодовых фраз для верификации личности. Такие слова не должны быть очевидными и должны периодически меняться.
4. Анализ поведенческих признаков: Несвойственный стиль общения, агрессия, попытки вызвать панику, навязывание решений – все это признаки мошеннической атаки. Zero Trust требует внимательного наблюдения за такими проявлениями.
5. Отказ от передачи конфиденциальных данных: Под предлогом безопасности мошенники часто просят предоставить код из SMS, номер карты или CVV. Согласно Zero Trust, никакие данные не должны передаваться по инициативе звонящего.
6. Технологическая защита: Использование приложений для идентификации звонков (например, Truecaller), блокировка неизвестных и скрытых номеров, фильтрация звонков по ключевым признакам.
7. Обучение и профилактика: Регулярное проведение обучающих мероприятий и тренингов, создание корпоративных стандартов коммуникации, разработка внутренних инструкций по верификации личности при звонках.

Рассмотрим ряд реальных кейсов, подтверждающих необходимость внедрения Zero Trust:

– случай в Германии (2024): Мошенники, подделав голос дочери пенсионерки, сообщили о ДТП и необходимости срочного перевода крупной суммы. Женщина спаслась от потери средств только благодаря привычке перезванивать близким и задавать уточняющие вопросы;

– инцидент в Великобритании (2023): Руководитель компании получил звонок от «директора» с просьбой о переводе средств. Грамотная проверка голоса и дополнительное подтверждение по электронной почте позволили предотвратить финансовые потери;

– финансовый сектор России (2022): Один из банков внедрил голосовую биометрию при входящих звонках от клиентов. Это позволило за год сократить количество успешных мошеннических звонков на 38 %.

Модель Zero Trust, адаптированная к телефонной коммуникации, предоставляет мощный инструмент противодействия современным угрозам. Переход от доверия к проверке позволяет минимизировать влияние манипулятивных и технически сложных атак.

Комплексный подход, включающий технологические средства, поведенческие практики и образовательные меры, делает метод нулевого доверия универсальным и масштабируемым [4]. Применение этого подхода способствует формированию цифровой гигиены общения и защите интересов граждан, организаций и общества в целом.

Перспективы дальнейших исследований включают разработку автоматизированных систем голосовой аутентификации, интеграцию Zero Trust в государственные стандарты связи, а также расширение практики обучения в образовательных учреждениях и организациях.

Список использованных источников:

1. Zero Trust Maturity Model. U.S. Department of Homeland Security. // CISA. URL: https://www.cisa.gov/zero-trust-maturity-model.

2. Как избежать атаки с использованием социальной инженерии // Kaspersky Lab. URL: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks.

3. Нейросети: как мошенники используют ИИ для обмана // Коммерсант. URL: https://www.kommersant.ru/ /doc/6616414.

4. Многоагентные системы как технологическая база реализации концепции нулевого доверия / С.С. Валеев, Н.В. Кондратьева, М.Б. Гузаиров, А.С. Исмагилова // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2024. № 3. С. 116–123. DOI 10.18137/RNU.V9187.24.03.P.116.

Davletshin B.M.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Salov I.V.
Ufa University of Science and Technology, Ufa

THE ZERO TRUST METHOD BETWEEN PEOPLE AS A RESPONSE TO THE SPREAD OF ARTIFICIAL INTELLIGENCE FOR TELEPHONE FRAUD

Abstract. The article examines the application of the Zero Trust Security concept and the transfer of cybersecurity principles to the level of interpersonal communication in the context of voice communications.

Keywords: zero trust, phone fraud, social engineering, behavioral authentication, digital security.

УДК 004

Дмитриева М.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Миронова Н.Г.
Уфимский университет науки и технологий, Уфа

ЭВОЛЮЦИЯ КИБЕРАТАК НА КРИТИЧЕСКУЮ ИНФРАСТРУКТУРУ

Аннотация. В статье рассматривается эволюция кибератак на критическую информационную инфраструктуру, а также актуальные угрозы и уязвимости информационной безопасности. Особое внимание уделено способам и средствам защиты от кибератак на объекты критической инфраструктуры в связи с инновациями в кибербезопасности.

Ключевые слова: нформационная безопасность, защита информации, кибератака, критическая инфраструктура, кибербезопасность.

В современных реалиях кибератаки на критическую информационную инфраструктуру (КИИ) происходят все чаще и при этом приводят к более разрушительным последствиям. Они представляют угрозу для энергетики, транспорта, здравоохранения, а также для финансового сектора. Для оптимальной защиты КИИ только технологических решений недостаточно, чтобы отразить атаки злоумышленников на критически важную инфраструктуру. Необходим всесторонний инновационный подход, включающий в себя не только современные инструменты, но и квалифицированный персонал, оптимизированные процессы и передовые стратегии развития.

До 2010 г. кибератаки на КИИ носили в основном экспериментальный характер и редко приводили к масштабным последствиям. Примером является атака вируса Stuxnet в 2010 г., направленная на иранские ядерные объекты, что продемонстрировало возможность использования цифровых атак для разрушения физических объектов.

В период с 2010 по 2020 г. наблюдался рост атак на промышленные и энергетические системы. Среди важных инцидентов можно выделить следующие:

– 2015 г. – атака BlackEnergy на энергосистему Украины, вызвавшая массовые отключения электричества;

– 2017 г. – атака вируса NotPetya, поразившего финансовые и государственные системы Украины, а затем распространившегося по всему миру;

– 2020 г. – взлом SolarWinds, затронувший правительственные и корпоративные сети США.

В последние годы кибератаки используются наравне с традиционными военными, экономическими и информационными методами ведения конфликтов. Это значит, что государства и злоумышленники активно применяют цифровые атаки для достижения стратегических политических и экономических целей. По данным компании KnowBe4, специализирующейся на кибербезопасности, во всем мире количество таких атак увеличилось на 30 % с 2022 г., достигнув более 420 млн атак в период с января 2023 по 2024 г., что эквивалентно 13 атакам в секунду. Крупнейшими инцидентами стали:

– 2022–2024 гг. – рост атак на транспортные системы и аэропорты (кибератака на лондонский Heathrow в 2023 г.);

– 2024 г. – США и союзные страны обвинили Россию в использовании вредоносного ПО WhisperGate для атак на Украину и НАТО.

В январе 2025 г. эксперты «Лаборатории Касперского» сообщили о росте количества целевых кибератак на промышленные предприятия в России. Так, по сравнению с предыдущим годом количество атак выросло в 2,5 раза и составило порядка 130 000 инцидентов, из которых критичными стали порядка 25 000. Чаще всего вредоносные объекты проникают на компьютеры автоматизированных систем управления из интернета. Доля утечек из серверов баз данных в общем числе составила 68 %. Кроме того, к кибератакам на объекты КИИ подключились различные группы хактивистов, начав активно атаковать компании, относящиеся к важным секторам экономики с позиции обеспечения национальной безопасности. Причиной стало недостаточное внимание разработчиков, администраторов и архитекторов баз к безопасности, наличие уязвимостей в используемых продуктах и решениях, а также неправильная конфигурация.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций уделяет приоритетное внимание укреплению защиты от киберугроз на территории России. В соответствии со своими функциями, в 2024 г. Роскомнадзор заблокировал доступ к 7724 мошенническим веб-страницам и прекратил деятельность 62 сайтов, занимавшихся распространением вредоносного софта. Все эти действия направлены на обеспечение безопасности КИИ от киберпреступлений, которые приобретают все более сложный и угрожающий характер. Принимаемые меры позволяют снизить риски и предотвратить возможный ущерб от действий злоумышленников в цифровой среде, поскольку успешная атака может привести к безвозвратной утрате данных и неприемлемым последствиям, таким как падение производственной эффективности. В свою очередь, злоумышленники также применяют ИИ для создания вредоносных инструментов и улучшения техник атак с использованием социальной инженерии.

Стоит отметить, в последнее время промышленные организации для увеличения продуктивности, активно внедряют передовые технологии:

искусственный интеллект (ИИ), машинное обучение, дополненную реальность и другие. Внедрение ИИ для улучшения управления производственными процессами уже демонстрирует значительные выгоды в различных отраслях: автоматизированное управление уменьшает риски поломок и остановок в работе, повышая тем самым производительность устройств. В связи с этим, подобные системы стремительно превращаются в критически важные производственные ресурсы, однако их применение также влечет за собой новые риски в области кибербезопасности. Неправильное использование искусственного интеллекта может спровоцировать случайную утечку информации и другие угрозы, многие из которых сложно предвидеть.

В связи с политикой импортозамещения в РФ, для субъектов критической информационной инфраструктуры (КИИ) приоритетным является использование отечественных средств защиты. В частности, для предотвращения несанкционированного доступа (НСД) рекомендуется применять разработки компаний «Код Безопасности», «Инфотекс» и «Конфидент». Для управления информационной безопасностью, оперативного реагирования на инциденты (SIEM) и контроля технологического трафика (INAD) эффективны решения от «Positive Technologies» и «Лаборатории Касперского». Защиту каналов связи (NGFW/VPN) целесообразно обеспечивать продуктами «UserGate», «Кода Безопасности», «Инфотекс», «КриптоПро» и «С-терра». В сфере промышленных межсетевых экранов, востребованными для защиты КИИ являются решения «UserGate» и «Инфотекс», а для управления уязвимостями – продукты «Positive Technologies» и «Алтэкс-Софт».

Надежная защита данных, безопасность ИТ-инфраструктуры, в том числе объектов КИИ, сохранение штатного функционирования бизнес-процессов и соблюдение требований законодательства – обязательные условия устойчивого развития современного бизнеса. Отечественные разработчики представляют для субъектов КИИ готовые решения, которые позволяют создать комплексную систему защиты, позволяющую обеспечить требуемый уровень информационной безопасности.

Список использованных источников:

1. Егорова А.О. Обеспечение безопасности критической информационной инфраструктуры: учебное пособие / сост. А.О. Егорова [и др.]. Севастополь: СевГУ, 2024. 110 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/450542 (дата обращения: 06.04.2025). URL: для авториз. пользователей.

2. Корниенко А.А. Система требований к обеспечению безопасности автоматизированных систем и значимых объектов критической информационной инфраструктуры: учебное пособие / А.А. Корниенко, В.С., А.П. Глухов. Санкт-Петербург: ПГУПС, 2022. 63 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/

book/329477 (дата обращения: 06.04.2025). URL: для авториз. пользователей.

3. Середкин С. П. Особенности кибератак на объекты критической информационной инфраструктуры в современных условиях // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. 2022. № 4 (16). С. 56–66.

4. Лаборатория Касперского, «Лаборатория Касперского» представила прогноз развития сложных кибератак в 2025 г. // kaspersky.ru. URL: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-predstavila-prognoz-razvitiya-slozhnyh-kiberatak-v-2025-godu.

Dmitrieva M.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Mironova N.G.
Ufa University of Science and Technology, Ufa

THE EVOLUTION OF CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

Abstract. The article examines the evolution of cyberattacks on critical information infrastructure, as well as current threats and vulnerabilities to information security. Special attention is paid to ways and means of protection against cyberattacks on critical infrastructure facilities in connection with innovations in cybersecurity.

Keywords: information security, information security, cyberattack, critical infrastructure, cybersecurity.

УДК 004

Драганова Д.В.
Санкт-Петербургский государственный
университет, Санкт-Петербург

Научный руководитель:
Дунаева Ю.Г.
Санкт-Петербургский государственный
университет, Санкт-Петербург

СТРАТЕГИЯ ЕВРОСОЮЗА В ОБЛАСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: СКООРДИНИРОВАННЫЙ ПЛАН И НАЦИОНАЛЬНЫЕ ПОДХОДЫ

Аннотация. В условиях стремительного развития технологий искусственного интеллекта (ИИ) формируется новое информационное пространство, в котором государства стремятся укрепить свои позиции посредством разработки стратегий технологического прогресса. Особое внимание уделяется стратегиям Европейского Союза, включая скоординированный план, национальные подходы Великобритании, Германии и Франции, а также правовые рамки, регулирующие ИИ. Рассматриваются Закон об ИИ, инвестиционные программы, этические инициативы и вызовы, связанные с глобальной конкуренцией.

Ключевые слова: искусственный интеллект, Европейский Союз, Закон об ИИ, скоординированный план, национальные стратегии, этика ИИ, Horizon Europe, InvestAI, Великобритания, Франция.

Развитие технологий искусственного интеллекта (ИИ) представляет собой один из ключевых факторов трансформации современного информационного пространства. Это обуславливает тот факт, что Европейский Союз (ЕС) стремится занять лидирующие позиции в этой области, разрабатывая комплексные стратегии, которые сочетают регулирование, инвестиции и инновации. Настоящая статья посвящена анализу скоординированного плана ЕС по развитию и внедрению технологий ИИ, национальных стратегий Великобритании, Германии и Франции, а также правовых и этических аспектов регулирования ИИ. Особое внимание уделяется Закону об искусственном интеллекте (AI Act), инвестиционным программам и вызовам, связанным с конкуренцией на глобальном уровне. Методология анализа включает сравнительный подход к нормативным актам и национальным стратегиям, качественную оценку экспертных мнений и количественный анализ данных по финансированию.

Исторический контекст развития дискурса по вопросу развития искусственного интеллекта в Европе уходит корнями в середину XX в., когда в 1956 г. на Дартмутской конференции был предложен термин

«искусственный интеллект». В Европе интерес к ИИ начал активно формироваться в 1970-х гг. с развитием экспертных систем и автоматизации. В 1980-х гг. европейские исследователи, такие как Алан Банди, внесли вклад в теоретические основы ИИ, включая внедрение таких понятий, как логические системы и машинное обучение. В свою очередь, создание Европейской ассоциации по искусственному интеллекту (EurAI) в 1982 г. и проведение первой Европейской конференции по ИИ (ECAI) заложили фундамент для междисциплинарных исследований. Однако до 2010-х гг. практическое внедрение ИИ в Европе оставалось ограниченным из-за недостаточного финансирования и фрагментации усилий, что контрастировало с прагматичным подходом США [1].

На данный момент тем не менее европейский регион занимает сильную позицию в общей технологической гонке. Современные европейские исследования ИИ сосредоточенные в ведущих центрах, таких как Немецкий исследовательский центр искусственного интеллекта (DFKI) и Французский национальный институт исследований в области цифровых наук (Inria), составляют значительную конкуренцию своим коллегам из других частей света. При этом основные направления включают разработку алгоритмов машинного обучения, исследования в области этики ИИ, кибербезопасности и интеграции квантовых технологий. Европейская сеть центров передового опыта в области ИИ, поддерживаемая программой Horizon Europe, способствует обмену знаниями и координации исследований [2].

Ключевым элементом стратегии ЕС является Закон об искусственном интеллекте, принятый 13 марта 2024 г. и вступивший в силу 1 августа 2024 г. AI Act представляет собой первый в мире всеобъемлющий нормативный акт, регулирующий ИИ на основе риск-ориентированного подхода. Системы ИИ классифицируются по четырем уровням риска: неприемлемый, высокий, ограниченный и минимальный. Системы с неприемлемым риском, такие как технологии социального рейтинга или биометрической идентификации в реальном времени, запрещены. Системы высокого риска, используемые в здравоохранении или правоохранительной деятельности, подлежат строгим требованиям, включая управление рисками и прозрачность. Закон основывается на принципах уважения основных прав, безопасности, прозрачности и ответственности, что соответствует ценностям ЕС [3].

Для обеспечения соблюдения AI Act созданы национальные надзорные органы и Европейский совет по искусственному интеллекту. Нарушение закона влечет штрафы до 6 % годового оборота компании или 30 млн евро. Крупные технологические компании, такие как Microsoft, поддержали AI Act, однако критики отмечают сложность классификации систем и потенциальные трудности гармонизации регулирования в 27 странах ЕС [4]. Успех AI Act будет зависеть от эффективной координации и независимости надзорных органов.

Скоординированный план ЕС по ИИ, обновленный в 2021 г., направлен на достижение глобального лидерства в этичном и конкурентоспособном ИИ. Программа Horizon Europe (93,5 млрд евро на 2021–2027 гг.) выделяет более 1 млрд евро на ИИ-проекты в 2023–2024 гг. Инициатива InvestAI (200 млрд евро) поддерживает развитие ИИ-инфраструктуры и стартапов. Программа EuroHPC обеспечивает создание суперкомпьютеров, таких как LUMI и Leonardo, для исследований ИИ. Инвестиции в языковые модели с открытым исходным кодом и образовательные программы, включая Erasmus+, способствуют подготовке кадров [5].

Национальные стратегии европейских государств дополняют общий подход ЕС. Великобритания, после Brexit, разработала Национальную стратегию ИИ (2021), инвестируя 1 млрд фунтов через Innovate UK и UKRI. Создание AI Standards Hub и поддержка стартапов через Alan Turing Institute укрепляют позиции страны в этичном ИИ. Германия, модернизировавшая стратегию ИИ в 2020 г., выделила 5 млрд евро до 2025 г., развивая DFKI и AI Startup Hub. Франция, в рамках стратегии «Франция-2030», инвестирует 109 млрд евро в ИИ, поддерживая компании, такие как Mistral, и создавая ИИ-кластер в Эссоне [6].

Несмотря на амбиции, ЕС сталкивается с серьезными вызовами. Финансирование ИИ в Европе уступает США и Китаю. Фрагментация подходов между странами ЕС затрудняет координацию. Нехватка кадров, например, дефицит 50 000 специалистов в Германии, ограничивает потенциал технологического развития всего региона. Строгие нормы AI Act могут замедлить инновации, а протестные движения, такие как Stop Killer Robots, подчеркивают риски автоматизации и нарушения прав [7].

В заключение, стоит отметить, что в целом политика ЕС демонстрирует комплексный подход к развитию ИИ, сочетая передовое регулирование, инвестиции и национальные стратегии. Однако для укрепления позиций в глобальной экосистеме необходимо увеличение финансирования, а также упрощение регулирования, развитие кадров и гармонизация стандартов. При этом отдельным приоритетом стоит выделить укрепление международного сотрудничества, в частности, с глобальными лидерами позволит установить диалог и обмен технологиями, обеспечивая устойчивое развитие ИИ в Европе.

Список использованных источников:

1. Artificial Intelligence: A European Perspective. Joint Research Centre, European Commission, 2018.

2. Coordinated Plan on Artificial Intelligence. URL: https://digital-strategy.ec.europa.eu/en/policies/plan-ai.

3. REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1689.

4. The New EU AI Act: The 10 Key Things You Need to Know Now. URL: https://www.dentons.com/en/insights/articles/2023/december/14/the-new-eu-ai-act-the-10-key-things-you-need-to-know-now.
5. European Approach to Artificial Intelligence. URL: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.
6. Germany AI Strategy Report. URL: https://ai-watch.ec.europa.eu/countries/germany/germany-ai-strategy-report_en.
7. Асадуллина А.В., Белоусов В.С. Регулирование технологий искусственного интеллекта на территории Европейского Союза // Российский внешнеэкономический вестник. 2022. № 8.

Draganova D.V.
Saint Petersburg State University, Saint Petersburg

Scientific supervisor:
Dunaeva Yu.G.
Saint Petersburg State University, Saint Petersburg

THE EUROPEAN UNION'S ARTIFICIAL INTELLIGENCE STRATEGY: COORDINATED PLAN AND NATIONAL APPROACHES

Abstract. In the context of the rapid development of artificial intelligence (AI) technologies, a new information space is emerging, where states aim to strengthen their positions through strategies for technological progress. Special focus is given to the European Union's strategies, including the coordinated plan, national approaches of the United Kingdom, Germany, and France, and legal frameworks regulating AI. The AI Act, investment programs, ethical initiatives, and challenges of global competition are analyzed.

Keywords: artificial intelligence, European Union, AI Act, coordinated plan, national strategies, AI ethics, Horizon Europe, InvestAI, United Kingdom, France.

УДК 004.056.5

Загиров Р.А.
Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск

Научный руководитель:
Кузьмина У.В.
Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск

ЗАЩИТА ИНФОРМАЦИИ ОТ ЦЕЛЕВОГО ФИШИНГА В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ

Аннотация. В статье рассматриваются методы защиты информации от целевого фишинга в автоматизированных системах. Описываются основные угрозы, связанные с фишинг-атаками, и предлагаются способы предотвращения таких атак с использованием современных технологий, таких как многослойная аутентификация, анализ поведения пользователей и машинное обучение. Подчеркивается важность интеграции этих подходов в существующие системы для повышения уровня безопасности и предотвращения утечек конфиденциальных данных.

Ключевые слова: защита информации, фишинг, аутентификация, машинное обучение, безопасность.

Целевой фишинг (spear phishing) является одной из самых распространенных и разрушительных угроз в области кибербезопасности, направленных на получение конфиденциальной информации, такой как пароли, личные данные и корпоративные сведения, с помощью манипуляций и социальных инженерий. Эффективность фишинговых атак зависит от тщательной подготовки и использования специфической информации о целевой аудитории, что делает их особенно опасными в контексте автоматизированных информационных систем.

Применение технологий защиты от целевого фишинга требует всестороннего анализа угроз и инновационных методов защиты, включая использование методов машинного обучения для автоматического выявления фишинговых ссылок и социальную инженерию для обеспечения человеческого барьера защиты. Данная теоретическая часть посвящена исследованию применения методов защиты от фишинга, основанных на социальных инженерных методах и машинном обучении, с учетом существующих научных разработок [1–2].

Социальная инженерия представляет собой метод манипуляции людьми с целью получения доступа к конфиденциальной информации или изменения поведения с использованием психологических факторов. В контексте фишинговых атак, социальная инженерия играет ключевую роль

в повышении эффективности атак, направленных на специфические цели. Одно из исследований подчеркивает, что фишинг как таргетированная атака использует не только технические уязвимости, но и слабости человеческой психологии. Основным механизмом является создание ложного чувства доверия у жертвы, что приводит ее к необдуманным действиям, таким как переход по вредоносной ссылке или предоставление личной информации [1].

Таргетированные атаки часто включают персонализированные сообщения, которые используют данные из социальных сетей или корпоративных систем для создания более убедительных фишинговых писем. Жертва получает сообщение, которое кажется исходящим от коллеги или руководителя, что значительно повышает вероятность того, что она откроет вредоносное вложение или кликнет по фальшивой ссылке. Данный подход требует от злоумышленников не только технической подготовки, но и знания психологии, что делает его еще более опасным.

Важным аспектом в контексте социальной инженерии является использование фальшивых сайтов, которые копируют интерфейсы известных интернет-ресурсов, что затрудняет обнаружение фишинга. По сути, это искусственная манипуляция восприятием, в ходе которой жертва не воспринимает сообщение как угрозу, доверяя отправителю [2].

Одной из современных тактик в реализации фишинговых атак является использование документов, созданных в приложениях Microsoft Office, как контейнеров для вредоносных программ (пейлоадов). В одном из исследований рассматривается использование уязвимостей в офисных приложениях для внедрения и распространения вредоносного кода. Документы, содержащие макросы или скрытые объекты, могут быть отправлены жертве как нормальные рабочие файлы, что делает этот способ чрезвычайно эффективным.

Когда пользователь открывает такой документ, он может активировать скрытый код, который, в свою очередь, запускает пейлоад – вредоносную программу, которая может записывать нажатия клавиш, красть данные или выполнять другие действия в фоновом режиме. В отличие от традиционных методов фишинга, где жертва должна перейти по ссылке, здесь достаточно просто открыть файл, чтобы подвергнуться атаке. Это делает использование документов MS Office весьма эффективным методом для распространения фишинга, так как многие пользователи привыкли работать с такими файлами и не воспринимают их как потенциально опасные [2].

Применение данной техники требует от злоумышленников не только технических навыков, но и знания специфики работы с офисными документами, что позволяет им скрывать вредоносные элементы в таких форматах, как Word или Excel. Обычные антивирусные программы могут не всегда эффективно выявлять такие угрозы, что увеличивает риск успешной атаки.

Современные технологии машинного обучения (МЛ) играют важную роль в предотвращении фишинговых атак. Использование алгоритмов, способных выявлять аномалии в поведении пользователя и анализировать фишинговые ссылки, становится важной частью защиты автоматизированных систем. В одном из исследований описывается методы машинного обучения для автоматического определения фишинговых ссылок.

Машинное обучение позволяет анализировать огромные объемы данных и выявлять паттерны, которые могут указывать на фишинг. Например, алгоритмы могут анализировать ссылки, проверяя их на предмет известных признаков фишинга, таких как странные доменные имена, нестандартные символы и другие аномалии. Использование машинного обучения для анализа URL-адресов позволяет значительно повысить точность и скорость обнаружения угроз. В дополнение к этому, методы анализа текста позволяют выявить фишинговые письма, которые на первый взгляд могут выглядеть как легитимные, но при детальном анализе содержат скрытые признаки мошенничества [3].

Кроме того, подходы машинного обучения могут быть использованы для анализа поведения пользователей в системах, что позволяет детектировать подозрительные действия. Например, если пользователь начинает действовать нехарактерно для своей роли или перемещается по ресурсам, которые обычно не посещает, система может предупредить о возможной атаке или даже заблокировать доступ до выяснения причин.

Алгоритмы машинного обучения, такие как нейронные сети и методы классификации, могут использовать исторические данные для обучения и повышения точности распознавания фишинговых атак. Это позволяет системе адаптироваться и становиться более эффективной с каждым новым опытом.

Целевой фишинг остается одной из самых опасных форм киберугроз, оказывающих серьезное влияние на безопасность информации в автоматизированных системах. Эффективная защита от фишинга требует комплексного подхода, который включает как технические меры (например, использование многослойной аутентификации, фильтрация фишинговых писем, внедрение технологий машинного обучения), так и внимание к социальной инженерии, которая является основой большинства атак. Современные исследования в этой области подчеркивают необходимость создания гибких и эффективных систем защиты, которые могут быстро адаптироваться к новым угрозам. Использование инновационных технологий, таких как машинное обучение для автоматического обнаружения фишинговых ссылок, является важным шагом на пути к более безопасной цифровой среде.

Список использованных источников:

1. Казаковцев М.С., Михайлова У.В. Афанасьева М.В. Социальная инженерия в таргетированных атаках // Тезисы докладов 77-й международной научно-технической конференции. 2019. С. 84–87.
2. Михайлова У.В., Кремлев Е.С. Использование документов MS OFFICE в качестве контейнеров пейлоада // Тезисы докладов 77-й международной научно-технической конференции. 2019. С. 414–415.
3. Алексеев А.К., Будылин Е.С. Определение фишинговых ссылок с использованием методов машинного обучения / Оригинальные исследования (ОРИС). 2024 № 7 (14). С. 116–120.

Zagirov R.A.
Nosov Magnitogorsk State Technical University, Magnitogorsk

Scientific supervisor:
Kuzmina U.V.
Nosov Magnitogorsk State Technical University, Magnitogorsk

INFORMATION PROTECTION AGAINST SPEAR PHISHING IN AUTOMATED SYSTEMS

Abstract. The article discusses methods for protecting information from targeted phishing in automated systems. It describes the main threats associated with phishing attacks and suggests ways to prevent such attacks using modern technologies, such as multi-layer authentication, user behavior analysis, and machine learning. It emphasizes the importance of integrating these approaches into existing systems to improve security and prevent leaks of confidential data.

Keywords: information security, phishing, authentication, machine learning, security.

УДК 004.8

Зыков А.И.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шафиков М.Р.
Уфимский университет науки и технологий, Уфа

ПРИМЕНЕНИЕ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И МАШИННОГО ОБУЧЕНИЯ ДЛЯ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОТ СЕТЕВЫХ АТАК

Аннотация. В статье рассматривается применение современных технологий искусственного интеллекта и алгоритмов машинного обучения

для обнаружения сетевых кибератак на объектах критической информационной инфраструктуры РФ. Фокус в статье сделан на написании программного кода для анализа вредоносного сетевого трафика с помощью предопределенных меток и машинного обучения без данных меток.

Ключевые слова: искусственный интеллект, машинное обучение, информационная безопасность, защита информации, кибератаки.

Обеспечение защищенности конфиденциальной информации – одна из приоритетных задач современного общества Российской Федерации. Это обусловлено стремительным развитием цифровых технологий и увеличением объемов сетевого трафика, с ростом которых неумолимо растет число кибератак. Большинство из них направлено на критическую информационную инфраструктуру (КИИ). Объекты КИИ представляют собой ключевые компоненты информационной экосистемы государства и бизнеса, атаки на которые могут привести к серьезным последствиям для государства.

Согласно данным TAdviser, с каждым годом наблюдается рост числа кибератак на объекты КИИ РФ. Если в 2020 г. число атак составляло около 120000, то к 2024 г. это число выросло более, чем в 5 раз. Это означает, что, в среднем, ежемесячно субъектам КИИ РФ приходится отражать более 20000 атак. Результатом анализа, проведенным компанией RED Security, стало то, что самой атакуемой отраслью в сфере КИИ в 2024 г. стала промышленность: ТЭК, энергетика, оборонная промышленность и др. На их долю пришлось около 1/3 от общего числа кибератак на КИИ [2]. За сферой промышленности следует область ИТ. На нее пришлось 20 % от всех атак из-за возросшей популярности кибератак на российские компании через их ИТ-подрядчиков – вендоров, интеграторов и т. п. Третьей по популярности атак киберпреступников считается финансовый сектор. В 2024 г. на банковские и другие финансовые предприятия было совершено 17 % от всего числа целенаправленных атак.

В контексте обеспечения сетевой безопасности искусственный интеллект и алгоритмы машинного обучения позволяют анализировать сетевой трафик в режиме реального времени, выявлять аномалии, прогнозировать угрозы и автоматически классифицировать кибератаки с высокой точностью. Согласно статистическим данным экспертов от Anti-Malware, более трети от всех ожидаемых инноваций в сфере информационной безопасности предписывают именно технологиям искусственного интеллекта и алгоритмам машинного обучения.

Наиболее широкое применение ИИ и МО получили в сфере сетевой защиты. Наиболее подходящим средством обеспечения безопасности данных от сетевых вторжений является система обнаружения вторжений с алгоритмами машинного обучения (ML IDS). При применении искусственного интеллекта и машинного обучения на этапе проектирования средств и систем готовый продукт должен отвечать требованиям как

ГОСТ Р 71476-2024, так и ГОСТ Р 71539-2024. Особенностью построения и применения таких систем является подготовка отдельной базы данных/знаний для обучения и настройки моделей, а также необходимость в верификации и непрерывной валидации – тестировании модели перед и после развертывания соответственно [1]. В ML IDS валидация модели машинного обучения необходима для обеспечения подтверждения их эффективности и точности в обнаружении угроз.

Проведем тестирование алгоритма машинного обучения, применяемый в ML IDS. Для этого смоделируем сетевую кибератаку на объект КИИ – автоматизированную систему управления технологическими процессами. Для этого возьмем готовый датасет CIS-IDS-2017, включающий нормальный трафик и различные виды атак, имитирующие реальные сценарии сетевой безопасности: DoS- и DDoS-атаки, Port Scan, Brute Force, Web Attacks, Infiltration, Botnet Activity, Heartbleed.

Для проведения программного анализа по тем меткам, которые присутствуют в датасете, отбросим трафик, соответствующий нормальной человеческой активности (BENIGN).

Согласно проведенному анализу (рис. 1), выделим следующее: в датасете присутствует 8 видов различных кибератак, их суммарное количество 425878, более 3/4 от всех атак пришлось на DoS- и DDoS-атаки – 45,5 % и 30 % соответственно, а наименьшая доля – на «Infiltration» и «Heartbleed».

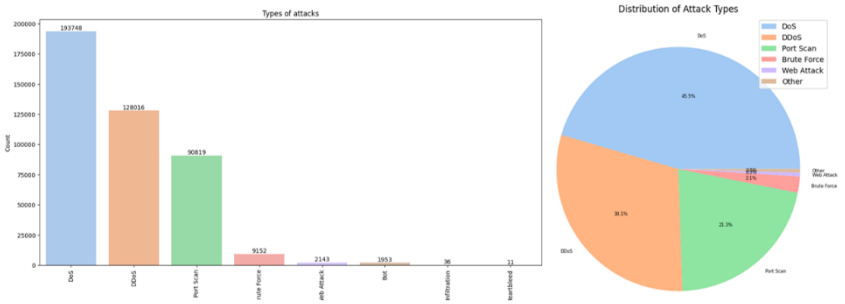

Рис. 1. Количество сетевых атак по видам (слева) и их процентное соотношение (справа) на основании программного анализа датасета

Получив исходные данные, можно приступить к обучению алгоритма для предсказания сетевых атак. Для обучения был выбран алгоритм машинного обучения – метод случайного леса (RandomForest), создающий случайные леса для решения задач классификации и регрессии [3]. Для того, чтобы обучить модель детектировать атаки, необходимо подготовить данные – удалить метку «Тип атаки», чтобы алгоритм МО обучался без подсказок, а также удалить BENIGN, разделить данные на обучающую и тестовую выборку в соотношении 80 % к 20 %, обучить алгоритм и провести оценку обученности алгоритма на тестовой выборке. Код программы по обучению модели показан на рис. 2.

```
filtered_data = data.loc[data['Attack Type'] != 'BENIGN']

features = filtered_data.drop(['Attack Type'], axis=1)
labels = filtered_data['Attack Type']

X_train, X_test, y_train, y_test = train_test_split( *arrays: features, labels, test_size=0.2, random_state=42)

model = RandomForestClassifier(n_estimators=100, random_state=42)
model.fit(X_train, y_train)

predictions = model.predict(X_test)
accuracy = accuracy_score(y_test, predictions)
print(f'Accuracy: {accuracy:.4f}')

print(classification_report(y_test, predictions))

plt.figure(figsize=(10, 6))
conf_matrix = confusion_matrix(y_test, predictions)
sns.heatmap(conf_matrix, annot=True, fmt='d', cmap='Blues', xticklabels=model.classes_, yticklabels=model.classes_)
plt.xlabel('Predicted Label')
plt.ylabel('True Label')
plt.title('Confusion Matrix')
plt.show()
```

Рис. 2. Фрагмент программного кода для обучения модели RandomForest по предсказанию сетевых атак датасета CIS-IDS-2017

Точность детектирования классов сетевых атак – 0,9998 из 1. Как видно из отчета (рис. 3), модель ошиблась в распознавании веб-атак, однако показатель правильных ответов также высокий – 0,99 из 1.

Accuracy: 0.9998

	precision	recall	f1-score	support
Bot	1.00	1.00	1.00	430
Brute Force	1.00	1.00	1.00	1856
DDoS	1.00	1.00	1.00	25653
DoS	1.00	1.00	1.00	38624
Heartbleed	1.00	1.00	1.00	3
Infiltration	1.00	1.00	1.00	6
Port Scan	1.00	1.00	1.00	18190
Web Attack	0.99	1.00	0.99	414
accuracy			1.00	85176
macro avg	1.00	1.00	1.00	85176
weighted avg	1.00	1.00	1.00	85176

Рис. 3. Оценка обученности модели RandomForest

Результатом сравнения графиков результатов программного анализа и алгоритма машинного обучения (рис. 4) является: общее количество сетевых атак пропорционально меньше при тесте ИИ-модели и составляет 20 % от всего датасета – 85176 и 425878 атак, в долевом соотношении наблюдается практически полное совпадение с результатами программного анализа, градация сетевых атак по частоте встречаемости также совпадает.

В результате проведенного анализа делаем вывод, что алгоритмы МО и ИИ способны с большой точностью выявлять атаки. Искусственный интеллект и машинное обучение – это передовые технологии, внедрение которых в системы безопасности КИИ является важным для защиты объектов. А активное развитие и применение ИИ и МО в области ИБ – необходимость современности, чтобы справляться с постоянно растущим количеством киберугроз и уязвимостей.

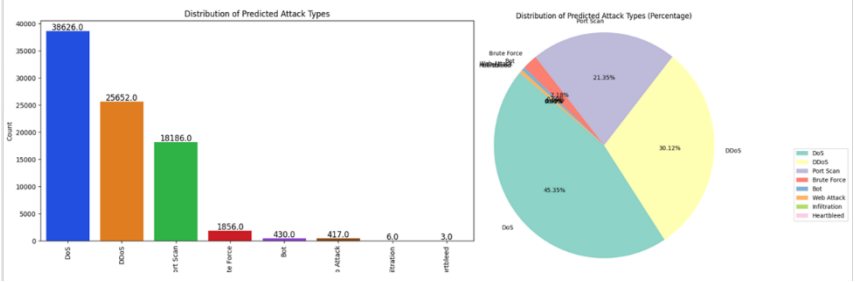

Рис. 4. Количество сетевых атак по видам (слева) и их процентное соотношение (справа) на основании предсказания модели RandomForest

Список использованных источников:

1. ГОСТ Р 71539-2024 (ИСО/МЭК 5338:2023). Национальный стандарт Российской Федерации. Искусственный интеллект. Процессы жизненного цикла системы искусственного интеллекта // КонсультантПлюс: [сайт]. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=43150#OU7AUhUSG1BHGtM81 (дата обращения: 30.03.2025).
2. RED Security SOC: хакеры усилили давление на критическую информационную инфраструктуру России // Компания «RED Security»: [сайт]. URL: https://redsecurity.ru/news/red-security-soc-khakery-usilili-davlenie-na-kriticheskuyu-informatsionnuyu-infrastrukturu-rossii (дата обращения: 30.03.2025).
3. Баланов А.Н. Машинное обучение и искусственный интеллект: учебное пособие для вузов [Текст] / А.Н. Баланов. 2-е изд. СПб.: Лань, 2025. 172 с.

Zykov A.I.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shafikov M.R.
Ufa University of Science and Technology, Ufa

USING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING METHODS TO PROTECT CRITICAL INFORMATION INFRASTRUCTURE FROM NETWORK ATTACKS

Abstract. In the article it is discussed using of modern artificial intelligence technologies and machine learning algorithms to detect network cyberattacks on critical information infrastructure objects of Russian Federation. The focus of the article is on writing software code to analyze malicious network traffic using predefined labels and a machine learning algorithm without these labels.

Keywords: artificial intelligence, machine learning, information security, information protection, cyberattacks.

УДК 004

Клыгин В.О.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Салов И.В.
Уфимский университет науки и технологий, Уфа

ДЕЦЕНТРАЛИЗОВАННЫЕ ИДЕНТИФИКАТОРЫ (DIDs) КАК ОСНОВА БЕСПАРОЛЬНОЙ АУТЕНТИФИКАЦИИ И УСТРАНЕНИЕ РИСКОВ ЦЕНТРАЛИЗОВАННОГО ХРАНЕНИЯ ДАННЫХ

Аннотация. В статье рассматриваются децентрализованные идентификаторы (DIDs) как метод беспарольной аутентификации, обеспечивающий безопасный вход и суверенное управление данными без рисков централизованного хранения.

Ключевые слова: аутентификация, идентификаторы, блокчейн, децентрализация, пароль.

Во время различных войн противники активно боролись со шпионами, используя кодовые слова или пароли, служившие способом отличить своих от врагов. Принцип «если я знаю секрет, значит, я тот, за кого себя выдаю» лег в основу современных систем аутентификации. Сегодня пароль остается ключевым элементом для подтверждения личности и защиты цифровых данных.

Но их использование сопровождается рядом проблем, главная из которых – баланс между удобством и безопасностью. Согласно исследованию DLBI, российской службы анализа утечек данных, в 2024 г. среди самых популярных паролей в российских доменных зонах оказались «123456», «1221123456», «12345», «йцукен» и «пароль». Такие простые и легко запоминаемые пароли уязвимы к атаке полным перебором (Brute Force), которая позволяет подобрать их за считанные минуты, особенно если злоумышленники используют словари распространенных паролей или радужные таблицы.

В отличие от простых паролей, сложные, состоящие из случайных символов, значительно увеличивают время, необходимое для их взлома. Однако высокая сложность создает другую проблему: такие пароли трудно запомнить. Это вынуждает пользователей прибегать к помощи менеджеров паролей – централизованных хранилищ, которые, в свою очередь, становятся основной целью злоумышленников. В случае их взлома злоумышленник может получить доступ ко всем паролям пользователя, а сам пользователь рискует потерять доступ к своим данным на различных ресурсах.

Для улучшения методов аутентификации были внедрены электронные инструменты, такие как двухфакторная аутентификация (2FA), которая добавляет дополнительный уровень защиты поверх традиционных паролей. Для обхода этого метода начались атаки с применением социальной инженерии, которая по данным экспертов Positive Technologies, в третьем квартале 2024 г. являлась наиболее популярным методом атаки как на организации (50 %), так и на частных лиц (92 %). Также значительно возросло количество фишинговых атак – в России их число в 2024 г. превысило 350 тысяч.

Из-за необходимости постоянной регистрации и ввода длинных паролей началось активное внедрение методов аутентификации, которые не требуют использования паролей. Одним из наиболее известных решений стала биометрическая аутентификация. Несмотря на свою инновационность, она также оказалась уязвимой для атак. На ранних этапах разработки биометрических систем аутентификацию по лицу можно было обойти с помощью качественных фотографий, 3D-масок или заранее записанных видео. В ответ на эти угрозы были разработаны алгоритмы определения живости (liveness detection), способные выявлять поддельные данные. Однако и эти меры не стали панацеей: с появлением генеративно-состязательных сетей (GAN) злоумышленники получили возможность создавать искусственные биометрические данные (deepfake), которые успешно проходят проверки на живость, создавая новые вызовы для биометрических систем.

Кроме того, как и обычные пароли, биометрические данные часто хранятся в централизованных хранилищах, что делает их приоритетной целью для атакующих. Но главным отличием от паролей, которые можно изменить в случае компрометации, биометрические данные остаются неизменными, что делает их утечку особенно критичной. Самым громким инцидентом стала утечка данных на платформе BioStar 2, разработанной компанией Suprema. В 2019 г. в открытый доступ попали более 27,8 млн записей (23 ГБ данных), затронув более 1 миллиона человек.

Осознавая эти проблемы, специалисты по безопасности еще в 1990-х гг. начали обсуждать новые методы аутентификации, включая принципы децентрализованных данных и контроля над личной информацией. Их цель заключалась в том, чтобы отказаться от необходимости использования длинных и уникальных паролей для разных сервисов и их хранения в централизованных базах.

Одним из пионеров децентрализованной идентификации стал Кристофер Аллен – архитектор блокчейна и соавтор стандартов IETF TLS и W3C DIDs. Вместе с Тимом Бернерсом-Ли, создателем всемирной паутины, он участвовал в разработке версии 1.0 децентрализованных идентификаторов (DIDs).

Согласно W3C, децентрализованные идентификаторы (DIDs) – это новый тип идентификаторов, которые обеспечивают проверяемую

децентрализованную цифровую идентификацию. DID может быть присвоен любому субъекту: человеку, организации, предмету, модели данных или даже абстрактному объекту. При этом контроль над идентификатором полностью принадлежит его владельцу [1].

Технология DIDs основана на криптографии с использованием приватных и публичных ключей и является одним из трех столпов суверенной идентификации. Ее основные компоненты включают:

Блокчейн – это децентрализованный цифровой реестр, поддерживаемый распределенной сетью компьютеров. Данные хранятся в блоках, связанных в хронологическом порядке, и защищены криптографией [2].

Децентрализованные идентификаторы (DIDs) – это пользовательские идентификаторы, создаваемые и контролируемые самими пользователями без участия централизованных органов.

Проверяемые учетные данные (VC) – это криптографически защищенные цифровые документы, позволяющие подтверждать личность или другие сведения без раскрытия избыточной информации.

Принцип работы технологии заключается в следующем: пользователь подписывает запрос от сервиса своим приватным ключом, а сервис, которому необходимо удостовериться в подлинности, расшифровывает данные с помощью публичного ключа, который хранится децентрализовано.

Технология децентрализованных идентификаторов (DIDs) может усилить безопасность данных, что особенно актуально в условиях роста киберугроз в России. В 2024 г. в сеть попало 710 миллионов записей, включая более 80 млн паролей. Основными целями стали объекты КИИ и базы МФЦ. Основной платформой для хранения персональных данных граждан РФ выступают «Госуслуги», где хранятся данные, позволяющие взаимодействовать с государственными органами и финансовыми организациями, что делает ее привлекательной целью для атак. Одной из главных задач злоумышленников является преодоление этапа аутентификации для доступа к этим данным.

Сегодня для входа в личный кабинет на «Госуслугах» используются логин и пароль с двухфакторной аутентификацией через SMS, сканирование QR-кода только с устройства, на котором уже выполнен вход или электронная подпись, на физическом носителе, как «Рутокен». Помимо проблем, о которых говорилось выше, еще одной проблемой, одинаковой для всех все трех способов, является хранение и обработка необходимых для входа идентификаторов в централизованной системе, что создает высокий риск атак и делает ее уязвимой для краж, уничтожения или изменения данных [3].

С внедрением DIDs можно избавиться от необходимости использовать пароли и дополнительные устройства для входа. Но самое главное – мы откажемся от централизованного хранения данных, перейдя к децентрализованной системе на основе блокчейна, что устранит единую точку отказа и снизит риски потери чувствительной информации.

В качестве эмитента сможет выступать орган исполнительной власти, подтверждающий личность пользователя и выпускающий децентрализованные идентификаторы (DIDs), заверенные государством. Эти идентификаторы будут размещаться в блокчейне вместе с публичными ключами пользователя и эмитента. Узлами блокчейна могут стать министерства, службы и даже частные компании. Для хранения приватного ключа, используемого для подписи запросов, можно задействовать приложение «Госключ», позволяющее пользователю подтверждать личность при аутентификации.

Однако, остаются определенные проблемы. Например, безопасность приложения «Госключ» потребует многофакторной защиты: пароля, биометрии, двухфакторной аутентификации (2FA) или сид-фразы для восстановления доступа. Кроме того, вектор атак сместится на пользователей, увеличивая риски атак с использованием социальной инженерии. Это подчеркивает важность повышения цифровой грамотности пользователей.

Список использованных источников:

1. Decentralized Identifiers (DIDs) v1.1 // W3C. URL: https://www.w3.org/TR/did-1.1/#example-a-simple-did-document.

2. Что такое блокчейн и как он работает? // Binance Academy. URL: https://academy.binance.com/ru/articles/what-is-blockchain-and-how-does-it-work.

3. Кириллов В.С. Проблематика использования электронных подписей / В.С. Кириллов, А.С. Исмагилова, Д.Т. Набиев // Информационные технологии интеллектуальной поддержки принятия решений (памяти проф. Н.И. Юсуповой) ITIDS'2024: труды X Международной научной конференции. В 2 томах. Уфа, 12–14 ноября 2024 г. Уфа: Уфимский университет науки и технологий, 2024. С. 1214.

Klygin V.O.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Salov I.V.
Ufa University of Science and Technology, Ufa

DECENTRALISED IDENTIFICATORS (DIDs) AS A BASIS FOR PASSWORDLESS AUTHENTIFICATION AND REDUCING RISKS OF CENTRALISED DATA STORAGE

Abstract. This paper discusses decentralised identifiers (DIDs) as a passwordless authentication method that provides secure login and sovereign data management without the risks of centralised storage.

Keywords: authentication, identifiers, blockchain, decentralisation, password.

УДК 004

Кудакаев И.Ф., Ракипов Д.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Юнусова Д.С.
Уфимский университет науки и технологий, Уфа

ОБНАРУЖЕНИЕ СПАМА В EMAIL

Аннотация. В статье рассматриваются базовые подходы к обнаружению спама в электронной почте с применением методов обработки естественного языка (NLP). Пошаговое руководство ориентировано на начинающих специалистов и студентов, интересующихся машинным обучением и лингвистическим анализом текстов. Подробно описываются этапы подготовки данных, методы предобработки текста (включая лемматизацию и токенизацию), выбор признаков и алгоритмы классификации. Отдельное внимание уделяется сравнительному анализу моделей и оценке их эффективности. Работа сопровождается практическими рекомендациями и примерами кода, что делает ее полезной для создания собственного инструмента фильтрации спама.

Ключевые слова: обработка естественного языка, машинное обучение, фильтрация спама, классификация текста, лемматизация.

Обнаружение спама в электронной почте представляет собой одну из важнейших задач в области информационной безопасности и интеллектуального анализа текста. В связи с ростом объема нежелательной корреспонденции возрастает необходимость в автоматизированных решениях, способных эффективно фильтровать спам. Одним из наиболее результативных направлений в решении данной задачи является применение методов обработки естественного языка (Natural Language Processing, NLP), позволяющих анализировать текст писем, извлекать ключевые признаки и классифицировать сообщения по определенным критериям.

Использование электронной почты больше не ограничивается только общением с другим человеком. В эпоху цифровизации пользователь постоянно получает по электронной почте информацию о текущих предложениях, статусе заказа или новостях в социальных сетях. Инженерия знаний (Knowledge Engineering) и машинное обучение (Machine Learning) – это два основных подхода, которые используются при фильтрации электронной почты. В подходе инженерии знаний необходимо задать набор правил, согласно которым электронные письма классифицируются как спам (нежелательная почта) или хам (нормальная почта).

Такой набор правил должен быть создан либо самим пользователем фильтра, либо другим уполномоченным органом (например, компанией-разработчиком программного обеспечения, предлагающей инструмент фильтрации спама на основе правил). Применение этого метода не демонстрирует обнадеживающих результатов, так как правила необходимо постоянно обновлять и поддерживать, что требует времени и неудобно для большинства пользователей. Подход машинного обучения является более эффективным, чем подход инженерии знаний; он не требует задания правил [1]. Вместо этого используется набор обучающих примеров – в данном случае это заранее классифицированные электронные письма. Для успешного внедрения системы обнаружения спама начинающим специалистам рекомендуется использовать поэтапный подход: от сбора и подготовки данных до анализа результатов классификации.

Важно учитывать не только точность модели, но и такие метрики, как полнота, точность, F-мера, а также способность модели обрабатывать и распознавать сложные случаи, включая сарказм, скрытые намерения и измененные шаблоны спама. Таким образом, применение NLP в задаче фильтрации электронной почты требует комплексного подхода, сочетающего лингвистический анализ и математические методы классификации. Специальный алгоритм затем используется для извлечения правил классификации из этих писем. Подход машинного обучения широко изучен, и существует множество алгоритмов, которые могут быть применены для фильтрации электронной почты [2].

NLP может применяться как для лингвистического анализа текста, так и для анализа настроений и мнений (Sentiment Analysis), переводов, а также в голосовых помощниках, чат-ботах и системах «вопрос-ответ». В сочетании с аспектами информатики, такими как системный анализ и моделирование, а также с областями теоретической информатики, например, теориями вычислимости и сложности, компьютерная лингвистика получает знания о структурах данных и использовании эффективных алгоритмов. Это позволяет решать прикладные задачи, такие как перевод предложений на разные языки или обработка заказа пиццы по телефону [3].

Для достижения этих целей необходимо охватить множество задач – от распознавания устной речи до построения парсера и разработки набора методов и алгоритмов, с помощью которых естественный язык и человеческая коммуникация могут быть проанализированы в программных системах. При этом важно извлечь как можно более глубокое понимание устной или письменной речи. Основой для этого является источник текстовых данных, называемый корпусом. Поскольку корпуса и другие текстовые данные, как правило, представлены в неструктурированном виде, применяется широкий спектр методов, чтобы преобразовать необработанные данные в четко определенные последовательности лингвистических компонентов. Обработка естественного языка (Natural

Language Processing, NLP) занимается пониманием человеческой речи – и именно в этом заключается основная сложность.

Язык очень сложен и не всегда однозначен. Дополнительно анализ человеческой речи сильно усложняется такими явлениями, как фразеологизмы, ирония или игра слов. Недостаточно, чтобы компьютер просто распознавал отдельные слова. Важно, чтобы машина понимала предложения и их контексты. Человек в этом плане имеет преимущество: он может опираться на жизненный опыт и учит язык с рождения. Поэтому язык для человека понятен и легко поддается интерпретации. Компьютеру же необходимо освоить этот навык с нуля с помощью алгоритмов. Правила, по которым происходит анализ языка, могут быть разной степени сложности [4].

Разница между ними в том, что корень-основа (стем) не всегда является корректным словом с точки зрения лексикографии, то есть может отсутствовать в словаре. Лемма же всегда является словарной формой. Процесс лемматизации значительно медленнее, чем стемминг, поскольку требует дополнительного шага – определения леммы путем удаления аффикса только в том случае, если соответствующая лемма действительно существует в словаре. Это требует дополнительной мощности со стороны компьютерной лингвистики, например, использования теггера частей речи (Part-of-Speech-Tagger) [5].

Освоение базовых инструментов NLP и алгоритмов машинного обучения позволяет не только повысить точность фильтрации, но и развить практические навыки в области анализа текста. Для начинающих специалистов данная область открывает широкие возможности для экспериментов и дальнейших исследований, а также способствует созданию более безопасной и комфортной среды электронного общения.

Список использованных источников:

1. Горюнова Д.А., Кузьмина Е.С. Обнаружение спама в электронной почте на основе машинного обучения: сравнение функциональной разработки и комплексных методов // Экономика и социум. 2024. № 6-1 (121). URL: https://cyberleninka.ru/article/n/obnaruzhenie-spama-v-elektronnoy-pochte-na-osnove-mashinnogo-obucheniya-sravnenie-funktsionalnoy-razrabotki-i-kompleksnyh-metodov-1 (дата обращения: 20.04.2025).

2. Корелов С.В., Петров А.М., Ротков Л.Ю., Горбунов А.А. Предобработка текстов электронных писем в задаче обнаружения спама // Труды учебных заведений связи. 2020. № 4. URL: https://cyberleninka.ru/article/n/predobrabotka-tekstov-elektronnyh-pisem-v-zadache-obnaruzheniya-spama (дата обращения: 20.04.2025).

3. Частикова В.А., Козачёк К.В. Обзор актуальных проблем основных методов фильтрации спама и анализ их эффективности // Вестник Адыгейского государственного университета. Серия 4: Естественно-

математические и технические науки. 2021. № 3 (286). URL: https://cyberleninka.ru/article/n/obzor-aktualnyh-problem-osnovnyh-metodov-filtratsii-spama-i-analiz-ih-effektivnosti (дата обращения: 20.04.2025).

4. Харитонова Ю.С., Савина В.С., Паньини Ф. Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права // Вестник Пермского университета. Юридические науки. 2021. № 53. URL: https://cyberleninka.ru/article/n/predvzyatost-algoritmov-iskusstvennogo-intellekta-voprosy-etiki-i-prava (дата обращения: 20.04.2025).

5. Хаммасова Л.Ш., Нестеров С.А. Распознавание спам-сообщений с использованием методов машинного обучения // SAEC. 2023. № 3. URL: https://cyberleninka.ru/article/n/raspoznavanie-spam-soobscheniy-s-ispolzovaniem-metodov-mashinnogo-obucheniya (дата обращения: 20.04.2025).

Kudakaev I.F., Rakipov D.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yunusova D.S.
Ufa University of Science and Technology, Ufa

EMAIL SPAM DETECTION

Abstract. This article explores fundamental approaches to email spam detection using natural language processing (NLP) techniques. Designed for beginners and students interested in machine learning and linguistic text analysis, the guide walks through the key stages of data preparation, text preprocessing (including lemmatization and tokenization), feature selection, and classification algorithms. Special focus is given to comparing models and evaluating their performance. The article includes practical tips and code examples, making it a valuable resource for those looking to build their own spam filtering tool.

Keywords: natural language processing, machine learning, spam filtering, text classification, lemmatization.

УДК: 004.492.3

Мухаметшина Р.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

ОПТИМИЗАЦИЯ СИГНАТУРНОГО АНАЛИЗА С ИСПОЛЬЗОВАНИЕМ БИТОВЫХ МАСОК: СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ

Аннотация. В данной статье представлен комплексный анализ метода оптимизации сигнатурного анализа с использованием битовых масок. Исследование включает теоретическое обоснование использования метода, детальное описание экспериментальной реализации, сравнительный анализ производительности и практические рекомендации по внедрению.

Ключевые слова: сигнатурный анализ, битовые маски, оптимизация производительности, IDS, обнаружение атак, Python.

При работе с современными системами обнаружения вторжений (IDS) специалисты по информационной безопасности сталкиваются с фундаментальной проблемой обработки экспоненциально растущего объема сетевого трафика при необходимости сохранения высокой точности обнаружения угроз. В современных системах защиты основным инструментом выявления атак остаются сигнатурные методы анализа сетевого трафика. Их эффективность в обнаружении известных угроз подтверждена многолетней практикой применения, однако она напрямую зависит от актуальности и полноты используемой базы сигнатурных правил [1]. Эта проблема особенно актуальна для промышленных систем, где требования к скорости передачи информации зависят от спецификаций протокольных сред каждого уровня [2].

Традиционные методы сигнатурного анализа, основанные на последовательном поиске, демонстрируют временную сложность O(n×m), что становится критичным при обработке гигабитных потоков данных. В данной статье предлагается метод оптимизации сигнатурного анализа с использованием битовых масок, который позволит значительно ускорить процесс обнаружения известных угроз без потери точности.

Метод битовых масок реализует эффективный механизм предварительной фильтрации трафика за счет использования компактных бинарных шаблонов, где каждый бит маски соответствует определенному признаку в анализируемом пакете. Как следует из принципов работы битовых масок, значение каждого бита отвечает за наличие соответствующего элемента в

подмножестве [3], что позволяет быстро идентифицировать потенциально опасные пакеты путем битовых операций.

Актуальность исследования подтверждается тем, что большинство коммерческих и открытых IDS до сих пор используют устаревшие алгоритмы поиска сигнатур. В отличие от статистических методов, анализирующих аномалии поведения, сигнатурный анализ остается основным подходом в коммерческих продуктах благодаря своей простоте и эффективности, но нуждается в модернизации алгоритмов поиска [4].

Ключевые преимущества метода битовых масок перед классическим линейным поиском:

1. Снижение вычислительной нагрузки на 30–50 % за счет использования быстрых битовых операций вместо последовательного перебора.
2. Режим реального времени обработки благодаря эффективному представлению данных (использование целочисленных типов для хранения масок).
3. Гибкость адаптации к изменениям в сигнатурных базах, так как перебор всех масок размера n можно удобно осуществлять путем перебора всех чисел от 0 до 22^n – 1.

Для проведения экспериментов был разработан скрипт generate_data.py, создающий:

Файл сигнатур (signatures.txt) – 1000 случайных строк длиной 20 символов, имитирующих сигнатуры атак.

Наборы пакетов (packets_*.txt) – файлы с данными, включающие легитимный и вредоносный трафик в различных пропорциях.

Для воспроизводимости результатов использовался фиксированный сид (random.seed(42)).

Были разработаны два подхода:

Базовый алгоритм (simple_detection.py) – последовательный поиск каждой сигнатуры в пакетах.

Оптимизированный алгоритм (optimized_detection.py) – предварительная фильтрация пакетов с помощью битовых масок (длиной 8 бит), что сокращает количество полных проверок.

Для сравнения алгоритмов использовались:

Время выполнения (сек) – среднее значение по 4 запускам и загрузка CPU (%) – измерена с помощью psutil.

Эксперименты проводились в виртуальной среде со следующей конфигурацией:

Хост-система:

Процессор: Intel Core i7-9700 (8 ядер @ 3.0 GHz)

Память: 32 GB DDR4;

Хранилище: NVMe SSD 1 TB;

Виртуальная машина (Oracle VirtualBox 7.1.4):

Гостевая ОС: Ubuntu 25.04 (Plucky Puffin).

Особое внимание уделялось мониторингу ресурсов во время тестов.

Использование памяти не превышало 60 % от доступной, температура CPU поддерживалась в допустимых пределах.

Ниже представлены результаты по времени и по загрузки процессора при проведении экспериментов с базовым алгоритмом и с предложенным в статье оптимизированным алгоритмом, который использует метод битовых масок, где БА – базовый алгоритм, ОА – оптимизированный алгоритм.

Таблица 1

Результаты проведенных экспериментов

Сценарий	Пакеты	Атаки	БА (время, с)	БА (CPU, %)	ОА (время, с)	ОА (CPU, %)
1	10000	7650	0,5295	0,505	0,2432	0,23
2	786	460	0,04885	0,73	0,019575	0,35
3	200	20	0,013975	1,19	0,005075	0,705
4	16	1	0,001175	0,7225	0,000475	2,5625

Были сделаны следующие выводы:

Оптимизированный алгоритм в 2–2,5 раза быстрее базового при больших объемах данных.

Загрузка CPU снижается на 30–50 % для большинства сценариев.

В качестве заключения можно отметить следующее: применение битовых масок позволило значительно ускорить сигнатурный анализ без потери точности. Однако исследование выявило несколько направлений для дальнейшей работы:

Оптимизация длины масок – подбор оптимального размера для баланса между скоростью и точностью.

Динамические маски – адаптация масок под статистику трафика с помощью машинного обучения.

Гибридные методы – комбинация с другими алгоритмами (например, хешированием) для дальнейшего ускорения.

Результаты могут быть интегрированы в легковесные IDS для IoT-устройств или серверов с ограниченными ресурсами, где критична эффективность обработки трафика.

Дополнительные исследования: Тестирование на реальных сетевых данных (например, дампы трафика с атаками DDoS).

Сравнение с другими методами оптимизации (например, префиксными деревьями).

Таким образом, использование битовых масок демонстрирует высокий потенциал для оптимизации сигнатурного анализа в современных системах кибербезопасности.

Список использованных источников:

1. Гетьман А.И. Сравнение системы обнаружения вторжений на основе машинного обучения с сигнатурными средствами защиты информации / А.И. Гетьман, М. Н. Горюнов, А.Г. Мацкевич, Д.А. Рыболовлев // Труды ИСП РАН. 2022. Т. 34, № 5. С. 111–126.
2. Подтопельный В.В. Особенности формирования сигнатурных последовательностей для обнаружения сетевых атак в АСУТП / В.В. Подтопельный // Modern Science. 2020. № 12-3. С. 303–307.
3. Переборы с помощью битовых масок // Средняя школа № 9. URL: https://sch9.ru/news/
4. Актуальные вопросы выявления сетевых атак // InfoSecPortal.ru. URL: https://infosecportal.ru/stati/aktualnye-voprosy-vyyavleniya-setevyh-atak/

Mukhametshina R.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.U.
Ufa University of Science and Technology, Ufa

OPTIMIZATION OF SIGNATURE ANALYSIS USING BITMASKS: A COMPARATIVE STUDY

Abstract. This paper presents a comprehensive analysis of a method for optimizing signature analysis using bitmasks. The study includes a theoretical justification of the method, a detailed description of its experimental implementation, a comparative performance analysis, and practical recommendations for deployment.

Keywords: signature analysis, bitmasks, performance optimization, IDS, attack detection, Python.

УДК 004

Николаев Ю.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Байрушин Ф.Т.
Уфимский университет науки и технологий, Уфа

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ МУНИЦИПАЛЬНЫХ УЧРЕЖДЕНИЙ

Аннотация. В статье рассматриваются ключевые угрозы информационной безопасности в государственных муниципальных учреждениях, включая фишинг, вредоносное ПО и человеческий фактор. Приводятся примеры угроз, представляющих опасность для государственных и муниципальных органов. Предложены меры устранения угроз информационной безопасности: обучение сотрудников, переход на отечественное ПО и усиление нормативной базы.

Ключевые слова: информационная безопасность, муниципальные учреждения, фишинг, программы-вымогатели, человеческий фактор, кибератаки, цифровая гигиена, импортозамещение, защита данных.

Государственные муниципальные учреждения становятся ключевой мишенью для киберпреступников из-за концентрации конфиденциальных данных и недостаточной готовности к современным угрозам. По данным аналитиков, на госсектор приходится 15 % успешных кибератак в России, при этом 66 % утечек данных происходят по вине сотрудников. В статье анализируются основные угрозы и предлагаются меры по укреплению защиты [1].

Рассмотрим основные угрозы информационной безопасности:

1. Фишинговые атаки и социальная инженерия. Данные атака направлены на кражу или повреждение данных. Злоумышленники активно используют методы социальной инженерии, маскируясь под официальные запросы. За этим следуют утечки данных в которых личные данные сливаются в общий доступ или к необратимому повреждению этих данных. В 2024 г. 57 % атак были направлены на сотрудников через:

- СМС с ссылками на фальшивые порталы;
- фишинговые формы сбора персональных данных;

Например, в г. Уфа зафиксирован случай утечки данных через поддельный запрос в соцсетях от имени администрации города [2].

2. Вредоносное ПО и программы-вымогатели. Вредоносное ПО является одной из угроз для безопасности госучреждений. Программа-вымогатель, Spyware и прочие программы которые могут украсть данные, шпионить за пользователем, забрать контроль над ПО у госслужащего,

DDoS-S атаки и блокировка работы всех систем. Атаки с использованием шифровальщиков выросли на 23 % за 2024 г. Муниципальные учреждения уязвимы из-за:

- устаревшего ПО (40 % систем не обновляются регулярно);
- отсутствия резервного копирования данных.

Каждая третья атака на госучреждения приводит к простою систем на 6+ часов [3].

3. Человеческий фактор. Человеческий фактор является основной проблемой утечки или потери информации. Основной она является в силу того, что остальные проблемы исходят именно из-за человека, так как он является главной из угроз для сохранности ПО. Загрузка вредоносного ПО, неспособность организовать грамотную программу для борьбы с кибератаками, практические ошибки в работе с ПО, приводящие к потере информации, и заинтересованность конкретного работника в потере информации. На это указывает статистика - 66 % инцидентов связаны с ошибками персонала:

- передача логинов и паролей третьим лицам;
- использование личных устройств для работы.

Таблица 1

Статистика угроз (2024 г.)

Показатель	Значение
Успешные атаки на госсектор	15 %
Утечки из-за человеческого фактора	66 %
Внедрение отечественных решений	37 %

Рис. 1. Распределение типов кибератак на муниципальные учреждения

Рассмотрим рекомендации по защите от угроз информационной безопасности:

1. Обучение сотрудников. В рамках борьбы с кибератаками обучение сотрудников и отсев «ненадежных» сотрудников является самым важным делом, в т. ч.:

• внедрение программ по цифровой гигиене (ежеквартальные тренинги);

2. Технические меры:

• переход на отечественное ПО (37 % учреждений уже используют российские программы);

• регулярное обновление систем;

• внедрение нейросетей с обучением сотрудников для работы с этой технологией.

3. Нормативное регулирование. Нормативная база является важным формальным механизмом закрепления основ борьбы с кибератаками, признавая их существование дарованием им определенного статуса и определяя права и обязанности сотрудников по борьбе с киберугрозами. Для этого необходимо:

• разработка стандартов безопасности для муниципальных ИС;

• создание единого центра мониторинга угроз

Например, в Республике Башкортостан внедрена система анализа уязвимостей, снизившая число успешных атак на 18 %. [4]

Таким образом, защита данных в муниципальных учреждениях требует комплексного подхода: сочетания технологий, обучения и нормативной базы. Приоритетными задачами остаются борьба с человеческим фактором и импортозамещение. Как показала практика, учреждения, внедрившие программы цифровой гигиены, сокращают риски утечек информации на 40 %.

Список использованных источников:

1. Попкова А.А. Парфенов К.В. Алборов А.Р. Угрозы информационной безопасности в государственном секторе России // Известия высших учебных заведений. Социология. Экономика. Политика. 2024. С. 77–92. Электрон. версия. URL: https://cyberleninka.ru/article/n/ugrozy-informatsionnoy-bezopasnosti-v-gosudarstvennom-sektore-rossii.

2. Как учитывать отечественное программное обеспечение. URL: https://cfo.bashkortostan.ru/presscenter/news/658844/.

3. Цифра дня: подсчитано количество всех кибератак на Россию за 2024 г. URL: https://hi-tech.mail.ru/news/121003-cifra-dnya-podschitano-kolichestvo-vseh-kiberatak-na-rossiyu-za-2024-god/.

4. Капкова В.А. Информационная безопасность в системе государственной и муниципальной службы // Молодой ученый. 2023. № 47 (494). С. 96–99. URL: https://moluch.ru/archive/494/107989/.

Nikolaev Y.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Bayrushin F.T.
Ufa University of Science and Technology, Ufa

THREATS TO INFORMATION SECURITY OF STATE MUNICIPAL INSTITUTIONS

Abstract. The article discusses the key threats to information security in government and municipal institutions, including phishing, malware, and the human factor. Examples of threats that pose a danger to government and municipal bodies are provided. Measures to eliminate information security threats are proposed: staff training, switching to domestic software, and strengthening the regulatory framework.

Keywords: information security, municipal institutions, phishing, ransomware, human factor, cyberattacks, digital hygiene, import substitution, data protection.

УДК 004.771

Панов Н.С.
Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск

Научный руководитель:
Холодилов С.С.
Магнитогорский государственный технический университет им. Г.И. Носова, Магнитогорск

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ VPN-СЕРВЕРА С ПОМОЩЬЮ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Аннотация. В статье проводится комплексный анализ криптографических и архитектурных основ двухфакторной аутентификации в VPN-сетях. Исследуются механизмы реализации временных одноразовых паролей, HMAC-аутентификации и протоколов расширенной аутентификации, проводится сравнительный анализ эффективности различных методов двухфакторной проверки подлинности против современных киберугроз. Особое внимание уделяется криптографической стойкости временных одноразовых паролей и их интеграции с существующими VPN-решениями.

Ключевые слова: VPN, двухфакторная аутентификация, TOTP, криптографические протоколы, информационная безопасность.

Современные угрозы информационной безопасности, включая фишинг, брутфорс-атаки и перехват сессий, требуют пересмотра традиционных методов аутентификации в VPN-сетях. Согласно последним исследованиям самыми распространенными видами атак становятся социальная инженерия (фишинг) и использование вредоносного программного обеспечения (ПО) [1].

В основе временных одноразовых паролей (TOTP) лежит алгоритм HMAC-SHA1, обеспечивающий генерацию 160-битного хеша. Работа этого механизма основана на 30-секундных временных интервалах, вычисляемых как Unix Time, деленное на 30, и секретном ключе длиной не менее 80 бит. Криптостойкость системы обеспечивается тремя основными факторами: необратимостью хеш-функции SHA-1, динамической природой генерируемых кодов и ограниченным временем жизни каждого пароля, которое обычно составляет от 30 до 60 секунд.

Среди протоколов аутентификации особого внимания заслуживают EAP-TTLS/PAP, обеспечивающий инкапсуляцию пароля в TLS-туннель, и PEAP-MSCHAPv2, который сочетает сертификаты сервера с парольной аутентификацией. Альтернативным решением является протокол OATH-HOTP, основанный на событиях и описанный в RFC 4226. Каждый из этих протоколов имеет свои преимущества и ограничения в контексте использования с VPN-технологиями.

При сравнении различных методов двухфакторной аутентификации выявляются существенные различия в их характеристиках. SMS-коды, несмотря на их широкое распространение и удобство использования, демонстрируют низкую стойкость к атакам типа SIM-swap и высокую уязвимость к перехвату. Временные одноразовые пароли (TOTP) [2], такие как реализованные в Google Authenticator, предлагают более высокий уровень защиты от брутфорс-атак, но остаются уязвимыми к фишингу. Наиболее безопасным решением являются U2F-токены, например YubiKey, которые обеспечивают максимальную стойкость к брутфорсу и практически нулевую уязвимость к атакам типа «человек посередине», хотя и уступают другим методам по удобству использования.

Модель RADIUS-сервера представляет собой трехуровневую архитектуру, где VPN-клиент взаимодействует с сервером RADIUS (например, FreeRADIUS с модулем pam_google_authenticator), который в свою очередь аутентифицирует пользователя через LDAP или Active Directory. Такая архитектура обеспечивает централизованное управление аутентификацией и поддерживает множество протоколов, включая PAP, CHAP и MS-CHAPv2.

Альтернативным подходом является использование PAM-модулей для OpenVPN [3]. В этом случае аутентификация осуществляется через

pam_exec с последующей верификацией с помощью специализированных скриптов на bash или Python, которые могут интегрироваться с генераторами TOTP. Этот метод обеспечивает гибкость в настройке и может быть адаптирован под конкретные требования системы безопасности.

Среди основных угроз для систем двухфакторной аутентификации в VPN следует отметить перехват временных паролей через фишинг, атаки на синхронизацию времени через подделку NTP-серверов и компрометацию seed-ключей.

Для противодействия этим угрозам рекомендуется использовать FIDO2/U2F вместо TOTP, внедрять квантово-устойчивые алгоритмы, такие как CRYSTALS-Kyber, и реализовывать жесткую привязку устройств через технологию device fingerprinting. Эти меры позволяют значительно повысить уровень безопасности VPN-соединений.

Проведенный анализ демонстрирует, что современные реализации двухфакторной аутентификации для VPN должны сочетать криптографически стойкие протоколы (например, TOTP с SHA-256), аппаратную верификацию через U2F-токены и защиту от асинхронизации времени через аутентифицированные NTP-серверы. Перспективным направлением развития является разработка квантово-устойчивых методов двухфакторной аутентификации, основанных на решетчатых криптосистемах, которые смогут обеспечить защиту даже в условиях появления квантовых компьютеров.

Список использованных источников:

1. Актуальные киберугрозы в странах СНГ 2023-2024 // АО «Позитив Текнолоджиз». URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/.

2. TOTP (Time-based one-time Password algorithm) // Habr. URL: https://habr.com/ru/articles/534064/.

3. OpenVPN, о котором вы так мало знали // Habr. URL: https://habr.com/ru/articles/435802/.

Panov N.S.
Nosov Magnitogorsk State Technical University, Magnitogorsk

Scientific supervisor:
Kholodilov S.S.
Nosov Magnitogorsk State Technical University, Magnitogorsk

ENHANCE YOUR VPN SERVER SECURITY WITH TWO-FACTOR AUTHENTICATION

Abstract. The article provides a comprehensive analysis of the cryptographic and architectural foundations of two-factor authentication in VPN

networks. The mechanisms for implementing temporary one-time passwords, HMAC authentication and extended authentication protocols are studied, and a comparative analysis of the effectiveness of various two-factor authentication methods against modern cyber threats is carried out. Particular attention is paid to the cryptographic strength of temporary one-time passwords and their integration with existing VPN solutions.
Keywords: VPN, two-factor authentication, TOTP, cryptographic protocols, information security.

УДК 004.8

Полышева А.К.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шафиков М.Р.
Уфимский университет науки и технологий, Уфа

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. В рамках данного исследования, акцент сделан на применении технологий искусственного интеллекта для оптимизации задач управления информационной безопасностью. Рассматриваются средства защиты информации отечественного рынка, которые используют в своей работе алгоритмы машинного обучения и искусственного интеллекта. Описываются встроенные модули систем.
Ключевые слова: искусственный интеллект, угроза, безопасность, система защиты информации, машинное обучение.

Реализация эффективной защиты информации сталкивается с серьезными трудностями, поскольку современные кибернетические угрозы характеризуются высоким уровнем сложности, а спектр используемых технологий – большим разнообразием [3]. Все более проблематичным становится выполнение таких важных задач, как постоянный контроль, аналитическая обработка данных и оперативное реагирование на инциденты.

Существуют разнообразные подходы к обнаружению киберугроз, в том числе сигнатурный анализ, а также методы, которые основаны на нейросетях и алгоритмах машинного обучения. Хотя сигнатурный анализ, базирующийся на сравнении с известными образцами, позволяет быстро находить определенные типы атак, он не эффективен против новых угроз [3].

Если сигнатурный анализ основывается на известных признаках угроз, то машинное обучение использует анализ больших данных для обнаружения аномального поведения, которое может свидетельствовать о готовящейся атаке. Нейросети повышают эффективность этого анализа, позволяя распознавать более сложные и адаптивные угрозы.

Тем не менее окончательная оценка ситуации и принятие мер остаются в компетенции человека.

Отечественный сектор IT и информационной безопасности активно внедряет инструменты на основе машинного обучения и искусственного интеллекта.

Для обнаружения и предотвращения кибератак все чаще применяют искусственный интеллект в качестве прогностического инструмента. ИИ используется в антивирусном ПО для автоматизации реагирования на атаки, а также для анализа обширных массивов данных с целью выявления скрытых угроз и реализации множества других функций.

Использует искусственный интеллект и DLP-система «СёрчИнформ КИБ». Система включает программные модули. Можно выделить те, которые отвечают за распознавание лиц и личных устройств. Искусственный интеллект, в частности, для мониторинга активности персонала в сети Интернет и отображаемой на мониторах информации. В общей сложности «СёрчИнформ КИБ» насчитывает одиннадцать модулей [2].

Одним из преимуществ DLP-системы является модуль MonitorController, который позволяет собирать информацию о работающих процессах и посещаемых сайтах в момент создания снимка экрана. Это дает возможность получить полное представление о действиях пользователя за время сбора данных.

Еще одним важным дополнением является функция распознавания лиц, которая позволяет определить, кто именно находился за компьютером в момент потенциального нарушения. Функциональность данной программы позволяет выявлять случаи несанкционированного использования чужих ПК сотрудниками [2]. Программа позволяет установить личность пользователя, осуществившего вход в систему с использованием чужого компьютера, зафиксировать точную дату и время инцидента.

Подход, используемый для анализа данных в «СёрчИнформ КИБ», отличается от подхода InfoWatch. DLP-система InfoWatch для прогнозного анализа собираемых данных использует искусственный интеллект.

Предиктивная аналитика данных, собираемых системой Traffic Monitor, осуществляется с помощью инструмента InfoWatch Prediction. Этот инструмент использует технологии машинного обучения для выявления рискованных паттернов поведения сотрудников, что способствует повышению эффективности управления группами риска. При построении паттерна поведения сотрудника для анализа инструмент использует более 54 параметров и типов событий.

Основной задачей предиктивной аналитики является автоматический анализ данных с целью выявления рискованных паттернов (цепочек событий) и своевременное оповещение о любых отклонениях от нормы. Такой подход позволяет службе безопасности работать на упреждение, прогнозируя риски, а не реагируя на уже произошедшие инциденты.

Согласно статистике, в двух случаях из трех сотрудники, покидающие компанию, копируют данные для последующего использования в новой организации. InfoWatch Prediction автоматически выявляет подобную активность, сопоставляет ее с другими признаками и выдает предупреждение об аномальном поведении.

Алгоритмы машинного обучения анализируют различные параметры, включая активность в рабочей переписке, посещение ресурсов по трудоустройству, время начала и окончания рабочего дня, и информируют о любых отклонениях от стандартного паттерна поведения конкретного работника.

В табл. 1 приведены ключевые характеристики двух решений для проведения сравнительного анализа.

Таблица 1

Сопоставление решений DLP

Характеристика/Система	«СёрчИнформ КИБ»	InfoWatch Traffic Monitor
Сертификат соответствия ФСТЭК	да	да
Реестр отечественного ПО	включен	включен
Возможность интеграции со СКУД системой	да	нет
Просмотр рабочего стола в режиме реального времени	да	нет

SIEM-система MaxPatrol – еще один пример. С помощью поведенческого анализа, который базируется на машинном обучении, такая система способна распознавать даже ранее неизвестные атаки, а также те, которые подразумевают обход стандартных правил корреляции.[1]

Ниже, на рис. 1, изображен процесс обнаружения угроз в MaxPatrol.

Рис. 1. Обнаружение угроз в SIEM-системе MaxPatrol

Определение границ ответственности интеллектуальных систем является ключевым вопросом при разработке искусственного интеллекта. Искусственный интеллект в России пока не признан субъектом права. Как следствие, в законодательстве отсутствуют нормы, регулирующие ответственность за возможные происшествия с его участием [3]. Процесс внедрения машинного обучения и искусственного интеллекта, хотя и управляется разработчиками, может приводить к результатам, которые трудно предугадать.

Ключевым условием для выявления потенциальных ошибок в функционировании искусственного интеллекта является эффективный контроль. Для этого процесс принятия решений должен быть понятен и прозрачен [3]. Высокое качество работы во многом зависит от анализа метаданных. В связи с этим, ключевым приоритетом при разработке является создание условий для безопасного хранения данных и предотвращения их несанкционированного использования, а также защиты от неправомерного доступа.

Список использованных источников:

1. Зачем SIEM-системе машинное обучение: реальные сценарии использования // ITSec.Ru: [сайт]. URL: https://www.itsec.ru/articles/zachem-siem-sisteme-mashinnoe-obuchenie-realnye-scenarii-ispolzovaniya (дата обращения: 06.03.2025).

2. Обзор DLP-системы «Контур информационной безопасности SearchInform» // Компания «Безопасность бизнеса» – Создание комплексных систем безопасности предприятий и объектов: [сайт]. URL: https://www.bugshunt.ru/info/articles/obzor-dlp-sistemy-kontur-informatsionnoy-bezopasnosti-searchinform-chast-1-osnovnye-funktsii-sistemy/ (дата обращения: 19.03.2025).

3. Повышение уровня безопасности ИТ-систем с помощью технологий ИИ // Secuteck.Ru: [сайт]. URL: https://www.secuteck.ru/articles/povyshenie-urovnya-bezopasnosti-it-sistem-s-pomoshchyu-tekhnologij-ii (дата обращения: 21.03.2025).

Polysheva A.K.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shafikov M.R.
Ufa University of Science and Technology, Ufa

USING MODERN TECHNOLOGIES WITH MACHINE LEARNING ALGORITHMS TO IMPROVE THE EFFECTIVENESS OF THE INFORMATION PROTECTION SYSTEM

Abstract. In the context of this article, the focus is on the application of artificial intelligence technologies to optimize information security management tasks. It considers information security tools of the Russian information security products, which use machine learning and artificial intelligence algorithms in their work. It describes the built-in modules of the systems.

Keywords: artificial intelligence, threat, security, information protection system, machine learning.

УДК 004.056

Савелиев Я.И.
Поволжский государственный университет телекоммуникаций и информатики, Самара

Научный руководитель:
Пугин В.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара

ОПЫТ ВНЕДРЕНИЯ РЕД ОС В ПГУТИ, ПОДХОДИТ ЛИ ОН ДЛЯ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?

Аннотация. В данной статье представлены различные методы защиты информации, реализованные в операционной системе РЕД ОС. Предлагаются вариации использования данной операционной системы и приводятся реальные примеры работы с РЕД ОС в учебном заведении

Ключевые слова: РЕД софт, информационная безопасность, отечественное ПО, РЕД ОС, Иинформационная безопасность вуза.

Современные информационные системы требуют надежных механизмов защиты. Операционная система РЕД ОС, разработанная компанией «РЕД СОФТ», предлагает широкий спектр инструментов и технологий. РЕД ОС – это российская операционная система общего назначения на

основе ядра Linux. Она предназначена для использования на серверах и рабочих станциях в различных организациях, включая государственные учреждения и коммерческие предприятия. В 2022 г. в целях реализации политики импортозамещения руководство Поволжского Государственного Университета Телекоммуникаций и Информатики (ПГУТИ) приняло решение о переводе ИТ-инфраструктуры вуза на российскую операционную систему. Проект также был нацелен на повышение опыта использования студентами и преподавательским составом вуза отечественного софта, а также его интегрирование в образовательный процесс [1]. Система имеет современные механизмы защиты информации, вот некоторые из них:

Принудительный контроль доступа: внедрение системы принудительного контроля доступа (SELinux) в операционной системе РЕД ОС в ВУЗе обеспечивает усиленную безопасность путем ограничения действий пользователей и программ в системе. SELinux реализует концепцию обязательного контроля доступа (MAC), где доступ к ресурсам системы регулируется на основе заранее определенных политик безопасности, что предотвращает несанкционированный доступ и минимизирует риски от уязвимостей в программном обеспечении [2]. Это особенно важно в образовательных учреждениях, где обрабатываются персональные данные студентов и сотрудников, а также проводятся экзамены и тестирования, требующие строгого контроля доступа к ресурсам.

Система изолированного запуска приложений: в рамках этой системы применяется Firejail – инструмент для изолированного запуска приложений, который ограничивает доступ программ к системным ресурсам, повышая безопасность и предотвращая потенциальные угрозы. Кроме того, используются технологии Flatpak и Snap, обеспечивающие создание изолированных сред для приложений, что способствует безопасному и контролируемому запуску программного обеспечения. Эти меры направлены на защиту данных и ресурсов университета, обеспечивая безопасную эффективную работу пользователей.

Flatpak и Snap предоставляют из себя системы для упаковки и распространения приложений в изолированных контейнерах. Они позволяют устанавливать и запускать приложения вместе со всеми необходимыми зависимостями, обеспечивая их работу независимо от основной системы. Это упрощает установку программ и повышает их безопасность.

Аудит: в РЕД ОС реализована система аудита, обеспечивающая мониторинг и регистрацию событий, связанных с безопасностью системы. В рамках этой системы используются различные механизмы, направленные на мониторинг и анализ событий [3]. В ПГУТИ аудит используется для защиты интеллектуальной собственности, предотвращения утечек конфиденциальной информации и обеспечения соответствия внутренним и внешним требованиям безопасности.

Контроль целостности системы: в ВУЗе контроль целостности системы может быть использован для защиты данных и обеспечения безопасности ИТ-инфраструктуры. Этот механизм позволяет отслеживать изменения в файловой системе и предотвратить несанкционированное изменение важных данных, таких как учебные материалы, отчеты, и личная информация студентов и сотрудников. Используя инструменты контроля, вуз может оперативно выявлять любые изменения в системе, что помогает вовремя обнаружить потенциальные угрозы или попытки несанкционированного доступа.

Организация доменной структуры: в университете использование доменной структуры РЕД ОС позволяет эффективно управлять учетными записями пользователей и контролировать доступ к различным сервисам. С помощью интеграции с решениями на базе FreeIPA и Samba DC [4], учебные заведения могут централизованно администрировать систему, отслеживать действия пользователей и обеспечивать единую авторизацию

Интеграция с криптографическими средствами: в ПГУТИ система РЕД ОС также используется для защиты данных с помощью отечественных криптографических средств, таких как КриптоПро CSP и VipNet CSP. Эти средства позволяют накладывать электронные подписи, шифровать и расшифровывать документы в соответствии с российскими стандартами безопасности, что необходимо для защиты конфиденциальной информации студентов и сотрудников [5]. Поддержка защищенных веб-соединений и совместимость с аппаратными средствами расширяют возможности защиты данных и обеспечивают безопасный доступ к государственным и корпоративным ресурсам.

Защищенный комплекс программ электронной почты: использование почтового клиента Evolution, встроенного в РЕД ОС, позволяет обезопасить переписку с помощью протоколов SSL, TLS и STARTTLS [3]. Шифрование с использованием GPG и S/MIME гарантирует защиту содержимого сообщений от несанкционированного доступа, что особенно важно при передаче научных данных, результатов экзаменов и других конфиденциальных материалов.

РЕД ОС остается актуальным решением в сфере информационной безопасности. Система сертифицирована ФСТЭК (Федеральная служба по техническому и экспортному контролю), что особенно важно для ВУЗов Минцфры, к которым и относится ПГУТИ [6]. Система оснащена современными криптографическими средствами и поддерживает отечественные стандарты защиты, что позволяет строить надежные информационные системы в условиях постоянного роста киберугроз.

Благодаря базе на Linux, РЕД ОС отличается гибкостью и надежностью, что облегчает ее интеграцию с другими решениями в области ИБ. Практический опыт эксплуатации в ПГУТИ показывает, что система успешно адаптируется под различные задачи, обеспечивая комплексную за-

щиту данных. Это делает отечественную ОС конкурентоспособным инструментом для создания эффективных и безопасных информационных систем.

Список использованных источников:

1. РЕД софт: сайт. URL: https://redos.red-soft.ru/about/news/novosti/pguti-rabotaet-na-red-os/ (дата обращения 22.04.2025).
2. Вермейлен С. Администрирование системы защиты SELinux. М.: ДМК Пресс, 2020.
3. База знаний РЕД ОС: сайт. URL: https://redos.red-soft.ru/base/ (дата обращения: 22.04.2025).
4. Samba.руководство системного администратора 2001 СПб: Электрон. библиотека. URL: https://clck.ru/3LbMqq (дата обращения 22.04.2025).
5. КриптоПро руководство: документ. URL: https://clck.ru/3LbN7A (дата обращения 22.04.2025).
6. Презентация РЕД СОФТ: документ. URL: https://clck.ru/3LbaTU (дата обращения 22.04.2025).

Saveliev Y.I.
Volga Region State University of
Telecommunications and Informatics, Samara

Scientific supervisor:
Pugin V.V.
Volga Region State University of
Telecommunications and Informatics, Samara

THE EXPERIENCE OF IMPLEMENTING RED OS IN PSUTI, IS IT SUITABLE FOR SOLVING INFORMATION SECURITY PROBLEMS?

Abstract. This article presents various information protection methods implemented in the RED OS operating system. Variations of the use of this operating system are proposed and real examples of working with the operating system in an educational institution are given.

Keywords: RED soft, Information security, domestic software, RED OS, Information security of the university.

УДК 004

Ситков А.С.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Миронова Н.Г.
Уфимский университет науки и технологий, Уфа

КАК ЗЛОУМЫШЛЕННИКИ ИСПОЛЬЗУЮТ ГЕНЕРАТИВНЫЙ ИИ ДЛЯ СЛОЖНЫХ КИБЕРАТАК И ПЕРСПЕКТИВНЫЕ МЕХАНИЗМЫ ЗАЩИТЫ/ПРОТИВОДЕЙСТВИЯ ПОДОБНЫМ АТАКАМ

Аннотация. Генеративный искусственный интеллект (ИИ) становится важным инструментом в руках злоумышленника при сложных кибератаках на конфиденциальную информацию. Рассмотрены вопросы применения механизмов защиты/противодействия данному типу кибератак с использованием ИИ.

Ключевые слова: информация, риски информационной безопасности, генеративный искусственный интеллект.

Среди кибератак на критическую информационную инфраструктуру особую группу составляют подготовленные целевые (Targeted Attack) и продвинутые кибератаки (APT, Advanced Persistent Threat, «развитая устойчивая угроза»). Подобные атаки растянуты во времени, сложнее обнаруживаются традиционными подходами к защите информации, а для подготовки APT-атак (в т. ч. сбора и обработки информации о жертве, тактики долгого сокрытия своего присутствия злоумышленника в системе организации-жертвы) злоумышленники все чаще применяют возможности инструментов на основе моделей машинного обучения. Стоит отметить, что сложные кибератаки – это высокотехнологичные атаки на информационные системы организаций или отдельных лиц, отличающиеся высокой степенью организации, сложности и подготовленности.

Генеративный ИИ (GenAI) представляет собой категорию технологий, основанных на искусственных нейронных сетях, которые умеют самостоятельно разрабатывать новый контент: текстовые материалы и различный мультимедийный контент. Среди прочих возможностей GenAI:

– трансформация текста в устную речь, синтез голоса, изготовление аудиозаписей и обработка звуковых сигналов (примеры подобных сервисов – Tacotron от Google, Lyrebird, WaveNet);

– моделирование/имитация физических процессов, поддержка в проведении научных исследований, в т. ч. анализ массивов данных, создание научных гипотез в некоторых отраслях науки;

– генерация по словесному описанию программного кода.

Эти возможности привлекают внимание не только добросовестных исследователей и специалистов, но и злоумышленников, стремящихся использовать GenAI для проведения сложных и масштабных кибератак, поэтому по мере развития и роста доступности ИИ-технологий возрастает важность поиска эффективных методов противодействия подобным угрозам (что представляет как задачу разработки ИИ-инструментов безопасности – так и задачу нормативно-правового регулирования разработки ИИ-технологий).

Как генеративный ИИ используется злоумышленниками?

1. Предварительный этап подготовки сложной кибератаки. Машинное обучение помогает злоумышленнику автоматизировать и ускорить этап сбора информации об объекте атаки, агрегируя и обрабатывая большие массивы открытых данных (профили сотрудников в социальных сетях, доменные имена, IP-адреса, медиа-истончики), формируя полную картину об организации.

2. Автоматизация, ускорение и упрощение разработки вредоносных программ с помощью сервисов на основе генеративных моделей (в т. ч. уникальные экземпляры вирусов, трудно идентифицируемые традиционными антивирусами, оперативно адаптирующиеся к изменениям в системах безопасности). Имитационное моделирование с использованием машинного обучения может для имитации разных вариантов проведения атак на конкретную инфраструктуру, обхода имеющихся средств защиты, чтобы найти лучшую (для атакующего) стратегию атаки. Признаками APT-атаки может служить увеличение в определенный период количества обнаруженных бэкдор-троянов [1, с. 88–89] (т. к. злоумышленники применяют бэкдоры в виде троянских программ для поддержания непрерывного доступа к системе, даже если учетные данные были скомпрометированы или изменены).

3. Социальная инженерия играет важнейшую роль в продвинутых APT (Advanced Persistent Threats) кибератаках, так как именно человеческий фактор зачастую становится слабым местом в самой сильной системе безопасности. Социальная инженерия используется на этапе предварительного сбора информации и первоначального проникновения в инфраструктуру организации. Применение злоумышленниками ИИ в социальной инженерии многообразно: генеративные нейросети позволяют злоумышленникам легко создавать убедительные фишинговые сообщений, фальшивые документы и профили в социальных медиа, фейковые фото и видео для ввода в заблуждение через соцсети и мессенджеры для сбора конфиденциальных данных, для персонализированных и результативных атак.

4. Нарушения конфиденциальности. Генеративные модели могут быть использованы для синтеза личных данных, что позволяет злоумышленникам получать доступ к конфиденциальной информации, такой как банковские данные, медицинские записи и личные идентификаторы. Эти

сведения впоследствии могут быть использованы для кражи личных данных или шантажа.

5. Манипулирование информацией. Возможности генеративного ИИ позволяют автоматически создавать ложный контент, искажающий действительность. К примеру, сфабрикованные фотографии, видеозаписи или тексты могут распространяться с целью дезинформации общественности или подрыва репутации компаний и частных лиц [2, с. 101].

Один из путей противодействия этим технологиям – совершенствование инструментов для выявления материалов, сгенерированных GenAI инструментами; зачастую они дают высокий процент ложных срабатываний, но могут быть полезны для распознания фейковых сообщений, применяемых хакерами для ввода в заблуждение атакуемых с целью получения от них конфиденциальной информации, для фишинга. Некоторые из таких инструментов: ИИ-детектор Smodin (глубокий анализ контента с применением машинного обучения); многофункциональный инструмент для обнаружения текста, изображений и программного кода, сгенерированных ИИ – Copyleaks (также на базе искусственного интеллекта) [3, с. 97]; детектор дипфейков, созданных с помощью нейросети StyleGAN; программа FakeBuster для выявления дипфейков во время трансляций в Zoom и Skype, сервис Deepware (scanner.deepware.ai) для обнаружения дипфейковых видео; в свое время Агентство DARPA (США) инициировало разработку программно-аппаратного комплекса Semantic Forensics (SemaFor, https://semanticforensics.com/ от PAR Government Systems Corp.) для автоматизированного семантического анализа текстов, аудио, изображений, видео в реальном времени, с учетом атрибутов фейков, а в России АНО «Диалог регионы» в 2023 г. запустил платформу мониторинга аудиовизуальных дипфейков «Зефир» (но подобные инструменты не всегда доступны для специалистов по ИБ и ограниченно пригодны для реализации нужд ИБ организаций) [4, с. 191]. Еще один метод противодействия - использовать проверенные каналы связи для деловой информацией, систематически перепроверять достоверность поступающей по цифровым каналам информации, прежде чем принимать важные решения; проявлять настороженность при запросах на предоставление конфиденциальной информации (например, при совершении финансовых операций и т. п.). Также необходимо использовать актуальные версии антивирусных программ, брандмауэров и других защитных механизмов; регулярно проводить тесты безопасности, чтобы убедиться в эффективности защитных мер.

Для проникновения в систему при реализации сложной кибератаки злоумышленники применяют широкий спектр приемов и технологий: эксплуатация ранее неизвестных уязвимостей (в т. ч. в ПО, используемом в информационной системе жертвы), манипуляция поведением с помощью социальной инженерии; точечные фишинговые атаки; использование уязвимости удаленного включения файлов (RFI); внедрение вредоносного

кода через RFI или SQL-инъекции; атаки с использованием межсайтового скриптинга; заражение систем вредоносным программным обеспечением путем физического доступа; использование туннелирования через систему доменных имен и др.

Одним из основных методов противодействия методами социальной инженерии и атаками, использующими генеративные модели, является информирование сотрудников организаций и общественности, повышение квалификации персонала. Важно, чтобы люди осознавали возможные риски, могли отличать настоящие данные от поддельных и придерживались правил безопасного поведения в сети.

Применение генеративного ИИ открывает широкие перспективы для бизнеса, науки, культуры и образования, однако одновременно порождает проблемы безопасности информации и информационные риски, связанные с авторским правом, приватностью и возможностью манипуляций информацией.

Список использованных источников:

1. Жданов А.А. Автономный искусственный интеллект: учебное пособие / А.А. Жданов. 5-е изд. (эл.). М.: Лаборатория знаний, 2024. 362 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/387629 (дата обращения: 19.04.2025).

2. Кацов И. Искусственный интеллект на предприятии: руководство / И. Кацов; перевод с англ. В. С. Яценкова. М.: ДМК Пресс, 2024. 710 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/456725 (дата обращения: 19.04.2025).

3. Правовое и этическое регулирование роботизации и внедрения искусственного интеллекта (ИИ): материалы научно-практической конференции с международным участием 18 марта 2022 г.: материалы конференции. М.: Дело РАНХиГС, 2022. 132 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/468215 (дата обращения: 19.04.2025).

4. Миронова Н.Г. Технологии медиабезопасности: методы противодействия фейк-контенту в цифровых медиа // Экономика и право: проблемы, стратегия, мониторинг: колл. монография. Чебоксары: «Издательский дом «Среда», 2024. 197 с. Элект. версия. URL: https://www.elibrary.ru/item.asp?id=78769542.

Sitkov A.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Mironova N.G.
Ufa University of Science and Technology, Ufa

HOW ATTACKERS USE GENERATIVE AI FOR COMPLEX CYBER ATTACKS AND PROMISING PROTECTION MECHANISMS/COUNTERING SUCH ATTACKS

Abstract. Generative artificial intelligence (AI) is becoming an important tool in the hands of an attacker in complex cyber attacks on confidential information. The article discusses the application of protection/counteraction mechanisms for this type of cyberattacks using AI.

Keywords: information protection rights, information security risks, generative artificial intelligence, APT (Advanced Persistent Threat).

УДК 004

Фатеев Р.Р., Шигапов А.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Юнусова Д.С.
Уфимский университет науки и технологий, Уфа

ВЫЯВЛЕНИЕ ПОТЕНЦИАЛЬНЫХ УГРОЗ СО СТОРОНЫ ВНУТРЕННИХ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ИХ ДЕЙСТВИЙ И ИСТОРИИ РАБОТЫ

Аннотация. В статье рассматривается методика выявления потенциальных угроз информационной безопасности, исходящих от внутренних пользователей организации. Основное внимание уделяется анализу их поведенческой активности, мониторингу действий и истории работы в корпоративной системе. Применение поведенческих моделей и систем выявления аномалий позволяет своевременно обнаруживать подозрительную активность, предотвращая утечки данных и внутренние атаки. Также обсуждаются современные программные решения, направленные на усиление защиты от инсайдерских угроз и формирование профилей пользователей на основе их цифрового поведения.

Ключевые слова: инсайдерские угрозы, информационная безопасность, поведенческий анализ, мониторинг активности, выявление аномалий.

Выявление потенциальных угроз со стороны внутренних пользователей требует систематического мониторинга их действий в информационных системах с использованием специализированных инструментов. Например, системы SIEM (Security Information and Event Management) собирают и анализируют логи активности, такие как попытки входа в систему, запросы к базам данных, копирование файлов на внешние носители или отправка данных через корпоративную почту [1]. Аномалии выявляются через сравнение текущей активности с историческими данными: если сотрудник из отдела маркетинга, обычно работающий с клиентскими презентациями, начинает обращаться к финансовым базам данных, это фиксируется как подозрительное поведение. Дополнительно используются метрики, такие как объем скачиваемых данных (например, более 1 ГБ за сессию) или частота доступа к критическим системам вне рабочего времени. Ключевым инструментом является анализ поведения на основе систем UEBA (User andEntityBehavior Analytics) [2].

Для повышения точности детекции угроз интеграция с системами DLP (Data LossPrevention) позволяет отслеживать действия, непосредственно связанные с утечкой данных. Например, DLP-правила могут автоматически фиксировать инциденты по шаблонам: «копирование более 10 файлов, помеченных как конфиденциальные, за 24 часа» или «пересылка документов с ключевыми словами «коммерческая тайна» через личную почту». Дополнительный уровень контроля обеспечивают системы PAM (Privileged Access Management), которые мониторят действия администраторов, имеющих доступ к критическим ресурсам, и блокируют несанкционированные изменения настроек, такие как модификация прав доступа [3].

На этом этапе устанавливаются критерии для оценки и классификации переменных, необходимых для анализа риска, а также критерии самой оценки рисков. Методы, используемые для этого, уже на стадии определения контекста задаются в общих чертах. Согласно действующим стандартам ISO, термин «оценка риска» включает три подпроцесса: идентификацию риска, анализ риска и оценку риска. Процесс оценки рисков повторяется и улучшается по мере поступления новой информации. Это может привести к расширению области применения или изменению контекста, если будут выявлены новые типы рисков [4].

Рассмотрим работу нейронной сети для решения задачи выявления потенциальных угроз на примере датасета, содержащего информацию о сотрудниках, их действиях и психометрических характеристиках.

Датасет содержит информацию:

- о сотрудниках (уникальный идентификатор пользователя, роль в организации (например, ITAdmin, Engineer), отдел (например, Finance, R&D), проекты, в которых участвует пользователь);
- о событиях входа и выхода пользователей из системы (идентификатор пользователя, дата и время события, тип активности, идентификатор компьютера);

- о веб-активностях сотрудников (идентификатор пользователя, дата и время запроса, посещенный URL, тип активности, содержимое запроса);
- об операциях с файлами (идентификатор пользователя, дата и время операции, имя файла, тип действия, флаг записи на съемный носитель);
- о подключении внешних устройств (идентификатор пользователя, дата подключения, путь к данным на устройстве, тип действия);
- о личностных характеристиках пользователей (Открытость, Добросовестность, Экстраверсия, Доброжелательность, Невротизм);
- о доступе к файлам-ловушкам (идентификатор пользователя, имя файла-приманки).

Для обнаружения аномалий использовалсяавтоэнкодер - нейронная сеть, которая обучается воссоздавать нормальное поведение пользователей. После обучения вычисляется среднеквадратичная ошибка восстановления (MSE) для каждого пользователя, классифицируя тех, чья ошибка превышает 97-й перцентиль, как потенциальные угрозы. ИИ также генерирует визуализации: график потерь обучения и диаграмму рассеяния, где аномалии выделены красным, что помогает аналитикам быстро идентифицировать подозрительных пользователей.

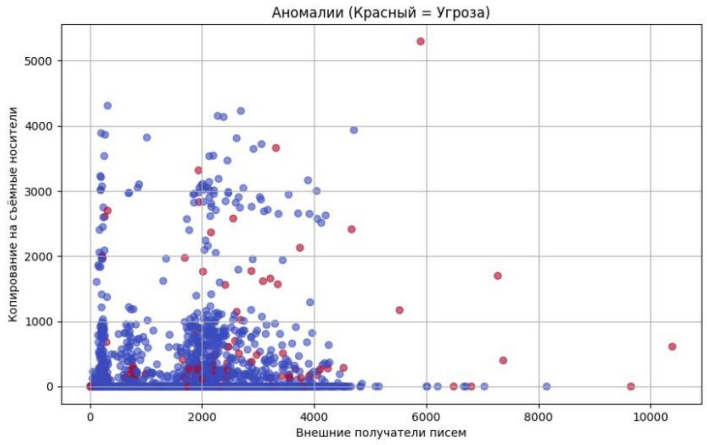

Рис. 1. Тепловая карта собранная по сделанной базе

Нейронная сеть показывает высокую эффективность в нахождении угроз (F1- мера примерно 0,85 на тестовых данных). Внедрение изменений политики безопасности на основе полученных рекомендаций позволяет существенно снизить риски и улучшить защиту данных.

Выявление потенциальных угроз со стороны внутренних пользователей является критически важной задачей в системе обеспечения информационной безопасности любой организации. Применение поведенческого анализа, мониторинга активности и систем обнаружения аномалий позволяет не только своевременно выявлять инсайдерские угрозы, но и снижать риски утечки конфиденциальной информации. Комплексный подход, включающий технологии машинного обучения, постоянную оценку цифровых профилей пользователей и интеграцию средств информационной аналитики, обеспечивает высокий уровень защиты и устойчивость корпоративной среды к внутренним атакам.

Список использованных источников:

1. Исхаков А.Ю., Гайдук К. К вопросу о реализации алгоритмов выявления внутренних угроз с применением машинного обучения // Вестник СибГУТИ. 2022. № 4 (60). URL: https://cyberleninka.ru/article/n/k-voprosu-o-realizatsii-algoritmov-vyyavleniya-vnutrennih-ugroz-s-primeneniem-mashinnogo-obucheniya (дата обращения: 20.04.2025).
2. Корниенко С.В., Пантюхина А.В. Методика выявления потенциальных внутренних нарушителей информационной безопасности // Интеллектуальные технологии на транспорте. 2023. № 2 (34). URL: https://cyberleninka.ru/article/n/metodika-vyyavleniya-potentsialnyh-vnutrennih-narushiteley-informatsionnoy-bezopasnosti (дата обращения: 20.04.2025).
3. Морданов М.А. Система контроллинга как основа эффективного управления рисками деятельности отечественных авиакомпаний // Этап. 2020. № 6. URL: https://cyberleninka.ru/article/n/sistema-kontrollinga-kak-osnova-effektivnogo-upravleniya-riskami-deyatelnosti-otechestvennyh-aviakompaniy (дата обращения: 20.04.2025).
4. Черных Л.В., Горбунова В.Б. Актуальные угрозы обеспечения экономической безопасности в киберпространстве // Вестник молодежной науки. 2022. № 3 (35). URL: https://cyberleninka.ru/article/n/aktualnye-ugrozy-obespecheniya-ekonomicheskoy-bezopasnosti-v-kiberprostranstve(дата обращения: 20.04.2025).

Fateev R.R., Shigapov A.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yunusova D.S.
Ufa University of Science and Technology, Ufa

DETECTION OF POTENTIAL THREATS FROM INTERNAL USERS BASED ON THEIR ACTIONS AND WORK HISTORY

Abstract. This article presents a methodology for detecting potential information security threats originating from internal users of an organization. The focus is on analyzing behavioral activity, monitoring actions, and evaluating user work history within corporate systems. The use of behavioral models and anomaly detection systems allows for timely identification of suspicious activity, thereby preventing data leaks and internal attacks. The paper also discusses modern software solutions aimed at enhancing protection against insider threats and building user profiles based on their digital behavior.

Keywords: insider threats, information security, behavioral analysis, activity monitoring, anomaly detection.

УДК 004

Хафизова Л.Ф.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

СОВРЕМЕННЫЕ УГРОЗЫ И УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАСТИ ОРГАНИЗАЦИОННОЙ ЗАЩИТЫ

Аннотация. Статья посвящена анализу современных угроз и уязвимостей информационной безопасности в области организационной защиты. С развитием технологий и цифровизации бизнеса, компании сталкиваются с растущими рисками, связанными с утечкой конфиденциальной информации, кибератаками, внутренними угрозами и другими проблемами.

Ключевые слова: информация, информационная безопасность, угрозы, организационные угрозы, уязвимости, организационные уязвимости, информационные технологии, защита информации, организационная защита.

Угрозы информационной безопасности (ИБ) часто являются следствием уязвимостей в самой системе защиты информации. Такие уязвимости могут возникать по разным причинам. Это могут быть случайные ошибки, допущенные специалистами при разработке или сопровождении программного обеспечения, а могут быть и намеренные действия – например, целенаправленная кража данных или внедрение вредоносного кода.

При рассмотрении таких угроз принято разделять их на две категории – технические и организационные. Технические включают в себя физиические и программные уязвимости на информационные системы. Организационные же, в свою очередь, связаны прежде всего с человеческим фактором – с действиями персонала и управленческими просчетами.

Несмотря на такую классификацию, во многих существующих подходах к анализу ИБ основное внимание уделяется именно технологическим аспектам безопасности. Организационные угрозы, напротив, часто остаются в стороне – их влияние недооценивают или не всегда принимают в расчет. Однако практика показывает, что именно они могут представлять серьезную опасность для устойчивости и защищенности ИС. Поэтому специалисты по информационной безопасности все чаще разрабатывают собственные классификации угроз, в которых наравне с техническими подробно рассматриваются и организационные риски.

Организационные угрозы могут проявляться в разных формах. Иногда это внешнее влияние на сотрудников со стороны третьих лиц – давление, манипуляции или даже угрозы. Воздействие может быть, как физическим, так и психологическим. Нередко бывает так что угрозы исходят от самих сотрудников – намеренно или по ошибке. Кто-то может сознательно нарушать правила безопасности, действуя из личной заинтересованности или по заказу, а кто-то, не имея достаточной квалификации или по невнимательности, допускает серьезные ошибки.

Таким образом, можно сказать, что организационные угрозы либо направлены на персонал, либо реализуются через него. Сотрудники компании могут быть как объектом, так и источником угроз информационной безопасности. Именно поэтому человеческий фактор играет ключевую роль в обеспечении устойчивой и надежной защиты информации.

Физическое воздействие на сотрудников предполагает применение силы или угроз, чтобы заставить человека – напрямую или через посредников – раскрыть конфиденциальную информацию либо нарушить работу процессов внутри компании. Подобные инциденты относятся к категории серьезных нарушений и, как правило, становятся предметом расследования со стороны службы ИБ, а также правоохранительных органов.

На практики существует более гибкая угроза, но не менее опасная – психологическое воздействие. В этой категории широко используются такие методы, как шантаж, подкуп, манипулирование, а также приемы социальной инженерии. Все они направлены на то, чтобы повлиять на поведение человека и получить от него нужные действия или информацию без применения технических средств.

Особенно стоит отметить методы социальной инженерии. Они представляют особую опасность, поскольку базируются на умении злоумышленника использовать человеческую психологию. Часто достаточно лишь изучить структуру компании, позвонить в отдел, представиться сотрудником или поставщиком – и можно получить доступ к внутренним данным. Нередко злоумышленники прибегают к хитростям: несанкционированный доступ в компьютер, через незакрытые USB-порты или возможности подключения устройств.

Именно поэтому в организациях все чаще внедряют системы контроля и управления доступом (СКУД). Эти меры позволяют ограничить вход на территорию, вести учет передвижений и минимизировать риски, связанные с социальной инженерией.

Среди методов психологического давления выделяется манипуляция – умелое управление поведением человека, при котором у него формируется желание действовать в интересах другого, зачастую вопреки своей воле. Такие воздействия могут быть неочевидны, но в итоге приводят к выполнению нежелательных действий.

Психологическая атака – это еще более активный способ влияния. Злоумышленник может создать у человека состояние замешательства, срочности или сильного впечатления, чтобы временно отключить логическое мышление. В результате сотрудник действует автоматически и совершает поступки, которых от него добивается атакующий.

Однако ни одна атака не осуществляется в пустоте – всегда требуется определенная уязвимость. Чтобы провести успешную информационную атаку, злоумышленник должен использовать слабое место в системе. Если эти уязвимости своевременно устранять или минимизировать, вероятность реализации угроз заметно снижается.

Особенно уязвимыми считаются организационные слабости, связанные с человеческим фактором. Они могут проявляться как через сотрудников компании, так и через подрядчиков или партнеров. Чаще всего это недостаток подготовки, слабая мотивация, нехватка контроля и отсутствующие знания по ИБ.

Если сотрудники не обучены, не знают правил или не понимают последствий своих действий – они становятся легкой мишенью. А при отсутствии внутреннего мониторинга, риски возрастают в разы, ведь инциденты остаются незамеченными.

Чтобы устранить подобные уязвимости, организациям необходимо регулярно обучать персонал, знакомить их с актуальными методами защиты, повышать квалификацию. Также большую роль играет нематериальная мотивация: сотрудник должен понимать, что его труд ценится не только финансово, но и на уровне признания со стороны руководства. Это помогает формировать ответственное отношение к вопросам безопасности.

Помимо этого, необходимо создать систему мониторинга, которая позволит отслеживать соблюдение правил и выявлять отклонения. Каждый сотрудник должен понимать свои обязанности, знать регламенты и последствия их нарушения.

Современные организационно-технические мероприятия должны включать в себя:

1. Контроль доступа к информации с помощью установления прав доступа к системе и данным.
2. Шифрование информации для защиты от несанкционированного доступа.
3. Аудит безопасности для мониторинга действий пользователей и выявления угроз.
4. Резервное копирование данных для обеспечения возможности восстановления после инцидентов.

Однако с техническими мерами не стоит забывать организационно-правовые. Это разработка внутренних политик безопасности, инструкций и регламентов. Важно, чтобы все сотрудники знали, что можно, а что нельзя,

и кто за что отвечает. Такие документы должны быть не формальностью, а реально работающим инструментом.

К сожалению, на практике основная проблема – это отсутствие элементарных документов. Если в компании нет утвержденной политики ИБ, сотрудники действуют на свое усмотрение. А это уже прямая дорога к инцидентам.

В целом, можно сказать, что организационные уязвимости чаще всего возникают не из-за отсутствия средств, а из-за отсутствия порядка, контроля и культуры безопасности. Если наладить эти процессы – ввести регламенты, обучить сотрудников, назначить ответственных – уровень защиты значительно возрастет.

Важно помнить: большинство организационных угроз связаны с персоналом. Это может быть, как внешнее воздействие, так и действия самих сотрудников. Поэтому эффективная защита информации невозможна без вовлечения людей, их подготовки, осознанности и ответственности.

Список использованных источников:

1. Гаценко О.Ю. Защита информации: основы организационного управления: учебное пособие / О.Ю. Гаценко. Сентябрь, 2011. 228 с.
2. Романов О.А. Организационное обеспечение информационной безопасности: учебник для высших учебных заведений / О.А. Романов. М.: Академия, 2008. 192 с.
3. Семкин С.Н. Основы организационного обеспечения информационной безопасности объектов информатизации: учебное пособие / С.Н. Семкин. М.: Гелиос АРВ, 2010. 185 с.
4. Стрельцов А.А. Организационно-правовое обеспечение информационной безопасности: учебник для высших учебных заведений / А.А. Стрельцов. М.: Академия, 2008. 248 с.

Khafizova L.F.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

MODERN THREATS AND VULNERABILITIES OF INFORMATION SECURITY IN THE FIELD OF ORGANIZATIONAL PROTECTION

Abstract. The article is devoted to the analysis of modern threats and vulnerabilities of information security in the field of organizational protection. With the development of technology and digitalization of business, companies

face increasing risks associated with confidential information leaks, cyber attacks, internal threats and other problems.

Keywords: information, information security, threats, organizational threats, vulnerabilities, organizational vulnerabilities, information technology, information security, organizational protection.

УДК 004

Шайнурова А.Г.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ С ПОМОЩЬЮ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Расследование инцидентов информационной безопасности с помощью искусственного интеллекта становится важным инструментом при решении задач защиты информации. В статье рассмотрены некоторые подходы при расследовании инцидентов информационной безопасности с помощью искусственного интеллекта, а также этапы проведения данного типа расследований.

Ключевые слова: информация, информационная безопасность, инциденты информационной безопасности, искусственный интеллект.

В эпоху цифровизации информация приобрела статус важнейшего актива, обеспечение информационной безопасности (ИБ) которой выдвигается на важное место в деятельности организации. Но оперативное и безошибочное определение инцидентов в сфере кибербезопасности предполагает обработку огромных массивов данных. В настоящее время искусственный интеллект (ИИ) может помочь в данном вопросе и предоставить эффективные средства для автоматизации и улучшения процесса расследования инцидентов ИБ. Более того, ИИ способен прогнозировать вероятные угрозы и разрабатывать защитные стратегии. Так, автоматизированные системы контроля и анализа данных с применением ИИ могут оперативно обнаруживать нетипичную активность в сетевой среде и сигнализировать о потенциальной опасности.

На данный момент искусственный интеллект способствует автоматизации этапа анализа и выявления угроз при расследовании инцидентов ИБ, применяя методы машинного обучения для анализа обширных объемов данных, таких как сетевой трафик, журналы серверов, электронные почты и прочие источники. Благодаря алгоритмам

машинного обучения, ИИ способен выявлять аномалии и нестандартную активность в сети, устанавливать взаимосвязи между различными событиями и идентифицировать возможные угрозы [1]. Также, ИИ может быть использован для формирования профилей пользователей и определения типовых моделей поведения, что позволяет выявлять отклонения и предотвращать потенциальные атаки злоумышленников еще до их реализации. В целом, автоматизация процессов анализа и выявления угроз в ходе расследования инцидентов значительно повышает результативность работы специалистов по информационной безопасности и обеспечивает более надежную защиту от угроз [2].

Этапы расследования инцидентов ИБ с использованием ИИ могут включать в себя:

1. Сбор и анализ данных. ИИ может помочь в этом процессе, используя алгоритмы машинного обучения для выявления аномалий и закономерностей в данных. Методами анализа данных может являться машинное обучение, анализ сетевого трафика и др.
2. Обнаружение угроз. ИИ может использоваться для мониторинга и анализа различных источников данных, включая журналы событий, сетевой трафик и поведение пользователей для выявления потенциальных угроз и уязвимостей.
3. Реагирование на инцидент. ИИ может автоматически инициировать процессы реагирования, такие как изоляция зараженных узлов, блокировка учетных записей и восстановление резервных копий. Основные шаги реагирования на инцидент: изоляция зараженного узла; блокировка учетных записей; восстановление резервных копий; уведомление заинтересованных сторон об инциденте ИБ.
4. Глубокий анализ и прогнозирование. ИИ может помочь в определении причины инцидента, его последствий и возможных мер профилактики.
5. Профилактика и улучшение мер безопасности. Полученные знания используются для улучшения общей стратегии безопасности организации. ИИ может предложить рекомендации по улучшению политики безопасности, настройке систем защиты и обучению сотрудников [3].

Для создания системы предотвращения инцидентов ИБ с применением искусственного интеллекта необходимо собирать и обрабатывать обширные массивы информации об инцидентах и слабых местах в защите информации. Эти сведения служат основой для обучения алгоритмов машинного обучения, способных анализировать и выявлять закономерности в подобных атаках. В дальнейшем, система использует накопленные знания для прогнозирования вероятных атак и разработки защитных стратегий. Специалисты в области информационной безопасности могут опираться на эти модели для определения наиболее актуальных угроз и принятия упреждающих мер. Более того, система способна автоматически обнаруживать и блокировать данные инциденты. Алгоритмы машинного

обучения анализируют данные о поведении пользователей и параметрах безопасности, автоматически реагируя на выявление подозрительной деятельности. Система для расследования инцидентов ИБ должна обладать интегрированным и многофункциональным характером, охватывая следующие возможности:

– отслеживание сетевого трафика и визуализация сетевой активности: выявление и анализ всех сетевых операций с целью обнаружения аномалий или потенциальных угроз, а также предоставление графического отображения трафика в сети с выделением уязвимых зон для оперативного обнаружения рисков;

– анализ рисков: предварительная оценка угроз с применением технологий искусственного интеллекта;

– оповещение на ранней стадии появления угроз: распознавание типичных или повторяющихся угроз с использованием анализа данных и машинного обучения для превентивных мер;

– активная и актуальная защита информации: обеспечение адаптации состояния безопасности в зависимости от текущей ситуации;

– оперативное расследование инцидентов: оценка и отчетность по инцидентам, их детальное расследование и предоставление полной информации для принятия мер и усиления защиты сети.

Одним из решений, позволяющим проводить расследования инцидентов с применением ИИ, является KIRA (Kaspersky Investigation and Response Assistant). Это специализированная платформа, разработанная компанией «Лаборатория Касперского», предназначенная для автоматизированного расследования инцидентов информационной безопасности. Она сочетает в себе передовые технологии искусственного интеллекта и экспертные знания специалистов по информационной безопасности, обеспечивая эффективное и быстрое реагирование на инциденты. KIRA способна автоматически обрабатывать большие объемы лог-файлов, выявляя подозрительные события и аномалии. Платформа поддерживает различные форматы лог-файлов, включая Syslog, Windows Event Logs и другие стандартные форматы. Платформа оснащена интерфейсами для интеграции моделей машинного обучения, позволяющими настраивать и применять собственные аналитические модели для конкретных сценариев. KIRA предоставляет возможность настройки платформы под специфику каждого клиента, позволяя добавлять уникальные сценарии и правила для детекции инцидентов. Интерфейс KIRA интуитивно понятен и удобен для пользователей различного уровня подготовки. Даже начинающие специалисты могут эффективно использовать платформу благодаря встроенным подсказкам и инструкциям. KIRA поддерживает стандарты обмена информацией об угрозах (STIX/TAXII), что упрощает интеграцию с внешними системами управления информацией и событиями безопасности (SIEM) [4].

Технологии искусственного интеллекта значительно улучшают выявление угроз ИБ, осуществляя анализ больших массивов данных и распознавая трудноуловимые взаимосвязи. Эти системы способны идентифицировать вредоносное программное обеспечение, даже если оно замаскировано сложным шифрованием. Автоматизированное реагирование на выявленные угрозы не только ускоряет процесс, но и облегчает работу специалистов по безопасности. Прогнозирование возможных атак и своевременное принятие мер предосторожности позволяют предотвратить их возникновение. Помимо этого, искусственный интеллект способствует более эффективному расследованию инцидентов, устанавливая взаимосвязи между различными событиями и автоматизируя процесс анализа отчетной документации.

Список использованных источников:

1. Исмагилова А.С. Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей / А.С. Исмагилова, Н.Д. Лушников // Инженерный вестник Дона. 2024. № 1(109). С. 178–188.

2. Жданов А.А. Автономный искусственный интеллект: учебное пособие / А.А. Жданов. 5-е изд. (эл.). М.: Лаборатория знаний, 2024. 362 с. Электрон. версия. URL: https://e.lanbook.com/book/387629 (дата обращения: 20.04.2025).

3. Кацов, И. Искусственный интеллект на предприятии: руководство / И. Кацов; перевод с англ. В.С. Яценкова. М.: ДМК Пресс, 2024. 710 с. Электрон. версия. URL: https://e.lanbook.com/book/456725 (дата обращения: 20.04.2025).

4. Терлецкий А.С. Нейронные сети и искусственный интеллект: основы нейронных сетей на языке Python: учебно-методическое пособие / А.С. Терлецкий, Е.С. Терлецкая. Липецк: Липецкий ГПУ, 2023. 76 с. Электрон. версия. URL: https://e.lanbook.com/book/439343 (дата обращения: 20.04.2025).

Shaynurova A.G.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

INVESTIGATION OF INCIDENTS USING ARTIFICIAL INTELLIGENCE

Abstract. Investigation of information security incidents using artificial intelligence is becoming an important tool in solving information security

problems. The article discusses some approaches to investigating information security incidents using artificial intelligence, as well as the stages of conducting this type of investigation.

Keywords: information protection rights, information security, information security incidents, artificial intelligence.

УДК 004.8

Шушакова А.А.
Уфимский университет науки и технологий, Уфа

Миронова Н.Г.
Уфимский университет науки и технологий, Уфа

НЕКОТОРЫЕ НОВЫЕ ВИДЫ АТАК НА МОБИЛЬНЫЕ И IOT-УСТРОЙСТВА С ПРИМЕНЕНИЕМ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ И ПРОТИВОДЕЙСТВИЕ ИМ

Аннотация. В статье рассматриваются некоторые новые виды атак на мобильные и IoT-устройства с использованием технологии машинного обучения и способы противодействия.

Ключевые слова: информация, кибератаки на мобильные устройства, машинное обучение в информационной безопасности, IoT-устройства.

Мобильные устройства оказались привлекательной целью для атак как непосредственно на эти устройства, так и на инфраструктуру, с которой они взаимодействуют. По мере развития интеграции технологий искусственного интеллекта с мобильной электроникой (например, т. н. периферийный ИИ) для злоумышленников открываются новые возможности, а для специалистов по защите информации растет сложность управления безопасностью. Помимо ставших уже традиционными атак на мобильные устройства с помощью вредоносного ПО, социальной инженерии и фишинга, киберпреступники стали применять инновационные подходы с использованием технологий машинного обучения, такие как создание персонализированных видео-, аудио- и фото-дипфейков для обмана пользователей [1]. Голосовые ассистенты мобильных устройств и системы распознавания речи становятся уязвимыми, позволяя злоумышленникам подменять голоса легальных пользователей, чтобы получить доступ [2] к личной информации пользователя.

Согласно данным исследования McAfee (компании по разработке антивирусного ПО), проведенного в 2024 г. среди 7000 респондентов, каждый четвертый сталкивался с использованием голосовых дипфейков или знает людей, которые столкнулись с этой проблемой. 72 % из

опрошенных испытывают ежедневное беспокойство по поводу мошенничества с использованием данного типа мошенничества.

Однако атаки с использованием технологий машинного обучения не ограничиваются только мобильными устройствами. IoT-устройства, в силу своей распространенности и часто недостаточной защищенности, также становятся все более привлекательной целью для злоумышленников, использующих машинное обучение для автоматизации поиска уязвимостей и повышения эффективности атак.

Хотя атаки с использованием IoT-ботнетов не являются принципиально новыми (например, печально известный ботнет Mirai, появившийся в 2016 г., использовал сотни тысяч уязвимых устройств для организации масштабных DDoS-атак) [3], наблюдается их эволюция. Злоумышленники используют методы машинного обучения для повышения живучести и эффективности ботнетов. В 2023 г. компания Nokia сообщила о 300-процентном росте DDoS-атак с использованием IoT-устройств в первой половине года. Ботнеты стали основой 90 % сложных многовекторных атак.

Многие IoT-устройства базируются на встроенных системах с легко анализируемой прошивкой. APT-группы все чаще используют автоматизированные инструменты, работающие на основе машинного обучения, для выявления уязвимостей в прошивках IoT-устройств [4]. Это позволяет им находить и эксплуатировать как известные, так и ранее неизвестные уязвимости.

Для эффективной защиты IoT-устройств от атак с использованием машинного обучения необходим многоуровневый подход:

Своевременная установка обновлений безопасности от производителя устройства критически важна для устранения известных уязвимостей. Многие производители, такие как Nest, Philips Hue и Samsung SmartThings, регулярно выпускают обновления для своих устройств.

Замена стандартного пароля, установленного производителем, на сложный и уникальный пароль, а также включение двухфакторной аутентификации, где это возможно, значительно повышает уровень безопасности.

Проведение регулярных проверок безопасности IoT-устройств и сети с использованием специализированных инструментов и сервисов.

Общая тенденция, наблюдаемая как в IoT-экосистеме, так и в сфере мобильных устройств, – это активное использование злоумышленниками машинного обучения для повышения эффективности, персонализации и адаптации атак к конкретным жертвам и условиям. Одним из примеров такого использования является применение генеративных нейросетей для создания дипфейков [5], используемых в атаках социальной инженерии, нацеленных на мобильные устройства.

Для детектирования фейк-изображений применяются методы машинного обучения, программы анализа подлинности видео; для опознания фальшивых профилей, с которых могут размещаться фейки,

применяются ИИ-инструменты поведенческого анализа. Например, программа FakeBuster для выявления дипфейков во время трансляций в Zoom и Skype, сервис Deepware (scanner.deepware.ai) распознает дипфейк-видео. К несовершенствам нейросетевой технологии распознания фейков относятся значительный процент ложных срабатываний и ограниченная эффективность (так, детекторы ИИ-контента, обученные искать определенные маркеры фейков, плохо справляются с другими типами фейков), а также малодоступность ИИ-инструментов распознавания фейков для большинства пользователей мобильных устройств [6]. Резкие движения актера, использующего цифровую дипфейк-маску, могут привести к ее «слетанию», движение рук перед лицом также может создать искажения [7]. Целесообразна избирательность в цифровом дистанционном общении, пониженное доверие сообщениям и звонкам с незнакомых номеров. Есть сервисы и фактчекинговые сайты для проверки подлинности присылаемых через соцсети фото- и видеоматериалов. Так есть сервис Deepfake Detector от Microsoft для детектирования фейковых фото и видео; в России АНО «Диалог регионы» в 2023 г. запустил платформу мониторинга аудиовизуальных дипфейков «Зефир» с помощью «алгоритмической оценки и анализа с помощью искусственного интеллекта», эффективность которой, по заявлению разработчиков, порядка 80 % [6].

Защита мобильных и IoT устройств должна строиться на комплексном подходе, учитывающем современные научно-технические достижения в области защиты информации. Важно быть в курсе новых видов угроз и принимать превентивные меры заранее до того, как нанесен ущерб пользователю.

Список использованных источников:

1. Исмагилова А.С. Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей / А.С. Исмагилова, Н.Д. Лушников // Инженерный вестник Дона. 2024. № 1(109). С. 178–188.

2. Бондаренко И.С. Информационная безопасность: учебник / И.С. Бондаренко. М.: МИСИС, 2023. 254 с. Электрон. версия. URL: https://e.lanbook.com/book/360344.

3. Будущее киберугроз: IoT-устройства в центре внимания хакеров // Anti-malware. URL: https://www.anti-malware.ru/analytics/ ThreatsAnalysis/ IoT-devices-attacks#part31 (дата обращения: 19.04.2025).

4. Прогнозы по продвинутым угрозам на 2025 г. // SecureList. URL: https://securelist.ru/ksb-apt-predictions-2025/111090/.

5. Конструктивное использование DeepFake технологии // Хабр. URL: https://habr.com/ru/articles/503038/.

6. Миронова Н.Г. Технологии медиабезопасности: методы противодействия фейк-контенту в цифровых медиа // Экономика и право: проблемы, стратегия, мониторинг: колл. монография. Чебоксары:

«Издательский дом «Среда», 2024. 197 с. Электрон. версия. URL: https://www.elibrary.ru/item.asp?id=78769542.

7. Прохорова О.В. Информационная безопасность и защита информации: учебник для СПО / О.В. Прохорова. 6-е изд., стер. СПб.: Лань, 2025. 124 с. Электрон. версия. URL: https://e.lanbook.com/book/445250.

Shushakova A.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Mironova N.G.
Ufa University of Science and Technology, Ufa

SOME NEW TYPES OF ATTACKS ON MOBILE AND IOT DEVICES USING MACHINE LEARNING TECHNOLOGIES AND COUNTERACTIONS TO THEM

Abstract. The article discusses some new types of attacks on mobile devices using machine learning technology and ways to counter them.

Keywords: information protection, cyber attacks on mobile devices, machine learning in information security, IoT devices.

УДК 004

Якупова И.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Миронова Н.Г.
Уфимский университет науки и технологий, Уфа

ПРОБЛЕМЫ БЕЗОПАСНОСТИ IOT-УСТРОЙСТВ И НАПРАВЛЕНИЯ ЗАЩИТЫ ИНТЕРНЕТА ВЕЩЕЙ

Аннотация. Развитие технологии IoT сопровождается ростом угроз; недостаточная исходная защищенность, слабые и устаревшие протоколы работы IoT- и IIoT-устройств, размытость зоны контроля киберфизических систем с использованием IoT это факторы риска, которые сложно закрыть при традиционном подходе к управлению безопасностью предприятия или кибер-объекта. В статье выполнен анализ проблем безопасности IoT-устройств и изложены пути и методы снижения рисков ИБ, связанных с IoT-устройствами.

Ключевые слова: IoT, интернет вещей, кибербезопасность.

Применение IoT-устройств стало массовым явлением, образуя киберфизические системы умных городов, транспорта и зданий, медицинского интернета вещей и промышленного (IIoT). Так, «IoT Analytics» [3] оценил количество устройств интернета вещей в мире в 2024 г. в 18,8 млрд, в 2025 г. их ожидается 21,5 млрд, а к 2030 г. прогнозируется от 32,1 млрд [4] до 41,1 млрд [3] устройств IoT. При этом активно развивается интеграция с IoT технологий искусственного интеллекта (например, т.н. периферийного ИИ), создавая новые неочевидные уязвимости и усложняя процессы управлениях безопасностью.

Большинство IoT-устройств штатно слабо защищены или не защищены вовсе, а их широкая распространенность привлекает киберхакеров, которые ищут способы эксплуатировать их уязвимости. Технологические цифровые инновации в производстве сопровождаются развитием промышленного интернета вещей, что делает промышленность основной мишенью для атак вредоносного ПО. В 2022 г. число кибератак на IoT выросло на 400 % по сравнению с предшествующим периодом (согласно отчету исследовательской группы Zscaler ThreatLabz [1]); к середине 2024, по оценке Zscaler ThreatLabz, количество лишь заблокированных атак на IoT увеличилось на 45 % по сравнению с 2023 [5], причем эти атаки шли преимущественно на промышленный IoT (в 3 раза чаще, чем на другие отрасли [1]). Анализ методов атак на IoT устройства свидетельствует о разнообразии эксплуатируемых уязвимостей IoT. Комбинирование традиционных и «инновационных» приемов позволяет хакерам обходить стандартные средства защиты и эксплуатировать вновь возникающие уязвимости на стыке технологий. Хакеры применяют вредоносы, в т. ч. шифровальщики (часто это Mirai и Gafgyt), используя уязвимости прошивок и недостаточную защиту операционных систем мобильных платформ, уязвимые протоколы передачи данных [6] (при этом для интернета вещей характерно большое разнообразие протоколов передачи данных, что усложняет защиту и требует стандартизации в этой сфере). Уязвимостями служат и ошибки в конфигурации систем безопасности (в т. ч. облачных центров хранения и обработки производственных данных), позволяя кибервзломщикам получать с помощью IoT доступ к критическим элементам киберфизической инфраструктуры. Хакеры используют социальную инженерию, ИИ-технологии для поиска уязвимостей, длительные скрытые (APT) кибератаки. Среди угроз IoT – эксплуатация аппаратных уязвимостей и недостатков прошивки, DDoS-атаки, заражение вирусами с последующим отказом в обслуживании и поломке оборудования киберфизических систем. Целью киберпреступников является проникновение в промышленные сети, искажение данных, получением контроля над управляющими командами в исполнительных устройствах, изменение в прошивках и программах промоборудования, и как итог – аварии. Стремительная эволюция методов и числа атак на IoT актуализируют проблематику кибербезопасности интернета вещей и

цифровой инфраструктуры с использованием IoT и ИИ, и важность комплексного подхода к защите информации предприятий и другой критической инфраструктуры, постоянное совершенствование методов и средств защиты, новых стратегий противодействия таким угрозам.

Анализ эксплуатируемых уязвимостей IoT показывает, что основными проблемами являются: уязвимости программного обеспечения, базовые настройки IoT-устройств без учета угроз, отсутствие надежной аутентификации, незащищенный выход в интернет, ошибки в конфигурации систем безопасности, отсутствие (или слабые схемы) шифрования данных, когда это необходимо; неправильная настройка сетевых протоколов упрощает [7] злоумышленникам доступ. В результате IoT-устройства оказываются заражены и используются в качестве входных точек для ботнет-атак на корпоративную инфраструктуру. При этом для IoT-устройств, подключаемых через интернет откуда угодно, нет контролируемой зоны, которую можно было бы изолировать традиционными средствами безопасности, что затрудняет контроль и удаленное управление устройством в случае его некорректной работы. IoT-устройства, как правило, невозможно непосредственно защитить, как компьютер или телефон, наложенными средствами защиты от киберугроз, поскольку операционная система если и есть – то упрощенная и несовместимая с традиционными средствами защиты, а разработчики «умных вещей», как правило, не закладывают в них функций информационной безопасности.

Многообразие угроз, реализуемых через IoT, указывает на важность системного подхода к кибербезопасности в отношении IoT-устройств, однако защита IoT на практике нередко возможна лишь на уровне каналов связи (сети, протоколов и средств коммуникации устройства с хранилищем или платформой, использующей данные IoT). Для управления трафиком от IoT к облаку или платформе применяются IoT-шлюзы, в функционал которых входит фильтрация данных от IoT, перевод протоколов, отправка данных в облако или интрасети, а также отслеживание событий безопасности; некоторые IoT шлюзы (например, продукт Kaspersky IoT Secure Gateway [2] предоставляют дополнительный слой защиты и возможность удаленного администрирования IoT-устройствами. Использование защищенных протоколов передачи данных, мониторинг событий безопасности для выявления аномалий помогают отслеживать и нейтрализовать атаки и повышает уровень защиты IoT-устройств. Стратегия защиты требует реализации принципов «нулевого доверия» при выстраивании системы защиты, продуманного конфигурирования настроек безопасности устройств, а также, когда это возможно для IoT, регулярности обновления ПО, применения антивирусов, усиления аутентификации, применения средств доверенной загрузки, средств анализа аномального поведения IoT-устройств. Угрозы для разных IoT-устройств в цифровой инфраструктуре (например, предприятия) должны быть описаны в модели угроз, а меры

защиты IoT-устройств изложены в политике безопасности, как это делается для «традиционных» компонентов объекта.

Список использованных источников:

1. Gandhi V. 2023 ThreatLabz Report Indicates 400 % Growth in IoT Malware Attacks // info.zscaler.com: [сайт]. URL: https://www.zscaler.com/blogs/security-research/2023-threatlabz-report-indicates-400-growth-iot-malware-attacks.

2. Kaspersky IoT Secure Gateway // kaspersky.ru: [сайт]. URL: https://www.kaspersky.ru/enterprise-security/kaspersky-iot-secure-gateway.

3. State of IoT 2024: Number of connected IoT devices growing 13 % to 18.8 billion globally // iot-analytics.com: [сайт]. URL: https://iot-analytics.com/number-connected-iot-devices.

4. Vailshery L. S. Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033 // statista: [сайт]. URL: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

5. Zscaler ThreatLabz 2024 Mobile, IoT, & OT Threat Report. URL: https://newsletter.radensa.ru/wp-content/uploads/2024/12/threatlabz-mobile-iot-ot-report.pdf.

6. Григорьев А.А., Орлов В.С. Современные методы киберзащиты мобильных и IoT-устройств. Новосибирск: Наука, 2021. 310 с.

7. Соколова Е.В. Критическая инфраструктура и информационная безопасность. М.: Инфра-М, 2022. 280 с.

Yakupova I.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Mironova N.G.
Ufa University of Science and Technology, Ufa

IOT DEVICE SECURITY PROBLEMS AND WAYS TO PROTECT THE INTERNET OF THINGS

Abstract. The development of Internet of Things technologies against the backdrop of a growing threat; reverse initial security, weak and outdated protocols for the operation of IoT and IIoT devices, and the blurring of the control zone of cyber-physical systems using IoT are risk factors that are difficult to close with the traditional approach to ensuring the security of enterprise or cyber facility management.The article analyzes the security issues of IoT devices and outlines ways and methods for reducing information security risks associated with IoT devices.

Keywords: IoT, Internet of Things, Cybersecurity.

УДК: 004.056

Янов И.В.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

Научный руководитель:
Киреева Н.В.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

ОСНОВНЫЕ УГРОЗЫ И УЯЗВИМОСТИ ВЕБ-САЙТОВ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

Аннотация. Статья посвящена вопросам обеспечения безопасности веб-сайтов в условиях роста числа кибератак. Рассматриваются основные угрозы, включая уязвимости по классификации OWASP Top-10, методы защиты – двухфакторная аутентификация, WAF, пентест и обучение персонала. Подчеркивается важность комплексного подхода к обеспечению безопасности, сочетающего технические и организационные меры для защиты данных и репутации организации.

Ключевые слова: веб-сайт, безопасность, кибератака, OWASP, WAF, 2FA, пентест, уязвимости, шифрование, мониторинг.

С бурным развитием интернета веб-ресурсы стали неотъемлемой частью бизнеса, коммуникаций и досуга. Однако их широкое распространение сделало их привлекательной целью для киберпреступников. Веб-сайты зачастую содержат личные и финансовые данные пользователей, а также могут использоваться как плацдарм для дальнейших атак.

В условиях стремительного роста числа угроз обеспечение информационной безопасности веб-приложений приобретает критическое значение. По данным компании Positive Technologies, в 2024 г. на веб-ресурсы в России приходилось 45 % всех кибератак, что показывает остроту проблемы [4].

Проект OWASP (Open Web Application Security Project, открытый проект безопасности веб-приложений [2]) формирует рейтинг наиболее опасных уязвимостей веб-приложений. В последнем OWASP TOP-10 (2021) были выделены следующие типовые угрозы:

1. Нарушение контроля доступа (Broken Access Control).
2. Ошибки в реализации криптографических алгоритмов (Cryptographic Failures).
3. Инъекционные уязвимости (Injection).
4. Недостатки архитектуры и проектирования (Insecure Design);
5. Неправильная настройка конфигураций (Security Misconfiguration);
6. Использование устаревших или небезопасных компонентов.
7. Проблемы с идентификацией и аутентификацией.

8. Нарушение целостности данных и ПО.

9. Отсутствие надлежащего логирования и мониторинга;

10. Подделка серверных запросов (SSRF).

Среди типичных векторов атак можно выделить SQL-инъекции, XSS (межсайтовый скриптинг), CSRF (подделка запросов), а также ошибки в настройке безопасности. SQL-инъекции позволяют злоумышленникам вмешиваться в работу баз данных и извлекать конфиденциальную информацию. XSS-атаки позволяют внедрять вредоносный код в страницы сайта, а CSRF может принудить пользователя к нежелательным действиям от имени его учетной записи.

Исследования компании «Лаборатория Касперского» показывают увелечение количества кибератак на веб-приложения на 38 % в 2024 г. по сравнению с предыдущти годом. Данные пресс-службы компании «Лаборатория Касперского» показывают, что в 2024 г. было официально зафиксировано 1 811 562 707 кибератак (при этом учитывались атаки с участием вредоносного ПО, предотвращенные средствами защиты и специалистами данной компании). Кроме того, специалисты компании указали, что за 2024 г. увеличился на 12 % объем инцидентов, которые связаны с различными мобильными устройствали с операционной системой Android.

Безопасность веб-сайтов обеспечивается с использованием различных методов. Одним из таких является применение двухфакторной аутентификации (2FA) и ориентирование на сложные пароли. Совместно это дает ощутимое снижение возможности несанкционнированного доступа, риск взлома.

Исследования Group-IB показывают, что 2FA снижает вероятность взлома учетных записей на 60 %, но не может являться абсолютной защитой. Совсеменные тенденции и технологии подрахумевают различные способы обхода данных мер защиты:

1. Социальная инженерия: манипулирование пользователями для получения доступа.

2. OAuth: использование уязвимостей открытой авторизации.

3. Brute-Force: перебор кодов, особенно при использовании устаревшего оборудования.

4. Сгенерированные ранее токены: использование резервных кодов, полученных злоумышленником.

5. Cookie-файлы сеанса: их кража для доступа к аккаунту без пароля и 2FA. Злоумышленники используют перехват сеансов, межсайтовый скриптинг, вредоносное ПО или Evilginx для захвата cookie.

6. SIM-jacking: получение контроля над номером телефона жертвы для перехвата SMS-кодов 2FA через обращение к оператору или вредоносные приложения.

Вследствии этого возникает необходимость применять дополнительные способы защиты, чтобы использование 2FA было эффективным [3], в

частности, рекомендуется не передавать временные или запасные ключи защиты; создавать сложные, из множества символов пароли; применять уникальные пароли для важных аккаунтов, использовать физические ключи для аутентификации; изучать популярныи тактики социальной инженерии. Говоря о сложности пароля, нужно понимать, что длина и сложность пароля это разные грани вопроса. Исследования Национального института стандартов и технологий (NIST) [4] показывают, что сложные пароли с различными символами и длинные пароли надежнее и риск взлома значительно ниже, например, взлом 12-символьного пароля занимает около 2000 лет.

Важной составляющей устранения уязвимостей являются регулярные обновления CMS, плагинов и серверного ПО. Качественные и частые обновления CMS показывают поддержку разработчиками и устранение уязвимостей.

С помощью веб-аппликационного межсетевого экрана (WAF) анализируется трафик и блокируются подозрительные запросы, что предотвращает SQL-инъекции и XSS-атаки. Данные пользователей защищаются протоколом HTTPS и шифрованием баз данных. WAF представляет комплексное решение, позволяющее защитить веб-приложения от множества атак, таких как: SQL-инъекции; XSS; инъекция локальных или удаленных файлов (LFI/RFI); PHP-инъекции; боты; Brute-force и другие методы перебора данных.

Важным методом защиты веб-сайтов от киберугроз, выявляющий уязвимости до злоумышленников, является тестирование на проникновение (пентест). По способу доступа к системе выделяют: внешние тесты и внутренние тесты. В зависимости от объема информации, доступной пентестеру, существуют разные подходы к пентесту:

- Black Box (черный ящик): полное отсутствие информации (имитация атаки извне);
- White Box (белый ящик): полный доступ к архитектуре (глубокий анализ);
- Gray Box (серый ящик): частичное знание системы (баланс между реализмом и полнотой).

Тестирование на проникновение является одной из ключевых мер обеспечения информационной безопасности веб-сайтов.

Другим значимым источником угроз информационной безопасности является человеческий фактор, приводящий к утечкам данных и взломам. Более трети инцидентов происходят из-за недостаточной осведомленности пользователей, использования ненадежных паролей и фишинга.

Для снижения рисков необходимо:

1. Регулярно обучать сотрудников основам кибербезопасности, используя практические примеры и актуальные данные об угрозах.

2. Внедрять технические средства, такие как многофакторная аутентификация и системы мониторинга, для минимизации ошибок и предотвращения несанкционированного доступа.

Обеспечение безопасности веб-сайтов требует комплексных мер, включая технические (WAF, шифрование, двухфакторная аутентификация) и организационные (мониторинг, тестирование, обучение сотрудников). С помощью комплексного подхода можно обеспечить минимизацию рисков и защитить данные пользователей и репутацию организации.

Вопросы обеспечения безопасности веб-сайтов требуют комплексного подхода, включающего как технические меры, так и организационные [1]. Активные и своевременные методы внедрения актуальных методов защиты, таких WAF, двухфакторная аутентификация и шифрование является крайне необходимым и своевременным решением на ряду с устранением текущих уязвимостей, связанных с увеличением числа кибератак. Использование постоянного мониторинга, тестирования и обучения сотрудников остаются основными и предпочтительными инструментами в борьбе с киберугрозами. Таким образом, только комплексный подход позволит минимизировать риски и защитить как данные пользователей, так и репутацию организации.

Список использованных источников:

1. Масалков А.С. Особенности киберпреступлений в России: инструменты нападения и защиты информации [Текст] / А.С. Масалков. М.: ДМК Пресс, 2018. 226 с.

2. Открытый проект обеспечения безопасности веб-приложений. URL: https://owasp.org/www-project-top-ten//.

3. NetSec.news. Портал для профессионалов и компаний, заинтересованных в защите своих данных и цифровых инфраструктур. URL: https://www.netsec.news/summary-of-the-nist-password-recommendations-for-2021/.

4. Positive Technologies. Лидер в области кибербезопасности, ориентированной на результат. URL:// https://global.ptsecurity.com/#analytics.

Yanov I.V.
Volga Region State University of
Telecommunications and Informatics, Samara

Scientific supervisor:
Kireeva N.V.
Volga Region State University of
Telecommunications and Informatics, Samara

THE MAIN THREATS AND VULNERABILITIES OF WEBSITES AND METHODS OF PROTECTION AGAINST THEM

Abstract. The article is devoted to the issues of ensuring the security of websites in the context of an increasing number of cyber attacks. The main threats are considered, including vulnerabilities according to the OWASP Top-10 classification, protection methods – two-factor authentication, WAF, pentest and staff training. The importance of an integrated approach to security is emphasized, combining technical and organizational measures to protect the organization's data and reputation.

Keywords: website, security, cyberattack, OWASP, WAF, 2FA, pentest, vulnerabilities, encryption, monitoring.

СЕКЦИЯ 3. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056

Аскарова Г.Ф.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. Статья посвящена анализу современных технологий защиты информации в условиях стремительного роста цифровизации и киберугроз. Рассматриваются причины уязвимости информационных систем, классификация методов защиты и перспективы внедрения интеллектуальных систем. Обоснована необходимость комплексного подхода, включающего правовую донастройку, обучение и интеграцию ИИ-технологий для эффективного управления информационной безопасностью.

Ключевые слова: информационная безопасность, киберугрозы, методы защиты, искусственный интеллект, правовое регулирование.

Открыть сегодня новостную ленту – и почти сразу наткнуться на очередной заголовок о масштабной утечке данных: от электронной почты госслужащих до всей переписки пользователей в мессенджерах. Что пугает больше всего – не масштаб потерь, а то, как рутинно воспринимаются такие события. В условиях, когда темпы цифровизации превосходят способность общества и государства выстроить устойчивую систему информационной безопасности, любая структура оказывается под угрозой. Уязвимость – это не аномалия, а новое «нормальное» состояние.

За последние три года, по данным Минцифры РФ, число инцидентов ИБ в критической инфраструктуре увеличилось на 48 %. Причем наибольшая доля пришлась на так называемые «человеческие» сбои – компрометация учетных данных, несанкционированный доступ через устаревшее ПО, ошибки в конфигурации систем [1]. Это подтверждают и наблюдения Мирсаидовой Н. С., которая подчеркивает: ключевые угрозы проистекают не только из-за внешнего вмешательства, но и из-за плохо настроенной архитектуры защиты самой системы [1].

Особо уязвимым слоем стали персональные данные – сырье для черного рынка и оружие в руках злоумышленников. Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006 г. хоть и декларирует защиту прав субъекта, но, по факту, практически не адаптирован к реалиям алгоритмического сбора и трансграничной передачи данных. Особенно это

заметно в контексте социальных сетей, где пользователь, соглашаясь с пользовательским соглашением, открывает доступ к своим предпочтениям, биометрии, геолокации, списку контактов. Как замечает Кириченко А.В., соцсети – это не просто площадки для общения, это настоящие платформы слежки, где безопасность сводится к «доверяй, но проверяй» [2].

Рынок, конечно, реагирует: появляются новые стандарты, решения, попытки регулирования. Однако пока технологическая и правовая базы развиваются с разной скоростью, уязвимость остается встроенной функцией цифровой среды. Это и есть та самая точка бифуркации, когда либо будут предприняты системные усилия по обновлению подходов, либо мы продолжим латать дыры на корабле, плывущем по штормящему морю данных.

Если упростить всю экосистему защиты информации до трех составляющих – технология, человек, регламент – то провалы случаются на каждом уровне. В техническом плане существует солидный арсенал: криптография, двухфакторная аутентификация, шифрование дисков, межсетевые экраны, антиспам-фильтры, DLP-системы, honeypot-ловушки и многое другое. Но какие из этих решений действительно работают?

Абдыраева Н.Р. классифицирует методы защиты по четырем направлениям: физические, аппаратные, программные и организационные [5]. Каждое из направлений имеет свою нишу. К примеру, аппаратные методы – это защита информации на уровне процессоров, линий связи, источников питания. Они почти не уязвимы для вирусов, но неэффективны против социальной инженерии. Программные методы включают антивирусы, фаерволы и операционные системы с встроенной политикой безопасности. Однако они уязвимы при наличии доступа администратора. Организационные меры – как ни странно – оказываются самыми слабыми: по данным Positive Technologies за 2023 г., в 76 % случаев причиной инцидентов становится именно игнорирование или отсутствие регламентов поведения с информацией.

Жидко Е.А. подчеркивает: одна из главных проблем в РФ – отсутствие продуманной информационной политики внутри организаций, особенно в малом и среднем бизнесе. Без нее все технические меры становятся декоративными [3]. Даже такие простые действия, как смена паролей раз в 90 дней или ограничение прав доступа по принципу необходимости, часто игнорируются.

Среди современных технологий на особом месте стоят системы биометрической идентификации и аутентификации [4]. Мирсаидова Н.С. подробно анализирует плюсы и минусы биометрических решений: с одной стороны, это высокая точность идентификации, с другой – почти полная невозможность «сменить» данные при утечке [1]. Кто-то может сменить пароль, но не сетчатку глаза.

Еще одна растущая область – шифрование. От шифра Цезаря до алгоритмов AES и RSA – прогресс очевиден. Но, как показал случай с

атакой на ColonialPipeline в США (май 2021 г.), наличие шифрования не спасает, если скомпрометирован ключ. Поэтому ключевое внимание в новых реалиях уделяется управлению ключами и их безопасному распределению.

Таким образом, эффективность технологии – это не только качество алгоритма, но и то, как она встроена в человеческий и регламентный контекст. Иначе – это бронежилет без солдата.

Применение искусственного интеллекта и поведенческой аналитики в защите информации – не из области фантастики. Уже сейчас в корпоративных системах начинают внедряться нейросетевые алгоритмы, способные распознавать аномалии в действиях пользователей, выявлять подозрительные паттерны доступа, прогнозировать потенциальные инциденты. Такие системы, как SIEM и UEBA, работают по принципу: «пользователь никогда не заходил в систему ночью – значит, сейчас есть риск компрометации». Это качественно новый уровень.

Сидлер М.О. акцентирует внимание на необходимости перехода от реактивных к проактивным мерам безопасности – и именно в этом направлении движутся интеллектуальные технологии [5]. Они не просто блокируют угрозы – они умеют учиться, адаптироваться, предугадывать.

Но вместе с этим появляются и новые вызовы. Например, насколько допустимо использовать поведенческий анализ без ведома самого пользователя? Где проходит граница между необходимой защитой и нарушением приватности? Законодательство пока не успевает реагировать. И если в ЕС действует GDPR с четкими принципами обработки данных, то в России регулирование фрагментарно и неполно. Закон № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации» содержит положения о защите, но не покрывает тонкости использования ИИ-систем в этой сфере [2].

При этом уровень угроз продолжает расти. Классический фишинг уже давно дополняется схемами социальной инженерии, а с развитием deepfake-технологий можно сгенерировать даже видеообращение «от начальника», просящее переслать конфиденциальный отчет. Кириченко А.В. подчеркивает: цифровая идентичность становится все менее защищенной, а уязвимости – все более психологическими [2].

Вывод здесь не в апокалипсисе, а в необходимости комплексного подхода. Без правовой донастройки, без образовательных программ, без усиления технологической суверенности говорить о надежной информационной защите – самообман. Сегодня надо не просто внедрять решения, а переосмыслять саму архитектуру цифровой безопасности. Потому что главная технология защиты информации – это мышление: системное, критическое и предвосхищающее.

Список использованных источников:

1. Мирсаидова Н.С. Основы информационной безопасности // Государственное управление. 2022. № 2 (56). С. 314–321.
2. Кириченко А.В. Защита информации в социальных сетях // Юридическая наука: история и современность. 2022. № 10. С. 78–83.
3. Жидко Е.А., Макаров Д.О., Небабин С.А. Защита информации с использованием информационных технологий // Информационные технологии в строительных, социальных и экономических системах. 2022. № 3 (29). С. 30–33.
4. Исмагилова А.С. Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей / А.С. Исмагилова, Н.Д. Лушников // Инженерный вестник Дона. 2024. № 1 (109). С. 178–188.
5. Абдыраева Н.Р., Турсунбаев Ф.С., Жумабай Уулу Н. Современные способы и средства защиты информации // Бюллетень науки и практики. 2022. Т. 8, № 4. С. 426–431.

Askarova G.F.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

INFORMATION PROTECTION TECHNOLOGIES

Abstract. The article examines modern technologies for information protection in the context of rapid digitalization and increasing cyber threats. It analyzes the causes of system vulnerabilities, classification of protection methods, and prospects for integrating intelligent systems. The paper highlights the need for a comprehensive approach, including legal adaptation, education, and implementation of AI technologies to ensure effective information security management.

Keywords: information security, cyber threats, protection methods, artificial intelligence, legal regulation.

УДК 003

Биктубаева К.С.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

К ВОПРОСУ ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация. Обеспечение информационной безопасности на объектах критической информационной инфраструктуры является одной из приоритетных задач государственных и частных организаций. Статья посвящена ключевым угрозам безопасности объектов критической информационной инфраструктуры. Особое внимание уделяется комплексной защите, сочетающей организационные, правовые, программные, аппаратные и технические меры защиты.

Ключевые слова: критическая информационная инфраструктура, информационная безопасность, защита информации, комплексная защита, угроза.

В условиях цифровизации обеспечение защиты объектов критической информационной инфраструктуры (КИИ) приобретает особую значимость. К ним относятся: информационные системы, информационно-телекоммуникационные сети, автоматизированные систему управления КИИ. Они являются важным элементом, которые поддерживают работу государства и бизнеса. Их защита требует комплексного подхода, включающего все средства защиты информации.

В соответствии с Федеральным законом от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (187-ФЗ), под КИИ понимается, объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов [1]. Значимый объект критической информационной инфраструктуры (КИИ) – это объект КИИ, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов КИИ.

Кибератаки на объекты КИИ представляют потенциальную угрозу и могут принимать различные формы. По данным исследований на 2024 г., отмечается рост сложности атак на 37 % по сравнению с предыдущим периодом. Согласно статистическим данным экспертов Anti-Malware, объекты КИИ подвергаются рискам трех типов: техническим, эксплуатационным и организационным. Каждый из этих факторов

представляет серьезную опасность для защиты критически важных объектов. Распространенные угрозы:

1. Наибольшую угрозу представляют несанкционированное получение доступа к защищаемой информации, которое может быть совершено как внешними злоумышленниками, так и инсайдером.

2. Опасность несут вирусные атаки с требованием выкупа, когда критически важная информация подвергается шифрованию с последующим шантажом. В 2024 г. наибольшую активность демонстрируют атаки с применением шифровальщиков. 51 % инцидентов в сегменте КИИ за второй квартал 2024 г. были связаны именно с этим типом вредоносного ПО [2].

3. Согласно данным НКЦКИ, распределенные атаки на отказ в обслуживании занимают значительную долю (16 % в 2023 г.) среди угроз, направленных на КИИ. Эти атаки входят в тройку самых распространенных наравне с вирусными программами и ошибками персонала [3].

4. Особое место занимают методы социальной инженерии. Фишинг и целевые рассылки с опасными вложениями сталь настолько изощренными, что 73 % успешных проникновений в систему КИИ начинаются именно с компрометации учетных данных через психологическое воздействие. Даже сложные многоступенчатые атаки начинаются с хищения учетных данных через методы социального воздействия.

Для эффективного противодействия современным угрозам безопасности объектов КИИ необходимо внедрение комплексной системы защиты, включая организационно-правовые, программно-аппаратные и технические меры [4].

Правовые меры составляют основу обеспечения безопасности объектов КИИ. Обязательным требованием является соблюдение положений ФЗ № 187 и соответствующих нормативных актов ФСТЭК № 235, 236, 239 и ФСБ России. Важном элементом правой защиты становится включение объектов в Реестр КИИ и полноценная реализация требований Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), являющаяся подразделением ФСТЭК, а также требований Национального координационного центра по компьютерным инцидентам (НКЦКИ), которая является подразделением ФСБ России [5]. Дополнительно каждая организация должна разрабатывать собственные нормативные документы, регламентирующие порядок обработки и защиты информации.

Технические меры защиты претерпевают значительные изменения благодаря внедрению инноваций. Перспективными направлениями являются системы на базе искусственного интеллекта (ИИ) для обнаружения аномалий, использование квантовой криптографии и развертывание облачных платформ безопасности с автоматическим реагированием [6].

Организационные меры включают три основных направления: регулярный аудит безопасности для выявления уязвимостей в системах, внедрение модели разграничения доступа с применением принципа

минимальных привилегий и многофакторной аутентификации, а также систематическое обучение персонала [7].

К программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры, относятся система защиты от несанкционированного доступа, межсетевые экраны, системы обнаружения и предотвращения вторжений (IDS/IPS), антивирусы, SIEM-системы, регулярное резервное копирование, обновление ПО и использование защищенных каналов связи [8], [9].

Кибератаки на КИИ прогрессируют, начиная от самых простых вирусов до сложных многоступенчатых атак. Эффективная защита объектов КИИ в современных условиях требует перехода от традиционных методов к адаптивным системам безопасности [10]. Реализация угроз может привести к прекращению или нарушению нормального функционирования значимого объекта, а также нарушению безопасности обрабатываемой информации (нарушению доступности, целостности, конфиденциальности информации). Законодательство дает основную базу для защиты, но без комплексного использования средств защиты, обеспечить полную защиту невозможно. Обеспечение безопасности значимого объекта достигается путем принятия в рамках подсистемы безопасности значимого объекта совокупности организационных, программно-аппаратных и технических мер, направленных на нейтрализацию угроз безопасности информации. Для снижения рисков КИИ необходимо проводить регулярный аудит, который помогает оценить текущий уровень защиты, проанализировать угрозы и принять ряд мер по повышению эффективности защиты системы.

Список использованных источников:

1. Федеральный законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=43150#OU7AUhUSG1BHGtM81/ (дата обращения: 10.04.2025).

2. Аналитический отчет Anti-Malware.ru «Безопасность КИИ: итоги 2024 г. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/CII-security-AMLive-2024. (дата обращения: 10.04.2025).

3. Отчет НКЦКИ за 2023 г. «Анализ киберугроз для объектов КИИ». URL: https://www.cert.gov.ru / (дата обращения: 10.04.2025).

4. Обеспечение защиты и безопасности объектов КИИ. URL: https://rtmtech.ru/articles/obespechenie-zashhity-i-bezopasnosti-obektov-kii /. (дата обращения: 10.04.2025).

5. Защита значимых объектов критической информационной инфраструктуры / URL: https://is.astral.ru/news/blog/zashchita-znachimykh-obektov-kriticheskoy-informatsionnoy-infrastruktury/ (дата обращения: 10.04.2025).

6. Изменения в работе с критической информационной инфраструктурой. URL: https://securitymedia.org/info/izmeneniya-v-rabote-s-kriticheskoy-informatsionnoy-infrastrukturoy-kii-v-2022-godu.html/ (дата обращения: 10.04.2025).

7. Методические рекомендации по обеспечению безопасности критической информационной инфраструктуры. URL: https://aciso.ru/files/docs/metodichka_2.0.pdf (дата обращения: 10.04.2025).

8. Яппаров Р.М. К вопросу о безопасности объектов критической информационной инфраструктуры / Р.М. Яппаров // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: Сборник материалов VII Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 24–25 мая 2024 г. Уфа: Уфимский университет науки и технологий, 2024. С. 55–58.

9. Андреев, М.Ф. Обработка сетевых пакетов в ядре Linux для противодействия атакам типа «отказ в обслуживании» / М.Ф. Андреев, А.С. Исмагилова // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 19–20 мая 2023 г. Уфа: Уфимский университет науки и технологий, 2023. С. 9–14.

10. Исмагилова, А.С. Теоретико-графовая интерпретация системы защиты информации / А.С. Исмагилова, И.А. Шагапов, И.В. Салов // Инженерный вестник Дона. 2024. № 9(117). С. 171–179.

Biktubayeva K.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

ON THE ISSUE OF ENSURING INFORMATION SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

Abstract. The article is devoted to the key security threats to critical information infrastructure facilities. Special attention is paid to comprehensive protection, combining organizational, legal, software, hardware and technical protection measures.

Keywords: critical information infrastructure, information security, data protection, complex protection, threat.

УДК 004.056.

Журавлева Ю.О.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

ОТНОШЕНИЕ МОЛОДЕЖИ К БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. В статье рассматривается возможные причины уровня осведомленности молодежи о безопасности персональных данных. В ходе работы был проведен опрос, по результатам которого были сделаны выводы относительно причин данного отношения. По результатам опроса были сделаны выводы о высоком уровне осведомленности молодых людей в данной сфере.

Ключевые слова: данные, конфиденциальность, утечка, информация, безопасность.

Согласно Федеральному закону «О персональных данных» от 27.07.2006 № 152-ФЗ, персональные данные – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [1].

Указ Президента № 188 от 6 марта 1997 г. «Об утверждении перечня сведений конфиденциального характера» определяет персональные данные как сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность [2].

Неотъемлемой частью современной жизни является использования множества электронных сервисов, обрабатывающих персональные данные пользователей. При этом частыми являются случаи компрометации персональных данных – получения доступа к этой информации неавторизованными пользователями в результате случайных либо намеренных утечек информации, хакерских атак. В результате подобной утечки информации могут пострадать как тысячи, так и миллиарды пользователей. Такие случаи чаще всего широко освещаются средствами массовой информации.

Целью данной работы является определение отношения молодых людей к безопасности их персональных данных.

Для определения уровня осведомленности молодых людей о безопасности персональных данных был проведен анонимный опрос среди студентов Уфимского Университета науки и технологии. Опрос содержал вопросы, направленные на оценку знания законодательства Российской Федерации в области персональных данных, понимания термина

«персональные данные» и знания правил безопасного обращения с персональными данными в сети Интернет.

В опросе приняли участие 46 студентов Уфимского университета науки и технологии, принадлежащих к возрастной категории 17–35 лет.

Большая часть опрошенных охарактеризовала персональные данные как личные данные человека либо же, как сведения, относящиеся к человеку. Это свидетельствует об общем понимании опрошенными сути термина. Однако лишь 45,7 % респондентов ознакомлены с законодательством Российской Федерации в данной области. Также 56,5 % респондентов никогда не отзывали согласие на обработку персональных данных.

Наиболее опасной большая часть опрошенных считает утечку паспортных данных (67 %), также упоминались данные банковских карт, домашний адрес, номер телефона, биометрические данные. Причем, несмотря на активное использование биометрии в системах идентификации (например, в банковской сфере), биометрические данные упомянули всего 6,5 % респондентов.

При этом 37 % опрошенных сталкивались с последствиями утечки персональных данных, 32 % опрошенных не ощущали последствий утечки персональных данных, 20 % заявили, что их персональные данные никогда не были скомпрометированы.

На рис. 1 продемонстрировано, что более 75 % респондентов готовы отказаться от получения какой-либо услуги или посещения мероприятия, в случае если при регистрации запрашивается больше данных, чем пользователь считает необходимым. Понимание молодыми людьми целей обработки персональных данных является, несомненно, положительно тенденцией.

Рис. 1. Результаты опроса

Свое эмоциональное состояние при предоставлении персональных данных при регистрации куда-либо охарактеризовали как спокойное 21,7 % респондентов. Тревога за сохранность своих данных возникает у 32,6 % респондентов. Однако большая часть респондентов (45,7 %) не высказывает однозначного мнения, заявляя, что их эмоциональное состояние при совершении данных действий зависит от организации либо сайта, при регистрации на котором они дают согласие на обработку своих персональных данных. При этом следует заметить, что в последние 15 лет наблюдались случаи утечки персональных данных и крупных компаний,

пользовавшихся доверием пользователей. Примером может послужить утечка данных пользователей поисковика «Yahoo!», в результате которой были скомпрометированы данные 3 миллиардов пользователей платформы [3].

Таким образом, можно сделать вывод, что молодые люди обладают высоким уровнем осведомленности в сфере безопасности персональных данных. Несмотря на сравнительно низкий процент знания законодательства в данной сфере, следует отметить положительные тенденции, такие как реалистичную оценку ценности персональных данных и понимание целей их обработки.

Список использованных источников:

1. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. URL: http://www.kremlin.ru/acts/bank/24154 (дата обращения: 26.10.2024).

2. Указ Президента № 188 от 6 марта 1997 г. «Об утверждении перечня сведений конфиденциального характера». URL: // http://www.kremlin.ru/acts/bank/10638 (дата обращения: 26.10.2024).

3. RockYou2024 и еще четыре самых крупных утечки данных в истории. URL: https://www.kaspersky.ru/blog/top-five-data-breaches-in-history/38127/ Дата обращения: 26.10.2024\.

Zhuravleva Iu.O.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

THE ATTITUDE OF THE YOUNG PEOPLE TO THE SECURITY OF PERSONAL DATA

Abstract. The article presents purposes of the young people to the safety of their personal data. In the course of the work, a survey was conducted, according to the results of which conclusions were drawn regarding the reasons for this attitude. According to the results of the survey, conclusions were drawn about the high level of awareness of young people in this area.

Keywords: data, confidentiality, breach, information, security.

УДК 004.056

Казанцев В.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ УДАЛЕННОЙ РАБОТЕ

Аннотация. В статье раскрываются особенности организации защиты информации, связанные с удаленной работой сотрудников, которые применяют мобильные устройства в своей деятельности. В содержании статьи акцентируется внимание на проблемах, возникающих в связи с этим, проводится анализ существующих мер безопасности при удаленной работе при помощи мобильных устройств и определяются направления совершенствования существующей практики их применения.

Ключевые слова: информация, информационная безопасность, мобильное устройство, смартфон, удаленный доступ, удаленное рабочее место.

Сегодня удаленная работа набирает все большую популярность, и формат работы продолжает укрепляться на рынке труда [1]. Но, не все организации готовы к полноценному переходу на такой формат, и даже те, кто перешли на удаленную работу, зачастую испытывают трудности с обеспечением надежной защиты конфиденциальной информации. Главная проблема, с которой сталкиваются при внедрении удаленной работы сотрудников, – это риски в сфере информационной безопасности (ИБ), способные нанести ущерб репутации и финансовому положению компании. Кроме того, встает также вопрос, связанный с адаптацией сотрудников при переходе на удаленный формат из офиса и поддержанием необходимой продуктивности в связи с отсутствием физического контроля.

Стоит отметить, что растущая тенденция использования личных устройств, в том числе и мобильных, для удаленной работы требует особого внимания к вопросам защиты информации. Современные смартфоны не так давно стали мощным инструментом для удаленной работы, решающим те задачи, которые ранее требовали применение персональных компьютеров (ПК). Для компаний основным преимуществом стало сокращение затрат на покупку оборудования для персонала и его техническое обслуживание, а повышение гибкости и мобильности сотрудников [2].

В формате, когда сотрудник уходит на удаленную работу, особенно с использованием личных мобильных устройств, возникает целый ряд проблем и рисков информационной безопасности. Утечка конфиден-

циальных данных может иметь серьезные последствия для организации. Поэтому крайне важно вовремя и эффективно выявлять уязвимости и угрозы информационной безопасности, а также разрабатывать и внедрять современные средства и методы защиты данных при организации удаленной работы с использованием мобильных устройств.

Удаленная работа вне офиса создает серьезные риски для защиты конфиденциальной информации [3]. Так, в случае потери или кражи устройства с данными, корпоративные сведения могут быть раскрыты неавторизованным лицом. Нельзя не взять во внимание и кибератаки, нацеленные на уязвимые и оставленные без надзора мобильные устройства. Для обеспечения надежной защиты информации требуется применять шифрование данных, использовать сложные пароли и внедрять другие охранные меры, а также регулярно проводить проверки на предмет угроз, особенно при удаленном формате работы.

Риск заражения мобильных устройств сотрудников вредоносным ПО или использования нелицензионных программ сотрудниками крайне значителен. Нельзя исключить вероятность перехода работника по подозрительной ссылке, что приведет к заражению устройства и, как следствие, к потере личной и конфиденциальной информации.

Зачастую домашние сети имеют слабую защиту. Пользователи пренебрегают сменой стандартных паролей Wi-Fi или делают сеть открытой, вовсе отключая парольную защиту. Настройка и выбор VPN могут представлять сложность для некоторых пользователей. Бесплатные VPN-сервисы также небезопасны, так как подвергают риску данные и конфиденциальность.

При переходе на удаленный режим работы взаимодействие между сотрудниками осуществляется через мессенджеры, электронную почту, видеоконференции и другие платформы. Вероятность взлома учетных записей значительно возрастает при недостаточном уровне защиты паролями.

Также руководство сталкивается с трудностями при внедрении правил информационной безопасности среди персонала в связи с тем, что личные гаджеты не являются собственностью компании. Довольно сложно обязать работников применять специальные программы для хранения паролей, вовремя устанавливать обновления антивирусного ПО и повсеместно активировать двойную аутентификацию при входе в сервисы. Особенно трудно это отследить, учитывая тот факт, что сотрудник находится на удаленном формате работы. Все вышеперечисленные факторы значительно повышают угрозу утечки и несанкционированного доступа к защищаемой информации, поэтому важно применять эффективные меры по защите, например обязательное внедрение организационных и технических мер от утечки и несанкционированного доступа.

К организационным мерам можно отнести [4]:

– разграничение прав доступа сотрудников при организации удаленной работы с мобильных устройств;

– соблюдение регламентов работы с конфиденциальной информацией;

– регулярное обучение и повышение квалификации сотрудников по защите информации.

Как отмечалось ранее, одной лишь организационной защиты информации недостаточно, необходимо внедрение и технических средств: антивирусных программ; использование VPN-сервисов на платной основе для обеспечения безопасного доступа к корпоративной сети; настройка двухфакторной аутентификации для доступа к важным сервисам; осуществление контроля за корпоративной электронной почтой и корпоративной телефонией; использование шифрования при передаче данных; применение лицензионного ПО; регулярное изменение паролей и усиление требований к их надежности; своевременное обновление операционных систем и ПО.

Стоит отметить, что использование DLP-систем является комплексным решением, которое имеет возможность анализа данных и в случае обнаружения угрозы незамедлительное оповещение. Примерами популярных российских DLP-систем, работающих на мобильных платформах iOS и Android, являются: Naumen Service Desk, SearchInform КИБ, InfoWatch Traffic Monitor и др.

DLP-системы имеют возможность контролировать потоки информации по различным каналам обмена информации, проводить аудит подключаемых накопителей, контроль распечатанных документов, реагирование на удаление и установку программ и другие важные функции. Популярность DLP-систем при переходе на удаленный формат работы растет с каждым годом, поскольку обеспечивает высокий уровень безопасности информации.

Список использованных источников:

1. Бирюков А.А. Информационная безопасность: защита и нападение: руководство / А.А. Бирюков. 3-е изд. М.: ДМК Пресс, 2023. 440 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/455351 (дата обращения: 15.04.2025).

2. Кибербезопасность: технические и правовые аспекты защиты информации: сборник научных трудов I Национальной научно-практической конференции (г. Москва, 24–26 мая 2023 г.) / под ред. А.А. Акаева [и др.]. М.: РТУ МИРЭА, 2023. 319 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/398231 (дата обращения: 15.04.2025).

3. Шевченко О.А. Удаленка. Дистанционная (удаленная) работа. Комментарий законодательства и схемы: учебное пособие / О.А. Шевченко, К. С. Балицкий, Е. А. Кашехлебова. М.: Проспект, 2021. 31 с. Электрон. Версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/281033 (дата обращения: 13.03.2025).

4. Яппаров Р.М. К вопросу о безопасности объектов критической информационной инфраструктуры / Р.М. Яппаров // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: Сборник материалов VII Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 24–25 мая 2024 г. Уфа: Уфимский университет науки и технологий, 2024. С. 55–58.

Kazantsev V.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

ENSURING INFORMATION SECURITY DURING REMOTE WORK

Abstract. The article reveals the specifics of the organization of information protection related to the remote work of employees who use mobile devices in their activities. The content of the article focuses on the problems that arise in this regard, analyzes the existing security measures for remote work using mobile devices and identifies areas for improving the existing practice of their application.

Keywords: information, rights, information protection, information security, mobile device, smartphone, remote access, remote workplace.

УДК 004.056

Каримова А.Р., Эгит Д.О., Кагарманов Д.Э.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМАХ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Расследование инцидентов безопасности информации в системах искусственного интеллекта представляет собой сложную задачу, требующую глубокого понимания как технологий искусственного интеллекта (ИИ), так и методов информационной безопасности. Успешное расследование может быть достигнуто с помощью разработки четких политик, обучения персонала и внедрения специализированных инструментов.

Постоянный мониторинг новых угроз и сотрудничество между экспертами в области ИБ и ИИ также играют важную роль в обеспечении защиты.

Ключевые слова: искусственный интеллект, инциденты безопасности, расследование, политики и процедуры, обучение персонала, методы анализа больших данных, Explainable AI, состязательные примеры, мониторинг и защита, сотрудничество специалистов.

Современные системы искусственного интеллекта (ИИ), активно внедряемые в различных сферах деятельности, становятся все более привлекательными целями для кибератак. Это связано с тем, что такие системы обрабатывают большие объемы конфиденциальной информации, обеспечивают работу критически важных инфраструктурных объектов и оказывают значительное влияние на бизнес-процессы компаний. Именно поэтому обеспечение защиты систем ИИ становится важнейшей задачей, особенно в контексте расследований инцидентов информационной безопасности.

В работе [4] приведены аспекты инцидентов ИИ-систем.

1. Автоматизация процессов принятия решений

Одна из ключевых особенностей систем искусственного интеллекта – автоматическое принятие решений. Если злоумышленник получит доступ к таким решениям, последствия могут оказаться непредсказуемыми. Например, атаки на алгоритмы распознавания лиц могут привести к ошибочным идентификациям людей, ложному допуску посторонних сотрудников на охраняемые объекты и другим негативным последствиям.

2. Уязвимость машинного обучения

Алгоритмы машинного обучения являются основой большинства современных ИИ-решений. Однако эти алгоритмы часто уязвимы перед атаками типа adversarial attacks, когда специально подготовленные данные приводят к некорректной работе модели. Такие атаки позволяют обойти механизмы идентификации и аутентификации, делая возможным несанкционированный доступ к ресурсам компании.

3. Атаки на инфраструктуру хранения данных

Важная особенность ИИ заключается в зависимости от больших объемов данных, используемых для тренировки моделей. Эти данные также представляют собой потенциальную цель для хакеров. Инцидент, связанный с утечкой данных, способен поставить под угрозу эффективность работы всей системы искусственного интеллекта и нарушить доверие пользователей.

Этапы расследования инцидентов в ИИ-системах.

В работе [2] предложен процесс расследования инцидентов информационной безопасности в системах искусственного интеллекта:

Анализ инцидента

На данном этапе происходит первичный сбор данных о произошедшем инциденте. Важно выявить следующие моменты: что именно произошло?

Какие данные были затронуты? Каковы возможные причины происшествия? Кто мог стать инициатором атаки? Эти вопросы помогают сформировать предварительную картину произошедшего и определить дальнейшие шаги.

Оценка последствий

После анализа инцидента проводится оценка возможных последствий нарушения безопасности. Необходимо оценить масштаб ущерба, включая финансовые потери, репутационные риски и угрозы для бизнеса организации. Важность данного этапа связана с необходимостью принимать оперативные меры по минимизации потерь.

По итогам расследования разрабатываются рекомендации по повышению уровня защищенности системы искусственного интеллекта. В работе [3] они подробно описываются, сюда входят мероприятия по улучшению архитектуры инфраструктуры, обновлению программного обеспечения, проведению регулярных проверок безопасности и обучению персонала правилам безопасной работы с системой. В работе [1] указан ряд специфических проблем, который возникает при расследовании инцидентов информационной безопасности в системах искусственного интеллекта:

Сложность выявления вредоносных действий из-за высокой автоматизации процесса обработки данных.

Недостаточная прозрачность механизмов принятия решений алгоритмами машинного обучения.

Возможность влияния третьих сторон через обучение нейронных сетей на основе искаженных данных.

Кроме того, существуют трудности правового характера, поскольку законодательство многих стран пока не предусматривает четких норм регулирования вопросов, связанных с искусственным интеллектом.

Расследование инцидентов информационной безопасности в системах искусственного интеллекта требует особого подхода, учитывающего особенности технологии и сложности ее функционирования. Грамотное расследование позволяет минимизировать ущерб от нападения и предотвратить подобные инциденты в будущем. Поэтому развитие компетенций специалистов по обеспечению информационной безопасности является приоритетной задачей современного общества.

Список использованных источников:

1. Коваленко А.И. Угрозы информационной безопасности в системах ИИ. Издательский дом РАЭК, 2020. URL: https://www.raeonline.ru/publications/ugrozy-info-bezopasnosti.

2. Борисов О.В. Методология расследования киберинцидентов. М.: Юрайт, 2019. URL: https://www.jurait.ru/book/metodologiya-rassledovaniya-kibertincidentov.

3. Романов, С. В. Защита информации в системах искусственного интеллекта. Издательство «БХВ-Петербург», 2022. URL: https://www.bhvpeterburg.ru/book/zashchita-informacii-v-sistemah-iskusstvennogo-intellekta.

4. Березкин, А. Г. Управление инцидентами безопасности в ИТ. Издательство «Гардарика», 2021. URL: https://www.gardarik.com/books/upravlenie-incidentami-bezopasnosti.

Karimova A.R., Egit D.O., Kagarmanov D.E.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

FEATURES OF INVESTIGATING INFORMATION SECURITY INCIDENTS IN ARTIFICIAL INTELLIGENCE SYSTEMS

Abstract. Investigating information security incidents in artificial intelligence systems is a complex task that requires a deep understanding of both AI technologies and information security methods. Successful investigations can be achieved through the development of clear policies, staff training, and the implementation of specialized tools. Continuous monitoring of new threats and collaboration among experts in the fields of information security and AI also play a crucial role in ensuring protection.

Keywords: artificial intelligence, security incidents, investigation, policies and procedures, staff training, big data analysis methods, Explainable AI, adversarial examples, monitoring and protection, collaboration of specialists.

УДК 004

Кириллов В.С.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

МОДЕЛИ УГРОЗ И ПОСТРОЕНИЕ СИСТЕМ ЗАЩИТЫ В КОРПОРАТИВНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Аннотация. В статье раскрыты особенности разработки модели угроз на предприятии, а также построения систем защиты в корпоративных автоматизированных системах. Рассматриваются и анализируются проблемы информационной безопасности при защите информации в системах защиты в корпоративных АС.

Ключевые слова: информация, система защиты информации, угроза информационной безопасности, модели угроз, автоматизированная система.

В настоящее время защита корпоративных автоматизированных систем (АС) является крайне актуальной задачей и тому есть определенные причины: организации все больше подвергаются различным сетевым атакам со стороны злоумышленников, которые могут нарушить бизнес-процессы и нанести финансовый и репутационный ущерб, поскольку организации хранят огромное количество важной и ценной информации - от клиентских баз и финансовых документов до интеллектуальной собственности. Защита корпоративных автоматизированных систем становится важнейшей частью стратегии развития любой современной компании, обеспечивая ее безопасность, стабильность и конкурентоспособность.

Для обеспечения безопасности организации очень важно выделить актуальные угрозы безопасности информации, которые оцениваются в ходе моделирования угроз на предприятии. Модель угроз необходима для эффективного управления рисками и разработки мер по защите информационных активов компании. Модель угроз – это формализованное представление возможных сценариев реализации угроз безопасности информационных ресурсов организации [1]. То есть модель угроз представляет собой систематический подход к идентификации возможных рисков и потенциальных уязвимостей, связанных с нарушением информационной безопасности (ИБ) в организации.

Модель угроз включает в себя:

– классификацию угроз: определение типов атак и уязвимостей системы;

– анализ вероятности возникновения угроз: оценка реализуемости различных сценариев атак;

– оценку последствий реализации угроз: рассмотрение возможного ущерба от реализации угроз нарушения ИБ.

Главная цель построения модели угроз заключается в выявлении слабых мест информационной инфраструктуры организации и разработке эффективных мер противодействия потенциальным угрозам, которые могут нанести ущерб компании. Существует определенный сценарий разработки модели угроз корпоративной АС, он основывается на Методике оценки угроз безопасности информации, разработанной ФСТЭК 5 февраля 2021г [2].

Этапами разработки модели угроз корпоративной АС являются:

1. Сбор исходных данных: идентификация активов, анализ используемых технологий и протоколов передачи данных, обзор существующих политик безопасности.

2. Идентификация потенциальных угроз от внутренних и внешних источников угроз.

3. Анализ уязвимости и оценка рисков: классификация уязвимых элементов инфраструктуры, проведение анализа влияния угроз на бизнес-процессы компании.

4. Разработка мероприятий по защите информации на основе проведенного анализа, уточнение набора мер защиты: создание политики управления доступом, развертывание антивирусных решений и межсетевых экранов, регулярная проверка и обновление программного обеспечения и др.

5. Мониторинг и контроль эффективности принятых мер по защите информации.

Стоит отметить, что в настоящее время появились специальные сервисы для автоматизированной разработки моделей угроз безопасности информации в соответствии с требованиями регуляторов (ФСТЭК России). Примером такого сервиса является «Цифровая модель угроз».

«Цифровая модель угроз» – это комплексное решение, позволяющее быстро разрабатывать модели угроз, учитывающие специфику различных отраслей и детально описывающие потенциальные риски для информационных систем и систем АСУ ТП [3]. Это специализированное программное обеспечение позволяет вести разработку сценариев реализации угроз, основанных на комбинации тактик и техник, представленных в матрице MITRE ATT&CK, и техник, определенных ФСТЭК в качестве актуальных для защиты информации.

Рассматривая методы и подходы к защите корпоративной АС, которые помогут увеличить защищенность системы от актуальных угроз, можно выделить: физическую защиту: защиту помещений и оборудования от несанкционированного доступа; техническая защиту: межсетевые экраны (firewalls), VPN-туннели, шифрование каналов связи и хранящихся данных, антивирусные программы и др.; организационную защиту: управ-

ление информационными потоками внутри компании посредством строгих регламентов и инструкций (например, Политика разграничения прав доступа пользователей); правовую защиту: нормативно-правовые акты.

Основными рекомендациями по повышению уровня защищенности корпоративной АС являются:

1. Постоянное обучение персонала вопросам, связанным с информационной безопасностью.
2. Регулярные обновления ПО: своевременное применение обновлений и исправление обнаруженных уязвимостей минимизирует вероятность успешных атак злоумышленников.
3. Использование многоуровневой защиты: применение комплексного подхода обеспечивает надежность даже при нарушении одного слоя защиты.
4. Постоянный аудит и тестирование: периодическое проведение тестов на проникновение и внутренний аудит информационной безопасности позволяют своевременно выявить слабые места и устранить уязвимости информационной безопасности.

Таким образом, разработка эффективной модели угроз и реализация соответствующих мер защиты от актуальных угроз является важным этапом в обеспечении устойчивости и надежности корпоративной автоматизированной системы.

Список использованных источников:

1. Прохорова О.В. Информационная безопасность и защита информации: учебник для СПО / О.В. Прохорова. 6-е изд., стер. СПб.: Лань, 2025. 124 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/445250 (дата обращения: 17.04.2025).
2. Методический документ Федеральной службы по техническому и экспортному контролю от 05.02.2021 г. «Методика оценки угроз безопасности информации»: URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 16.04.2025).
3. Цифровая модель угроз. URL: https://digital-threat-model.ru/#about (дата обращения: 16.04.2025).

Kirillov V.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.Yu.
Ufa University of Science and Technology, Ufa

THREAT MODELS AND CONSTRUCTION OF PROTECTION SYSTEMS IN CORPORATE AS

Abstract. The article reveals the features of developing threat models, as well as construction of protection systems in corporate automated systems. The problems of information security in protecting information in protection systems in corporate AS are considered and analyzed.

Keywords: information, rights, information protection, information protection system, information security threat, threat models, automated system.

УДК 004

Набиев Д.Т.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В ОРГАНИЗАЦИИ НА БАЗЕ ПЛАТФОРМЫ DOCSVISION

Аннотация. В статье рассматривается роль системы электронного документооборота (ЭДО), ее основные цели и задачи, а также повышение уровня защиты информации (ЗИ) в организациях с применением системы электронного документооборота на базе платформы Docsvision. В центре внимания - угрозы и уязвимости безопасности электронных документов и средства, методы защиты ЭДО с применением специальных решений на базе платформы Docsvision.

Ключевые слова: информация, защита информации, документ, электронный документ, документооборот организации, система электронного документооборота, Docsvision.

Современный бизнес стремительно эволюционирует, и информационные технологии (ИТ) безусловно занимают центральное место. Они внедряются практически во все сферы коммерческой деятельности, становясь важной составной частью бизнес-процессов. Каждая компания

сталкивается с организацией и внедрением систем электронного документооборота (СЭД), и с ростом объема документации возникает острая потребность в увеличении скорости бизнес-процессов и переходе на электронный документооборот. В результате этого всего формируется концепция внедрения системы электронного документооборота [1–2].

При использовании бумажного документооборота существует вероятность случайной утраты документов, а также значительные затраты времени на их создание, редактирование и уничтожение. Переход на электронный документооборот позволяет автоматизировать процессы, что снижает время, затрачиваемое на обработку, и практически исключает риск случайной потери, так как документы хранятся на цифровых носителях. Кроме того, СЭД дает хорошую возможность руководству более быстро и эффективно осуществлять контроль за движением документации [3–4].

Однако переход на электронный формат также затрагивает вопросы безопасности данных, ограничений доступа и проверки подлинности документов [5]. Для этого можно использовать электронную подпись (ЭП), имеющую юридическую силу. Получить ЭП можно в аккредитованном удостоверяющем центре. Аутентификация и управление правами пользователей обеспечивают защищенный доступ к данным внутри СЭД. Наиболее распространенный метод аутентификации – пароли, но их надежность зависит от человека. Альтернативы включают смарт-карты и биометрические данные, которые являются наиболее безопасными.

Конфиденциальность информации защищается с помощью применения криптографии, которая может предотвращать утечки даже при несанкционированном доступе. Нормативно-правовые акты (НПА), которые регулируют вопросы электронного документооборота в России, такие как Федеральный закон «Об информации, информационных технологиях и о защите информации», обеспечивают их правовую основу. К техническим средствам защиты относятся антивирусные программы, резервное копирование и регулярные обновления программного обеспечения (ПО).

Особое внимание заслуживает отечественное программное обеспечение «Приоритет», разработанное на базе платформы DocsVision Core. Это решение входит в Реестр отечественного ПО с 2016 г., что подтверждает его соответствие требованиям государственной ИТ-политики по импортозамещению. В условиях внешнеэкономической нестабильности, когда компании вынуждены отказываться от зарубежных решений, использование российской платформы становится не только стратегически оправданным, но и экономически выгодным.

В отличие от зарубежных аналогов, «Приоритет» полностью адаптирован под российское законодательство и предоставляет организациям гибкость в настройке процессов документооборота, включая обработку персональных данных, юридически значимые электронные

подписи и строгую ролевую модель безопасности. Это особенно актуально для государственных учреждений и коммерческих организаций, работающих с конфиденциальной информацией.

Таблица 1

Сравнительная таблица систем ЭДО

Критерий	Традиционные системы (например, 1С:Документооборот)	Современные системы (например, Directum, ELMA)	Docsvision («Приоритет»)
Юридическая значимость	Требует дополнительных модулей для ЭП	Поддержка ЭП встроена	Полная интеграция с ЭП, соответствие российскому законодательству
Безопасность данных	Базовые механизмы защиты (пароли, роли)	Расширенные методы (биометрия, шифрование)	Криптография, строгая ролевая модель, аудит действий
Интеграция с другими системами	Ограниченная (в основном с 1С)	Широкая (CRM, ERP, бухгалтерские системы)	Гибкая интеграция (1С, СЭД, CRM), поддержка API
Удобство использования	Сложный интерфейс, требует обучения	Интуитивный интерфейс, мобильные приложения	Адаптивный интерфейс, настраиваемые маршруты документов
Масштабируемость	Ограничена для крупных организаций	Подходит для средних и крупных компаний	Высокая масштабируемость, поддержка распределенных архивов
Импортозамещение	Частичное соответствие	Соответствует требованиям	Включен в Реестр отечественного ПО с 2016 г.
Стоимость внедрения	Низкая (для базовых версий)	Средняя	Конкурентная, экономически выгодная в долгосрочной перспективе
Поддержка и обновления	Редкие обновления	Регулярные обновления	Активная поддержка, частые обновления в соответствии с НПА

Практический эффект от внедрения «Приоритета» подтверждается положительным опытом десятков российских организаций, которым удалось значительно сократить временные и трудозатраты на документооборот, повысить точность и достоверность учета, а также обеспечить высокий уровень информационной безопасности без зависимости от иностранных решений.

В заключение, можно отметить, что автоматизированные системы документооборота становятся все более распространенными и широко внедряемыми в самых различных организациях. Преимуществом от интеграции системы электронного документооборота в организации заключается в том, что СЭД значительно сокращает время на обработку информации, увеличивает уровень безопасности информации, позволяет хранить большие объемы данных без необходимости аренды отдельных помещений для архивов, увеличивает прозрачность управленческих процессов и предоставляет множество других полезных функций.

Список использованных источников:

1. Грибков Д.Н. Технологии электронного документооборота: учебное пособие / Д.Н. Грибков, А.В. Калянов. Орел: ОГИИК, 2021. 105 с. Электрон. версия. URL: https://e.lanbook.com/book/261932 (дата обращения: 28.11.2024).

2. Егорова О.Н. Делопроизводство и документоведение: учебно-методическое пособие / О.Н. Егорова. Чебоксары: ЧГИКИ, 2023. 104 с. Электрон. версия. URL: https://e.lanbook.com/book/392702 (дата обращения: 01.12.2024).

3. Куняев Н.Н. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник / Н.Н. Куняев; под редакцией Н.Н. Куняева. 2-е изд., перераб. и доп. М.: Логос, 2020. 500 с. Электрон. версия. URL: https://e.lanbook.com/ book/163041 (дата обращения: 01.12.2024).

4. Ульянова Н.Д. Электронный документооборот: учебно-методическое пособие / Н.Д. Ульянова. Брянск: Брянский ГАУ, 2021. 24 с. Электрон. версия. URL: https://e.lanbook.com/book/304610 (дата обращения: 28.11.2024).

5. Кириллов В.С. Проблематика использования электронных подписей / В.С. Кириллов, А.С. Исмагилова, Д.Т. Набиев // Информационные технологии интеллектуальной поддержки принятия решений (памяти проф. Н.И. Юсуповой) ITIDS'2024: труды X Международной научной конференции. В 2 томах, Уфа, 12–14 ноября 2024 г. Уфа: Уфимский университет науки и технологий, 2024. С. 12–14.

Nabiev D.T.
Ufa University of Science and Technology, Уфа

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Уфа

PROTECTION OF ELECTRONIC DOCUMENT MANAGEMENT IN AN ORGANIZATION BASED ON THE DOCSVISION PLATFORM

Abstract. The article discusses the role of the electronic document management system (EDI), its main goals and objectives, as well as increasing the level of information security (II) in organizations using the electronic document management system based on the Docsvision platform. The focus is on threats and vulnerabilities to the security of electronic documents and tools, methods of EDI protection using special solutions based on the Docsvision platform.

Keywords: information, information protection, document, electronic document, organization's document management, electronic document management system, Docsvision.

УДК 004

Насифуллина Э.И.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

АНАЛИЗ СООТВЕТСТВИЯ СУЩЕСТВУЮЩИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ТРЕБОВАНИЯМ ГОСТ ПРИ СОЗДАНИИ АС В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Аннотация. В данной статье проводится анализ соответствия современных средств защиты информации требованиям государственного стандарта, регулирующих создание автоматизированных систем в защищенном исполнении. Целью исследования является выявление степени готовности рынка средств защиты информации к обеспечению необходимого уровня защиты информации в автоматизированных систем, создаваемых в соответствии с требованиями государственного стандарта.

Ключевые слова: средства защиты информации, ГОСТ, автоматизированные системы, сертификация, ФСТЭК.

В настоящее время проблема соответствия СЗИ требованиям ГОСТ Р 51583-2014 остается крайне актуальной [8]. Развитие технологий приводит к появлению новых угроз, что делает важным постоянное обновление механизмов защиты информации. Многие организации сталкиваются с трудностями при выборе сертифицированных средств защиты, а также с необходимостью интеграции разнородных систем безопасности. Анализируя ГОСТ Р 51583-2014, мы видим, что стандарт распространяется на создаваемые (модернизируемые) информационные автоматизированные системы, в отношении которых законодательством уже определены, а заказчиком определяются требования по их защите, содержание и порядок выполнения работ на соответствующих стадиях и этапах создания в защищенном исполнении [1]. Иными словами, стандарт устанавливает базовые принципы, требования и рекомендации по организации процесса создания и функционирования защищенных АС.

Таким образом, ГОСТ Р 51583-2014 определяет общий порядок создания АС в защищенном исполнении, охватывая весь жизненный цикл системы: от этапа предпроектных исследований до ввода в эксплуатацию и последующего вывода из нее. Это можно установить по перечню, в котором содержатся отсылочные нормы, регулирующие конкретные этапы. Так, на этапе предпроектных исследований необходимо выполнить ряд ключевых шагов, среди которых:

- определение целей защиты информации;
- формирование перечня актуальных угроз;
- проведение анализа рисков;
- разработка модели угроз и модели нарушителя.

На основе этих данных формируются требования по защите информации, включающие в себя требования конфиденциальности, целостности и доступности информации. Технический проект должен детально описывать архитектуру системы защиты, состав и характеристики СЗИ, а также методы их интеграции и настройки. Процесс внедрения СЗИ должен включать в себя аттестацию, которая подтверждает соответствие внедренных средств установленным требованиям по безопасности информации. После ввода в эксплуатацию АС в защищенном исполнении требуется обеспечить постоянное сопровождение системы защиты: ее актуализацию, регулярный мониторинг и анализ инцидентов информационной безопасности.

Для детального анализа соответствия существующих средств защиты информации требованиям ГОСТ при создании АС в защищенном исполнении проанализируем и оценим, насколько современные средства защиты информации соответствуют требованиям ГОСТ Р 51583-2014, выявим возможные расхождения и несоответствия различных категорий СЗИ предъявляемым требованиям.

В современных межсетевых экранах (МСЭ), например «Страж NT» (версия 4.0) компании ООО «РУБИНТЕХ», который может применяться

для комплексной защиты информационных ресурсов от несанкционированного доступа и фильтрацию трафика при работе в одно- и многопользовательских автоматизированных системах (АС) [2] и «Континент» (разработчик – компания «Код Безопасности»)[3] сертифицирован ФСТЭК России и соответствует требованиям ГОСТ в части фильтрации трафика, защиты от несанкционированного доступа и обеспечения безопасных соединений, несмотря на соответствие ключевым требованиям, возможны сложности в интеграции с определенными зарубежными решениями, а также они нуждаются в дополнительной настройке под специфические политики безопасности конкретных организаций.

В свою очередь, антивирусные решения Kaspersky Endpoint Security и Dr.Web соответствуют требованиям по обнаружению и нейтрализации вредоносного кода [4], однако при их применении в крупных автоматизированных системах важно учитывать необходимость централизованного управления, что может потребовать дополнительных программных средств, таких как «Касперский Центр Управления Безопасностью». Кроме того, обновление сигнатурных баз и механизмов поведенческого анализа должно быть оперативным, чтобы соответствовать современным требованиям защиты информации, установленным в ГОСТ Р 51583-2014.

Система обнаружения вторжений «Рубикон» (разработчик – компания «НПО Эшелон») [5], соответствует требованиям ГОСТ, обеспечивая мониторинг сетевого трафика, выявление аномалий и автоматизированное реагирование на инциденты. Однако их эффективность зависит от своевременной настройки политик безопасности, анализа инцидентов и актуальности баз данных угроз.

Современные отечественные средства криптографической защиты информации ViPNet CSP (разработчик – «ИнфоТеКС») [6], а также «КриптоПро CSP» полностью соответствуют сертификационным требованиям ФСБ России. Более того, ViPNet CSP обладает дополнительными возможностями по обеспечению защищенного соединения в распределенных сетях и поддерживает современные алгоритмы шифрования. Однако, несмотря на соответствие ключевым требованиям, здесь также могут возникать сложности с интеграцией в инфраструктуру, где используются зарубежные решения или устаревшие системы.

DLP-системы, такие как SearchInform и InfoWatch, а также «Стахановец» [7], соответствуют требованиям ГОСТ, контролируют каналы передачи данных и предотвращают утечки информации. При этом «Стахановец» предлагает расширенные возможности аналитики пользовательской активности, что позволяет не только предотвращать утечки, но и выявлять потенциальные внутренние угрозы. Однако для эффективного применения всех возможностей этих систем требуется детальная настройка под бизнес-процессы организации.

Таким образом, современные средства защиты информации в целом соответствуют требованиям ГОСТ Р 51583-2014. Однако на практике

могут возникать определенные сложности, связанные с проведением дополнительных настроек, их интеграцией в существующие программные и аппаратные решения, а также прохождения процедур аттестации, что требует комплексного подхода на всех этапах жизненного цикла защищенной автоматизированной системы.

Список использованных источников:

1. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения». URL: https://docs.cntd.ru/document/1200108858 (дата обращения: 23.03.2025).
2. Страж NT 4.0. URL: https://guardnt.ru/gnt_40.html (дата обращения: 24.03.2025).
3. Решения Код безопасности. URL: https://kontinent-ipc.ru/ (дата обращения: 24.03.2025).
4. Kaspersky Endpoint Security для Windows | Лаборатория Касперского URL: https://www.kaspersky.ru/small-to-medium-business-security/endpoint-windows (дата обращения: 28.03.2025).
5. ПАК «Рубикон». URL: https://npo-echelon.ru/production/65/11342 (дата обращения: 28.03.2025)
6. Сертифицированный криптопровайдер ViPNet CSP 4 | ИнфоТеКС. URL: https://infotecs.ru/products/vipnet-csp/ (дата обращения: 28.03.2025).
7. Предотвращение утечек информации – DLP-система | Стахановец URL: https://stakhanovets.ru/dlp/ (дата обращения: 28.03.2025).
8. Яппаров Р.М. К вопросу о безопасности объектов критической информационной инфраструктуры / Р.М. Яппаров // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VII Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 24–25 мая 2024 г. Уфа: Уфимский университет науки и технологий, 2024. С. 55–58.

Nasifullina E.I.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

ANALYSIS OF THE COMPLIANCE OF EXISTING INFORMATION SECURITY TOOLS WITH THE REQUIREMENTS OF GOST WHEN CREATING AUTOMATED SYSTEMS IN A SECURE DESIGN

Abstract. This article analyzes the compliance of modern information security tools with the requirements of the state stardart governing the creation of automated systems in a secure design. The purpose of the study is to identify the degree of readiness of the information security market to ensure the

necessary level of information protection in automated systems created in accordance with the requirements of the state standard.

Keywords: information security tools, GOST, automated systems, information security, FSTEC.

УДК 004.056:34

Резбаева В.М.
Стерлитамакский филиал Уфимского
университета науки и технологий, Стерлитамак

Научный руководитель:
Корнилова А.А.
Уфимский университет науки и технологий, Уфа

ИЗМЕНЕНИЯ В ЗАКОНОДАТЕЛЬСТВЕ ОБ ОТВЕТСТВЕННОСТИ ЗА УТЕЧКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. В данной статье рассмотрены новые законы об ответственности за утечки персональных данных. Изменения затрагивают всех операторов и субъектов персональных данных. Они направлены на создание механизмов защиты прав и свобод субъектов персональных данных.

Ключевые слова: персональные данные, утечка, субъект персональных данных, оператор.

Масштабы количества утечек персональных данных (ПДн) выходят на уровень мировой проблему. Кража ПДн способна в корне изменить дальнейшую жизнь человека. Раскрытие личной, конфиденциальной информации может привести к тяжелым последствиям не только для бизнеса, правительственных структур, но и затронуть безопасность частных лиц. Человек порой даже не знает о том, что его ПДн попали злоумышленникам и естественно не предпринимает ничего для сохранения своей жизни в безопасности. В то время как преступники уже начинают предпринимать действия для использования похищенных данных с получением выгоды для себя. Без должного внимания даже небольшая уязвимость может привести к масштабной утечке личных данных. Несмотря на общедоступность и открытость информации по утечкам ПДн, мошеннических схемах и последствий таких действий для человека в современном обществе все еще не принято говорить о безопасности личных данных, что безусловно облегчает задачу хакерам. По данным экспертно-аналитического центра InfoWatch Россия вошла в 5 стран с максимальным количеством утекших данных [1]. По данным Роскомнадзора [2], в 2023 г. количество зафиксированных утечек ПДн

увеличилось на 37 % по сравнению с 2022 г. В результате чего в открытом доступе оказалось более 300 млн записей. Особую тревогу вызывает изменение типа преступления, ранее основную массу инцидентов составляли случайные утечки, сегодня все более распространенными являются целенаправленные атаки и сложные мошеннические схемы.

Ответом на вызовы стало существенное ужесточение наказаний за утечку ПДн. В начале 2024 г. в России были приняты законы об административной и уголовной ответственности за действия, повлекшие за собой утечку ПДн, что кардинально меняет подход к защите ПДн [3].

В соответствии с Федеральным законом от 30 ноября 2024 г. № 421-ФЗ незаконное использование/сбор/передача/хранение ПДн, полученных незаконным путем влечет за собой ответственность в виде штрафа до 300 тыс. рублей, принудительных работ до 4 лет; лишения свободы на этот же срок (ч. 1 ст. 272.1 Уголовного кодекса РФ (УК РФ)). В случае утечки информации лиц, не достигших 18 лет частью 2 этой же статьи УК РФ нарушителю, грозит штраф в размере до 700 тыс. руб.; принудительные работы или лишение свободы сроком до 5 лет. Если данные действия совершенны из корыстной заинтересованности, с причинением крупного ущерба, группой лиц по предварительному сговору, с использованием своего служебного положения, то согласно часть 3 статью 272 УК РФ преступнику(ам) грозит:

– штраф в размере до одного миллиона рублей с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет;

– принудительные работы до 5 лет со штрафом в размере до 1 млн руб. с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет;

– лишение свободы на срок до 6 лет со штрафом в размере до 1 млн руб. с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет.

В случае использования ПДн для их передачи иностранному государству согласно статье 272.1 части 4 УК РФ нарушителю грозит лишение свободы до 8 лет со штрафом до 2 млн рублей или в размере заработной платы за период до 3 лет, с лишением права занимать руководящие должности или заниматься определенной деятельностью в период до 4 лет [3]. В случае если действия повлекли тяжкие последствия либо совершены организованной группой, то согласно части 5 этой же статьи правонарушителю грозит лишение свободы до 10 лет со штрафом в размере до 3 млн руб. с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет.

За создание или обеспечение функционирования информационного ресурса (например, сайта или страницы в интернете, программы, информационной системы, приложения и др.) предназначенного для незаконных использования компьютерной информации, содержащей ПДн,

полученной незаконным путем также предусмотрено уголовное наказание в виде штрафа до 700 тыс. рублей, принудительных работ или лишения свободы на срок до 5 лет.

Отметим, что действия статьи 272.1 не распространяются на случаи обработки ПДн физическими лицами для личного использования.

Также с 30 мая 2025 г. начнет действовать ФЗ от 30 ноября 2024 г. № 420-ФЗ, ужесточающий административную ответственность за нарушения в сфере ПДн [4].

Штрафные санкции за нарушения выросли в многократно. Например, максимальной штраф за незаконную обработку ПДн для юридических лиц при повторном нарушении достигнет 500 тысяч рублей, что превышает прежние штрафные пределы в 1.5 раза. Для должностных лиц верхняя планка санкций возросла в 4 раза (200 000 рублей) [4].

Согласно части 1 статьи 13.11 Кодекса Российской Федерации об административных правонарушениях (КоАП РФ) за обработку ПДн в случаях, не предусмотренных законодательством, либо обработку ПДн, несовместимую с целями их сбора влечет за собой ответственность в виде штрафа:

– для граждан – в размере от 10 тыс. до 15 тыс. руб., для сравнения этот штраф ранее составлял 2000-6000 рублей;

– для должностных лиц и индвидуальных предпринимателей (ИП) финансовые потери составят от 50 тыс. до 100 тыс. руб. (ранее должностные лица в данном случае оплатили в среднем штраф в размере 15 тыс. руб.);

– для организаций – от 150 тыс. до 300 тыс. руб. (ранее – от 60 тыс. до 100 тыс. руб.).

Повторное совершение административного правонарушения, предусмотренного части 1 статьи 13.11 КоАП РФ увеличивает размер штрафа:

– для граждан до 30 тысяч рублей;

– для должностных лиц до 200 000 руб.;

– для организаций и ИП до 500 000 руб.

С 30 мая 2025 г. операторы ПДн будут несут ответственность за несвоевременное уведомление Роскомнадзора о фактах утечки ПДн. Если уведомление было предоставлено позднее, чем через 1 сутки, оператору грозит штраф до 3 млн рублей [4]. В случае не уведомления Роскомнадзора о намерении осуществлять обработку ПДн и за действия оператора, повлекшие неправомерное распространение ПДн введены штрафы. Согласно статье 13.11 части 10 КоАП РФ штраф составит:

– для граждан – от 5000 до 10 000 руб.;

– для должностных лиц государственного или муниципального органа – от 30 000 до 50 000 руб.;

– для организаций, которые не являются государственным или муниципальным органом – от 100 000 до 300 000 руб.

В нововведениях особое внимание контролирующих органов направлено на первых лиц организации. Даже при формальном назначении лица, отвечающего за защиту ПДн, именно на руководителе лежит вся ответственность за соответствие процессов обработки ПДн требованиям законодательства. В перспективе обсуждается введение уголовной ответственности за грубую халатность, породившую массовые утечки ПДн [5].

ФЗ № 420-ФЗ ужесточает ответственности для предпринимателей сейчас ИП будут нести ответственность на уровне юридические лица, то есть их штрафы существенно увеличиваются.

Ужесточение регулирования в сфере защиты ПДн является следствием резкого роста числа утечек ПДн, которые ведут к большим потерям как для организации, так и для человека. Современным компаниям сейчас необходимо организовать надежных систем защиты информации.

Список использованных источников:

1. Утечки информации в мире, 2022-2023 гг. Экспертно-Аналитический центр InfoWatch. 2024 г. URL: https://www.infowatch.ru/sites/default/files/analytics/files /issledovaniye-utechek-informatsii-v-mire-za-2022-2023-gody.pdf?ysclid=m9kwhev8ln20907 4874 (дата обращения: 17.04.2025).

2. Роскомнадзор: в сеть утекло 24 млн записей россиян с начала 2025 г. Iaassaaspaas. Обзор ИТ решений для бизнеса и государства. 13.03.2025 г. URL: https://iaassaaspaas.ru/news/okolo-milliarda-strok-personalnyh-dannyh-uteklo-v-set-za-polgoda-nikakie-shtrafy-ne-pomogayut (дата обращения: 17.04.2025).

3. Уголовный кодекс Российской Федерации // Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/?ysclid=m9nqa3dtg3694793877 (Дата обращения: 19.04.2025).

4. Федеральный закон о внесении изменений в кодекс Российской Федерации. Об административных правонарушениях // Консультант Плюс. URL: https://www.consultant.ru/document/cons_doc_LAW_491932/?ysclid=m9nwtgdgi252479281 (Дата обращения: 19.04.2025).

5. Ужесточение ответственности за обработку персональных данных в 2025 г. // Контур|Журнал. URL: https://kontur.ru/articles/55870-otvetstvennost_za_obrabotku_pers_dannyh?ysclid=m9ns1w11ee638184836 (Дата обращения: 19.04.2025).

Rezbaeva V.M.
Sterlitamak branch of Ufa University of
Science and Technology, Sterlitamak

Scientific supervisor:
Kornilova A.A.
Ufa University of Science and Technology, Ufa

CHANGES IN THE LEGISLATION ON LIABILITY FOR PERSONAL DATA LEAKAGE

Abstract. This article examines new laws on liability for personal data leaks. The changes affect all operators and subjects of personal data. They are aimed at creating mechanisms to protect the rights and freedoms of subjects of personal data.

Keywords: personal data, leak, subject of personal data, operator.

УДК 004

Рябова К.А.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

О НЕОБХОДИМОСТИ ПРИМЕНЕНИЯ ПРОГРАММ БЕЗОПАСНОГО ПОВЕДЕНИЯ И КУЛЬТУРЫ ИБ (SBCP)

Аннотация. В статье раскрыты особенности использования программ безопасного поведения и культуры ИБ (SBCP) на примере ПО системы мониторинга «ИНСАЙДЕР». В содержании статьи рассматриваются и анализируются проблемы обеспечения информационной безопасности в контроле и мониторинге рабочего времени сотрудников компании.

Ключевые слова: информация, система защиты информации, контроль работы, программы безопасного поведения, эффективность работы сотрудников.

В настоящее время программы безопасного поведения и культуры информационной безопасности (SBCP – Safe Behavioral Culture Programs for Information Security) являются важными инструментами для защиты организаций от инцидентов информационной безопасности (ИБ) и снижения рисков нарушения конфиденциальности, целостности и

доступности информации. Их актуальность обусловлена несколькими факторами:

1. Рост числа кибератак. Количество и сложность подобного вида атак постоянно увеличиваются с появлением новых технологий. Современные угрозы включают фишинговые атаки, программы-шифровальщики, инсайдерские риски и другие виды угроз ИБ. Для эффективной борьбы с даными рисками необходимы комплексные меры безопасности, включающие как обучение сотрудников, так и повышение уровня осведомленности о мерах предосторожности [2, с. 22].

2. Изменение законодательства. Законы и нормативные акты, регулирующие защиту персональных данных и конфиденциальной информации, становятся все строже. Например, российские законы № 152-ФЗ «О персональных данных» и № 187-ФЗ «О безопасности критической информационной инфраструктуры», а также международные стандарты, такие как GDPR (General Data Protection Regulation), требуют от компаний внедрения эффективных мер защиты информации. Программы безопасного поведения и культуры информационной безопасности помогают организациям соответствовать требованиям регуляторов и избежать штрафов и репутационных потерь.

3. Повышение ответственности сотрудников. Многие инциденты ИБ происходят из-за человеческого фактора: недостаточной внимательности, незнания правил безопасной работы с защищаемой информацией или случайных ошибок пользователей. Регулярное обучение сотрудников правилам работы с такими данными помогает снизить вероятность нарушений ИБ и повысить уровень общей защищенности информации в организации [1, с. 18–19].

Основными элементы программ SBCP являются следующие показатели: обучение и информирование: регулярные занятия, вебинары и тестирование знаний сотрудников о правилах ИБ. Разработка и внедрение инструкций и руководств по соблюдению требований информационной безопасности. Проведение мониторинга и постоянный контроль: системы мониторинга действий пользователей, проведение аудитов и проверок соблюдения политики безопасности. Управление изменениями: обеспечение постоянного обновления процедур и технологий защиты информации.

Система мониторинга «Инсайдер» является одним из примеров программ безопасного поведения и культуры информационной безопасности. Она представляет собой специализированное решение, предназначенное для выявления и предотвращения внутренних угроз информационной безопасности (инсайдеров). Она позволяет эффективно контролировать деятельность сотрудников внутри организации, предотвращая возможные утечки данных, несанкционированный доступ (НСД) к конфиденциальной информации и прочие нарушения политики безопасности.

Особенностями системы «Инсайдер» можно выделить: постоянный анализ активности пользователей. Система автоматически фиксирует и анализирует активность пользователей в сети и локальных системах организации. Это включает мониторинг операций с файлами, сетевых соединений, использование внешних устройств хранения и другие действия, потенциально угрожающие безопасности информации. Также создаются профили активности каждого сотрудника, основанные на его привычных действиях. Отклонения от нормального профиля (например, попытка скачивания большого объема данных или подключение неизвестного устройства) регистрируются системой и поступает сигнал руководству. При выявлении подозрительных действий система «Инсайдер» оперативно уведомляет службу информационной безопасности, позволяя своевременно принять необходимые меры по защите информации. Также контролируется передача файлов между сотрудниками, взаимодействие с внешними ресурсами, включая электронную почту, облачные сервисы и социальные сети [3, с. 56].

В системе «Инсайдер» имеются инструменты для быстрого анализа инцидентов информационной безопасности, сбора доказательств и составления отчетов, необходимых для дальнейшего расследования и принятия управленческих решений при возникновении угрозы. Предусмотренные в программном обеспечении автоматизированные процессы позволяют существенно сократить временные затраты на выявление потенциальных угроз и реагирование на возникающие инциденты [4, с. 48].

Стоит отметить, что преимуществами использования системы «Инсайдер» являются:

– минимизация риска утечек данных и краж интеллектуальной собственности;

– оперативное выявление потенциальных угроз ИБ, предотвращение происшествия и минимизация ущерба от инцидентов;

– улучшение эффективности службы информационной безопасности благодаря автоматизации рутинных задач и своевременному обнаружению угроз;

– повышение дисциплины и осознание важности вопросов информационной безопасности среди сотрудников.

Таким образом, использование специализированных систем, таких как «Инсайдер», становится необходимым условием устойчивого развития бизнеса и минимизации финансовых и репутационных рисков. В условиях, когда хозяйствующие субъекты постоянно сталкиваются с всевозрастающими требованиями по обеспечению информационной безопасности, особенно в условиях современных реалий и ужесточающихся нормативно-правовых актов в области защиты информации, подобные системы мониторинга значительно повышают уровень надежности организаций, предприятий, учреждений, помогая защитить их данные и бизнес-

процессы от внутренних и внешних угроз. Программы безопасного поведения и культуры информационной безопасности играют ключевую роль в обеспечении надежной защиты информации и снижении риска возникновения инцидентов ИБ в организации.

Список использованных источников:

1. Бондаренко И.С. Информационная безопасность: учебник / И.С. Бондаренко. М.: МИСИС, 2023. 254 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/360344 (дата обращения: 18.04.2025).

2. Никифорова Г.С. Психология менеджмента. Психологический практикум: учебное пособие / под ред. Г.С. Никифорова. 2-е изд. М.: Проспект, 2021. 504 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com /book/280712 (дата обращения: 18.04.2025).

3. Прохорова О.В. Информационная безопасность и защита информации: учебник для СПО / О.В. Прохорова. 6-е изд., стер. Санкт-Петербург: Лань, 2025. 124 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/445250 (дата обращения: 19.04.2025).

4. Яппаров Р.М. Роль и значение автоматизированных информационных систем в правоохранительной деятельности / Р.М. Яппаров // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов V Всероссийской молодежной научно-практической конференции, Уфа, 20–21 мая 2022 г. Уфа: Башкирский государственный университет, 2022. С. 48–53.

Ryabova K.A.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

ON THE NEED TO APPLY SAFE BEHAVIOR AND INFORMATION SECURITY CULTURE PROGRAMS (SBCP)

Abstract. The article reveals the features of using safe behavior and information security culture (SBCP) programs using the example of the INSIDER monitoring system software. The content of the article discusses and analyzes the problems of ensuring information security in the control and monitoring of working hours of company employees.

Keywords: information, rights, information protection, information protection system, work control, safe behavior programs, employee performance.

УДК 004.056

Хайруллина Г.Ф.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

ИСПОЛЬЗОВАНИЕ VIPNET EDI В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Аннотация. ViPNet EDI обеспечивает безопасный электронный документооборот, включая криптозащиту и поддержку ЭП. Соответствует требованиям ФСБ (сертификат № СФ/124-4369), интегрируется с СЭД и СМЭВ, минимизируя риски утечек. Решение подходит для госучреждений и бизнеса, работающего с конфиденциальными данными, гарантируя защиту на всех этапах – от создания до хранения документов в соответствии с российским законодательством.

Ключевые слова: ViPNet EDI, электронный документооборот, криптографическая защита, электронная подпись, ФСБ России, КСЗ.

Системы электронного документооборота (СЭД) широко используются в различных отраслях для управления и обмена документами [5]. СЭД позволяют автоматизировать процессы, увеличить эффективность работы и сократить время на выполнение задач. Однако, поскольку СЭД содержат конфиденциальную и важную информацию, то их безопасность становится критически важной [8]. Уязвимости в СЭД могут привести к несанкционированному доступу, утечке данных и нарушению целостности документов.

Совместное использование СЭД и ViPNet EDI создает многоуровневую систему защиты данных. Благодаря интеграции ViPNet EDI в систему электронного документооборота обеспечивается безопасность информации на каждом этапе ее существования – от создания до передачи и хранения. Внедряется комплекс мер, включающий шифрование информации, жесткую систему контроля доступа, настраиваемое распределение пользовательских прав и постоянное отслеживание всех операций. Этот подход позволяет существенно снизить вероятность утечек, исключить неавторизованные действия и обеспечить высокий уровень безопасности конфиденциальных сведений.

ViPNet EDI – это эффективное решение для информационной безопасности, предназначенное для надежной защиты данных и обеспечения их максимальной сохранности. ViPNet EDI использует передовые технологии шифрования и аутентификации, позволяя обеспечивать конфиденциальность, целостность и доступность информации. ViPNet EDI может быть интегрирован с различными системами, включая СЭД, что делает его универсальным решением для защиты информации [4].

Актуальность темы подчеркивается постоянными угрозами кибербезопасности, с которыми сталкиваются организации и частные лица. Кибератаки становятся все более изощренными и распространенными, что требует разработки и внедрения эффективных средств защиты. ViPNet EDI, как современное и надежное СЗИ, может помочь в борьбе с этими угрозами, обеспечивая защиту информации на уровне, соответствующем современным требованиям.

Согласно требованиям Федерального закона № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», организации, уполномоченные на оказание таких услуг, обязаны направлять необходимые документы и информацию в соответствующие органы и инстанции. Кроме того, на них возложена обязанность по запросу и получению нужных сведений и документов от других государственных органов и муниципальных учреждений [1].

Обмен информацией между федеральными и региональными органами исполнительной власти, а также различными учреждениями и организациями, осуществляющими государственные и муниципальные услуги через Единый портал госуслуг, а также в ходе выполнения государственных функций в цифровом формате, осуществляется через Систему межведомственного электронного взаимодействия (СМЭВ).

Решение ViPNet EDI G2G 3 предоставляет возможность организации электронного обмена данными через СМЭВ, эффективно связывая государственные органы, коммерческие структуры и граждан в процессе предоставления государственных услуг и реализации полномочий органов власти.

Решения ViPNet EDI G2G 3 предоставляют возможность организовать систему электронного документооборота внутри учреждения либо интегрировать данную платформу в уже действующие информационные среды. Продукт поддерживает использование усиленной квалифицированной электронной подписи, соответствующей требованиям Минцифры и ФСБ РФ, что является обязательным условием для участия в межведомственном электронном взаимодействии. С помощью этого решения можно управлять форматами документов, контролировать сроки их обработки и автоматизировать процессы обработки запросов в рамках СМЭВ. Кроме того, ViPNet EDI G2G 3 совместим с инфраструктурой удостоверяющих центров, другими системами ЭДО, средствами PKI, а

также с продуктами «ИнфоТеКС» для реализации электронной подписи [7] на клиентской, серверной и облачной сторонах.

Это решение также имеет сертификат соответствия ФСБ России № СФ/124-4369, который был выдан 25 октября 2022 г. для программного продукта ViPNet EDI Client 3 (ViPNet ЭДО АРМ Госуслуг 3).

Указанный сертификат подтверждает, что ViPNet EDI Client 3 соответствует стандартам криптографической защиты информации класса КС3, который не включает сведения, относящиеся к государственной тайне, и требованиям, установленным для средств электронной подписи в соответствии с приказом ФСБ России № 796 от 27 декабря 2011 г. [3] для класса КС3.

Данный продукт предназначен для обеспечения криптографической защиты [6], включая операции с хэш-функциями [2] файлов и данных в оперативной памяти, создание и проверку электронной подписи при обработке информации, не содержащей гостайну.

Список использованных источников:

1. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг». URL: https://www.consultant.ru/docшnent/consdoc LAW 103023/ (дата обращения: 17.04.24).

2. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования». URL: https://docs.cntd.ru/document/1200095035 (дата обращения: 17.04.24).

3. Приказ ФСБ РФ от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра». URL: https:/ /Ьase.garant.ru/70139150/ (дата обращения 08.04.25).

4. Духан Е.И., Синадский, Н.И., Хорьков, Д.А. Программно-аппаратные средства защиты компьютерной информации: практический курс, 2018. С. 191.

5. Коржук В.М., Попов, И.Ю., Воробьева, А.А. Защищенный документооборот. Часть 1. 2019. С. 49.

6. Нестеров С.А. Информационная безопасность: учебник и практикум для академического бакалавриата / С.А. Нестеров. М.: Юрайт, 2018. С. 322.

7. Трушин В.А. Введение в информационную безопасность и защиту информации: учебное пособие / В.А. Трушин. Новосибирск: Изд-во 1ПТУ, 2018. С. 132.

8. Яппаров Р.М. Некоторые проблемы защиты конфиденциальной информации в системах электронного документооборота / Р.М. Яппаров // Вестник Уфимского юридического института МВД России. 2019. № 1(83). С. 74–80.

Khairullina G. F.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

THE USE OF VIPNET EDI IN ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

Abstract. ViPNet EDI provides secure electronic document management, including cryptographic protection and item instance support. Complies with FSB requirements (certificate No. SF/124-4369), integrates with EDMS and SMEV, minimizing leakage risks.

The solution is suitable for government agencies and businesses working with confidential data, guaranteeing protection at all stages – from creation to storage of documents in accordance with Russian legislation.

Keywords: ViPNet EDI, electronic document management, cryptographic protection, electronic signature, FSB of Russia, CSR.

СЕКЦИЯ 4. КОНЦЕПЦИЯ И МЕТОДЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

УДК 004

Ахметов У.Р.
Российский государственный университет нефти и газа
(национальный исследовательский университет)
им. И.М. Губкина, Москва

Научный руководитель:
Корнилова А.А.
Уфимский университет науки и технологий, Уфа

ПОДДЕРЖКА ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ (2ФА) В ИНФРАСТРУКТУРЕ SAMBA AD

Аннотация. В данной статье рассматривается настройка двухфакторной аутентификации на основе инфраструктуры Samba AD. Осуществляется внедрение аппаратных решений в инфраструктуре Samba AD, где за основу взята российская разработка – Рутокен.

Ключевые слова: Samba AD, двухфакторная аутентификация, безопасность, аутентификация, Рутокен, Active Directory, Alt Linux.

В эпоху постоянных информационных угроз рассматривается вопрос повышения безопасности с доступом к корпоративным сетям. Чтобы решить данную проблему сегодня все чаще используют средства двухфакторной аутентификации (2ФА). Данный метод в современном мире является одним из наиболее эффективных способов защиты от несанкционированного доступа (НСД).

В данной работе рассматривается внедрение двухфакторной аутентификации в инфраструктуру Samba AD с использованием Рутокена.

Суть 2ФА заключается в проверки подлинности, который использует два различных фактора для подтверждения личности пользователя, что безусловно повышает уровень безопасности.

Выделяют три фактора аутентификации [1], используемые в различных комбинациях: на основе знания чего-либо, обладания чем-либо, на основе биометрических характеристик (табл. 1)

Таблица 1

Факторы аутентификации [2]

Фактор аутентификации	Классификация типов факторов аутентификации NCSC-TG-017	Примеры
На основе знания чего-либо (1-й)	Type 1: Authentication by Knowledge	Пароль или парольная фраза; PIN-код
На основе обладания чего-либо (2-й)	Type 2: Authentication by Ownership	Физический ключ; Карта с магнитной полоской; OTP-токен, генерирующий одноразовый пароль
На основе биометрических характеристик (3-й)	Type 3: Authentication by Characteristic	Отпечаток пальцев; Рисунок сетчатки; Голос

Принцип работы двухфакторной аутентификации состоит из двух взаимосвязанных компонентов:

1. Пароль, который требуется при доступе к ресурсу и хранится у пользователя.

2. Сгенерированный тип данных, который может храниться на физическом устройстве или в зависимости от времени пересоздаваться.

Только при наличии этих компонентов у пользователя имеется доступ к данным.

Для реализации данной технологии существуют различные инструменты двухфакторной аутентификации (табл. 2).

Таблица 2

Инструменты двухфакторной аутентификации

Категория	Название	Описание	Linux пакеты
1	*2*	*3*	*4*
Аутентификационные приложения (Authenticator Apps)	Google Authenticator	Наиболее востреебованные приложение среди аналогов, позволяющее генерировать временные, одноразовые пароли	libpam-google-authenticator
	Microsoft Authenticator	Аналог Google Authenticator, с дополнительными функциями	authenticator
	Authy	Аналог с мультиустройственной синхронизацией, так же поддерживает защиту удаленных акаунтов	Perl-WWW-Authy

Окончание табл. 2

1	*2*	*3*	*4*
Аппаратные токены (Hardware Tokens)	Рутокен	Российская разработка для аппаратной аутентификации и ЭЦП (электронной цифровой подписи)	pcsc-lite-ccid, libpcsclite, pcsc-tools, opensc
SMS и Голосовая аутентификация	SMS	Отправка одноразового кода через SMS или звонок на телефон (последнии цифры номера)	Платформа OpenUDS Server: *openuds-server-nginx*
	Голосовые вызовы	Отправка кодов с помощью голосового вызова	Платформа OpenUDS Server: *openuds-server-nginx*
Биометрическая аутентификация	Распознавание голоса	Встроенное устройство, для сканирования отпечатка пальца (широко распространено)	Платформа VoiceKey.PLATFORM: vk-monitoringcomponent vk-routercomponent vk-securitycomponent vkchroniclercomponent vk-databasecomponent vk-licensingcomponent vk-mediahubcomponent vk-voicegridprocessor
	Распознавание лица	Встроенное устройство для распознавания биометрии лица. Технология, используемая в Apple Face ID и других	howdy
Программные решения для интеграции 2ФА	Duo Security	Поддерживает широкий спектр решений для аутентификации	duo_unix
	Okta Verify	Облачный сервис, который позволяет управлять удостоверениями и доступом	Okta (через API)

В нашем случае для примера реализации 2ФА был выбран Рутокен ЭЦП 3.0. Это активный ключевой носитель, являющийся представителем новой линейки USB-токенов и смарт-карт для подписания документов электронной подписью и строгой 2ФА на настольных и мобильных устройствах. Продукты линейки являются полнофункциональными аппаратными СКЗИ [3].

В смарт-картах и USB-токенах аппаратно-реализованы: ГОСТ Р 34.10–2012.3 [4] с длиной ключа 256/512 бит и ГОСТ Р 34.11–2012.4 [5], а также симметричные шифры Магма и Кузнечик и международные алгоритмы электронной подписи RSA и ECDSA. Криптографические операции выполняются без копирования ключа в память компьютера.

Часть моделей линейки, помимо традиционного контактного интерфейса, оснащена бесконтактным интерфейсом (NFC). При этом функции устройств доступны через оба интерфейса. Это позволяет подписывать документы на смартфонах и планшетах так же легко, как расплачиваться бесконтактной банковской картой, при наличии поддержки в используемом мобильном приложении.

Настройка Samba AD на базе ОС ALT Linux и интеграция с Рутокеном реализована по следующему алгоритму:

Шаг 1: Подготовка программного обеспечения. Обновляем репозитории и устанавливаем необходимые компоненты:

Шаг 2: Подключение устройства и генерация ключевой пары.

Шаг 3: Создание сертификата.

Шаг 4: Настройка локальной аутентификации с использованием Рутокена.

Шаг 5: Финальное тестирование.

Таким образом в данной работе реализована поддержка двухфакторной аутентификации в инфраструктуре SAMBA AD.

Список использованных источников:

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; под ред. А.А. Шелупанова, С.Л. Грузаева, Ю.С. Нахаева. М.: 2009. 552 с.

2. NCSC-TG-017 – документ «A Guide to Understanding Identification and Authentication in Trusted Systems», опубликованный U.S. National Computer Security Center. Руководство содержит комплект рекомендуемых инструкций по процедурам идентифицкации и аутентификации.

3. Уймин, А.Г. Разработка методики тестирования системы безопасности автоматизированных систем управления технологическими процессами на основе корпоративного стандарта // Автоматизация и информатизация ТЭК. 2024. Т. 610. № 5. С. 59–65.

4. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электр-

онной цифровой подписи» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. № 215-ст).

5. ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. № 216-ст).

Akhmetov U.R.
Gubkin Russian State University of Oil and Gas (National Research University), Moscow

Scientific supervisor:
Kornilova A.A.
Ufa University of Science and Technology, Ufa

SUPPORT FOR TWO-FACTOR AUTHENTICATION (2FA) IN SAMBA AD INFRASTRUCTURE

Abstract. This article discusses setting up two-factor authentication based on the Samba AD infrastructure. The implementation of hardware solutions in the Samba AD infrastructure is carried out, where the Russian development - Rutoken - is taken as a basis.

Keywords: Samba AD, two-factor authentication, security, authentication, Rutoken, Active Directory, Alt Linux.

УДК 004

Биктубаева К.С.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шафиков М.Р.
Уфимский университет науки и технологий, Уфа

АДВЕРСАРНЫЕ АТАКИ НА ZERO TRUST-СИСТЕМЫ: УЯЗВИМОСТИ И МЕТОДЫ ЗАЩИТЫ

Аннотация. Архитектура Zero Trust считается перспективной для защиты от современных киберугроз. Однако ее внедрение не гарантирует абсолютной защиты: злоумышленники разрабатывают адверсарные атаки, направленные на обход механизмов непрерывной аутентификации, манипуляцию контекстно-зависимыми политиками и эксплуатацию уязвимостей машинного обучения, используемого в ZT-системах. В данной статье анализируются основные уязвимости архитектуры

нулевого доверия и предлагаются стратегии защиты, такие как адаптивная аутентификация, устойчивые к манипуляциям модели машинного обучения и гибридные методы обнаружения аномалий.

Ключевые слова: Zero Trust, адверсарные атаки, машинное обучение, динамический контроль доступа, кибербезопасность.

Zero Trust (ZT, нулевое доверие) – концепция информационной безопасности, предполагающая отсутствие доверия к каким бы то ни было объектам IT-инфраструктуры организации, будь то пользователи, устройства или программы. Концепция ZT радикально меняет парадигму кибербезопасности, заменяя традиционные модели на постоянную верификацию пользователей, устройств и транзакций [1].

Адверсарные атаки (adversarial attacks, состязательные атаки) – это тип атак, направленных на обман или вывод из строя моделей машинного обучения. В отличие от традиционных кибератак, которые нацелены на взлом систем или кражу данных, адверсарные атаки манипулируют входными данными модели, заставляя ее выдавать неправильные результаты, совершать ошибки или демонстрировать неожиданное поведение [2].

С 2021 по 2024 г. наблюдается значительный рост числа кибератак, что затрагивает и системы, основанные на концепции ZT. По данным FACCT с 2021 по 2023 г. число инцидентов увеличилось в 3 раза. Пик пришелся на 2022–2023 г., что было связано с массовым переходом компаний на ZT-модель без должной адаптации механизмов защиты. В 2024 г. темпы роста снижаются, однако значения остаются высокими. Это свидетельствует о том, что, несмотря на постепенную адаптацию ZT, угрозы эволюционируют.

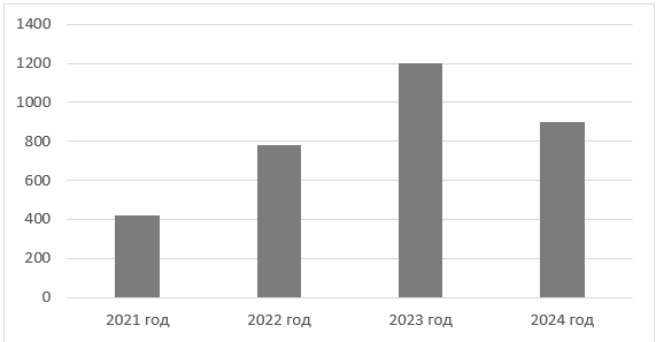

Рис. 1. Количество адверсарных атак на Zero Trust-системы за 2021–2024 гг.

Архитектура (ZT) демонстрирует высокую устойчивость к традиционным кибератакам, но все же подвержена и остается уязвимой к ряду адверсарных атак [3]. Рассмотрим основные векторы атак, которые можно классифицировать на три основные категории:

1. Уязвимости аутентификации и авторизации. Механизмы аутентификации и авторизации являются основными уязвимостями в архитектурах ZT. Ключевые угрозы включают компрометацию учетных данных через фишинг и атаки типа Credential Stuffing, обход многофакторной аутентификации (например, с помощью SIM-свопинга и MITM-атак), а также кражу токенов доступа (JWT/OAuth через XSS/CSRF). Особенно опасной является подмена refresh_token, которая позволяет сохранять доступ даже после изменения учетных данных. В среде ZT, где каждый запрос требует аутентификации, эти уязвимости могут стать критическими точками отказа.

2. Уязвимости микросервисной архитектуры и API. Переход на микросервисную архитектуру в Zero Trust-системах, несмотря на свои преимущества, создает новые векторы для потенциальных атак, особенно через уязвимости API. Согласно OWASP API Top 10, наиболее опасными являются атаки типа BOLA (Broken Object Level Authorization), позволяющие злоумышленникам получать несанкционированный доступ к данным через манипуляцию идентификаторами объектов, а также различные виды инъекций (SQLi, NoSQLi), эксплуатирующие недостаточную валидацию входных параметров при запросах к базам данных [4]. Не менее серьезной угрозой является подмена параметров API, когда злоумышленники изменяют HTTP-заголовки или query-параметры с целью эскалации привилегий. Эти проблемы становятся серьезнее из-за плохого разделения сети между микросервисами. Взломав один сервис, злоумышленник может атаковать другие.

3. Уязвимости систем мониторинга и машинного обучения. Злоумышленники стали активно использовать стандартные инструменты администрирования (PowerShell, RDP) для маскировки вредоносных действий под обычную работу администраторов. В тоже время стремительно развиваются adversarial ML-атаки, злоумышленники искусно подделывают данные, чтобы аномалии оставались незамеченными [5]. Атакующие специально создают множество ложных тревог, чтобы перегрузить аналитиков и скрыть настоящие атаки. Также они используют медленный подбор данных, который часто проходит незамеченным из-за неправильных настроек систем защиты. Данные методы демонстрируют, что даже современные системы мониторинга на основе машинного обучения (ML) не обладают абсолютной устойчивостью, поэтому необходимо постоянно совершенствовать алгоритмы обнаружения [6].

Для эффективного противодействия выявленным уязвимостям Zero Trust-систем, выделяют следующие меры защиты:

Для защиты механизмов аутентификации и авторизации в Zero Trust-системах необходимо реализовать многоуровневый подход. Во-первых, использовать современные методы входа – биометрию (сканирование отпечатков пальцев или лица) и физические ключи безопасности вместо ненадежных SMS-кодов, дополняя это проверкой привычного

местоположения и устройств пользователей для выявления подозрительных попыток доступа; во-вторых, усиленно защищать токены доступа – устанавливать короткий срок их действия (не более 15 минут), применять электронную подпись и систему мгновенной блокировки при компрометации; в-третьих, регулярно проводить комплексные проверки – контролировать настройки системы входа, проверять ссылки перенаправления, шифровать серверы выдачи токенов и своевременно устранять обнаруженные уязвимости.

Для защиты микросервисов и API в ZT-средах необходимо реализовать комплекс мер. На уровне API-шлюзов критически важны: проверка прав доступа к каждому объекту, блокировать вредоносные команды, ограничивать частоту обращений [7]. Использовать защищенные соединения, выдавать минимальные права, применять принцип «запрещено все, что не разрешено». Обязательным элементом является мониторинг всех API-вызовов с анализом аномалий и автоматической блокировкой массовых или подозрительных запросов.

Для эффективного противодействия сложным атакам, таким как Adversarial ML, необходимо совершенствовать системы мониторинга и машинного обучения. Ключевыми мерами являются: внедрение устой--чивых ML-моделей, включая алгоритмы обнаружения аномалий и регулярного проверять их на уязвимость, совмещать поведенческий анализ с проверкой известных шаблонов атак, а также автоматически адаптировать чувствительность систем для выявления медленных и скрытых атак.

Исследование адверсарных атак на системы ZT-системы имеет важное практическое значение для современной кибербезопасности, поскольку выявляет ключевые уязвимости перспективной архитектуры и предлагает конкретные меры защиты. Полученные результаты позволяют организациям, внедряющим ZT, заранее устранять слабые места в механизмах аутентификации, защите API и системах мониторинга. Но, несмотря на существующие уязвимости, концепция ZT при правильной реализации и постоянном совершенствовании остается одним из наиболее перспективных подходов к обеспечению кибербезопасности в современных условиях.

Список использованных источников:

1. Национальный институт стандартов и технологий (NIST). Zero Trust Architecture (NIST Special Publication 800-207). 2020. URL: https://newsletter.radensa.ru/wp-content/uploads/2025/ 01/NIST-SP800-207.pdf.

2. Krivonogov A.A., & Petrov V.S. (2023). Explainable Adversarial Mitigation Framework for Zero-Trust Cyber Warfare. ResearchGate. URL: https://www.researchgate.net/publication/375071924_Explainable_Adversarial_Mitigation_Framework_for_Zero-Trust_Cyber_Warfare.

3. Многоагентные системы как технологическая база реализации концепции нулевого доверия / С.С. Валеев, Н.В. Кондратьева,

М.Б. Гузаиров, А.С. Исмагилова // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2024. № 3. С. 116–123.

4. Open Web Application Security Project (OWASP). OWASP API Security Top 10 2023. 2023. URL: https://owasp.org/API-Security.

5. Smith J., Johnson A. Advanced Adversarial Attacks on Machine Learning Systems. Springer, 2022. 315 p. URL: https://link.springer.com/book/10.1007/978-3-030-99772-4.

6. TechRepublic. Zero Trust Security: A Cheat Sheet (Free PDF). 2023. URL: https://www.techrepublic.com/resource-library/downloads/zero-trust-security-a-cheat-sheet-free-pdf/.

7. Zhang L., Wang Y. Adversarial Attacks on Zero Trust Security Systems: Methods and Countermeasures // arXiv preprint. 2021. URL: https://arxiv.org/pdf/2112.02797.

Biktubaeva K.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shafikov M.R.
Ufa University of Science and Technology, Ufa

ADVERSARIAL ATTACKS ON ZERO TRUST SYSTEMS: VULNERABILITIES AND PROTECTION METHODS

Abstract. The Zero Trust architecture is considered promising for protection against modern cyber threats. However, its implementation does not guarantee absolute protection: attackers develop adversarial attacks aimed at bypassing continuous authentication mechanisms, manipulating context-sensitive policies, and exploiting machine learning vulnerabilities used in ZT systems. This article analyzes the main vulnerabilities of the zero-trust architecture and suggests protection strategies such as adaptive authentication, manipulation-resistant machine learning models, and hybrid anomaly detection methods.

Keywords: Zero Trust, adversarial attacks, machine learning, dynamic access control, cybersecurity.

УДК 004.056

Давлетова Д.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

ПОСТРОЕНИЕ МОДЕЛИ ДУБЛИРОВАНИЯ ПОДСИСТЕМ В ЗАЩИТЕ ИНФОРМАЦИИ

Аннотация. Защита информации является критически важной задачей во многих областях деятельности человека – от бизнеса до государственного управления. Одним из способов повышения надежности защиты информации выступает дублирование подсистем, обеспечивающих безопасность информационных ресурсов. Данная работа посвящена построению модели дублирования подсистем в защите информации.

Ключевые слова: защита информации, дублирование подсистем, построение модели.

Метод дублирования подсистем является эффективным способом повышения надежности и устойчивости информационных систем перед внешними угрозами и внутренними сбоями. Однако простое внедрение дублирующих механизмов недостаточно для полноценного совершенствования системы защиты информации [1]. Необходимо учитывать ряд аспектов и направлений развития:

1. Избыточность аппаратных ресурсов.

Следует использовать избыточные серверы, базы данных, сетевые устройства и другие компоненты инфраструктуры, работающие параллельно. Например, активация механизма горячего резерва позволяет мгновенно переключаться на запасной узел при отказе основного компонента.

Основные преимущества: повышается доступность системы, сокращается время реакции на аварийные ситуации.

2. Географическая распределенность дублируемых узлов.

Размещение дублирующих элементов в различных географических зонах, удаленных друг от друга. Это снижает риск одновременного отказа нескольких ключевых узлов вследствие природных катастроф, атак хакеров или иных чрезвычайных ситуаций.

Основные преимущества: устойчивость к локальным происшествиям, улучшенная защита от внешних воздействий.

3. Мониторинг и автоматическое обнаружение неисправностей.

Автоматизированные инструменты постоянного мониторинга состояния каждого узла позволяют своевременно выявлять отклонения и предупреждать инциденты еще до возникновения серьезных проблем. [2-3]

Основные преимущества: быстрое реагирование на неисправности, минимизация риска потери данных и нарушений непрерывности бизнеса.

4. Регулярные проверки готовности дублированных решений.

Проведение периодического тестирования дублирующих подсистем путем планового отключения основных компонентов имитирует реальные условия эксплуатации и проверяет работоспособность резервных ресурсов.

Основные преимущества: постоянная готовность дублирующих элементов, своевременное выявление слабых мест и недостатков архитектуры.

Для успешного внедрения метода дублирования подсистем в системах защиты информации важно соблюдать определенные шаги и подходы. Ключевые этапы процесса внедрения:

Этап 1: Анализ существующей инфраструктуры.

Перед внедрением метода дублирования необходимо провести детальный аудит текущих технических ресурсов и архитектурных особенностей вашей системы. Проверить состояние используемых физических и виртуальных серверов, сетей, хранилищ данных и прочих компонентов. Определить слабые места и наиболее уязвимые участки сети. Оценить потенциальные угрозы и риски, связанные с авариями, взломами и отказами оборудования.

Этап 2: Выбор стратегии дублирования.

Существует несколько стратегий дублирования подсистем, каждая из которых имеет свои особенности и подходит для конкретных сценариев:

Активно-пассивная стратегия: один экземпляр постоянно функционирует, а второй ожидает своей очереди активации в случае аварии первого.

Активно-активная стратегия: оба экземпляра функционируют одновременно, распределяя нагрузку между собой.

Географически распределенная система: дублируемые ресурсы находятся в разных географических точках, уменьшая влияние локальных происшествий.

Этап 3: Проектирование архитектуры.

Проектировать архитектуру стоит таким образом, чтобы минимизировать возможные точки отказа и обеспечить быстрое переключение между основными и резервными элементами. Использовать специализированные решения для балансировки нагрузки и автоматического перенаправления трафика при выходе одного из узлов из строя. Применять механизмы хранения конфигураций и протоколов взаимодействия между элементами системы.

Этап 4: Тестирование и проверка.

После разработки проекта необходимо провести тщательное тестирование дублирующей системы:

Имитация реальных условий работы, проверка возможности быстрого перехода на резервные узлы, отработка сценария запуска при возникновении неполадок в основной системе.

Тестирование должно выявить любые недостатки и убедиться в работоспособности системы в экстремальных ситуациях.

Этап 5: Внедрение и мониторинг.

Важно контролировать процесс миграции данных и настроек, регулярно проверять корректность функционирования дублирующих элементов. Следует настроить системы мониторинга для оперативного выявления отклонений и ошибок, а также организовать процедуры регулярного анализа состояния системы и внесения изменений по мере необходимости.

Рекомендации по успешному внедрению.

Выбор оптимального уровня дублирования. Не обязательно дублировать абсолютно все оборудование, можно выбрать важные модули и системы, требующие повышенной защищенности.

Обучение персонала. Сотрудники, обслуживающие инфраструктуру, должны четко понимать принципы работы дублированных систем и уметь быстро реагировать на нестандартные ситуации.

Постоянное улучшение процессов. После завершения этапа внедрения следует продолжать анализировать работу системы, вносить необходимые усовершенствования и устранять возникающие проблемы.

Модель дублирования подсистем в защите информации представляет собой организационно-техническое решение, направленное на обеспечение непрерывности работы информационной системы даже при частичном выходе из строя отдельных ее компонентов. Такая модель основывается на принципе наличия дополнительного оборудования или программных модулей, готовых принять на себя выполнение функций вышедших из строя элементов. [3]

Ключевые элементы модели дублирования подсистем:

1. Основной рабочий модуль.

Это первичный ресурс, обеспечивающий нормальное функционирование информационной системы. Обычно это сервер, база данных, сетевое устройство или другое важное звено IT-инфраструктуры.

2. Резервный модуль.

Дополнительный компонент, аналогичный основному рабочему модулю, готовый немедленно заменить последний в случае его отказа. Существует две основных формы резервирования:

Горячий резерв: модуль постоянно готов к работе и подключен к сети, ожидая сигнала о переходе в активный режим.

Холодный резерв: резервный модуль отключен и должен пройти процедуру подготовки к запуску перед началом полноценной работы.

3. Система обнаружения неисправностей.

Специальный механизм контроля и диагностики, отслеживающий состояние обоих модулей. Он способен оперативно фиксировать

возникновение проблем в основном рабочем модуле и инициировать переход на резервный элемент.

4. Механизм переключения.

Механизм переключения определяет порядок действий при обнаружении неисправности. Возможны различные сценарии:

Автоматический перенос нагрузки на резервный модуль без участия оператора.

Предупреждение администратора о возникшей проблеме с возможностью ручного принятия решения.

Типовые схемы реализации моделей дублирования:

1. Active-Passive схема («основной + горячий резерв»).

Основной рабочий модуль активно обрабатывает запросы пользователей, пока резервный находится в состоянии ожидания. При выходе из строя основного модуля нагрузка сразу переходит на резервный, поддерживая непрерывность обслуживания.

Пример реализации: серверная инфраструктура с двумя серверами, где один сервер активно обслуживает клиентов, а второй готов вступить в действие при любом сбое.

2. Active-Active схема («двойная активность»).

Оба модуля функционируют одновременно, разделяя нагрузку между собой. Если один из них выходит из строя, оставшийся модуль берет на себя всю рабочую нагрузку.

Пример реализации: базы данных, хранящиеся на нескольких независимых серверах, работающих параллельно и осуществляющих взаиморезервирование.

Практические аспекты проектирования модели дублирования.

При проектировании модели дублирования стоит учитывать следующие моменты:

– технические характеристики оборудования и совместимость компонентов;

– время переключения на резервный модуль и возможная потеря данных;

– уровень автоматизации процесса переключения и необходимость вмешательства человека.

– стоимость приобретения и поддержки резервных элементов.

Таблица 1

Плюсы и минусы использования модели дублирования

Преимущества	Недостатки
Высокая надежность и стабильность работы системы	Дополнительные расходы на приобретение и эксплуатацию оборудования
Незначительные перерывы в обслуживании при отказах оборудования	Требуется грамотное проектирование и настройка механизма переключения
Повышенный уровень защиты от угроз и кибератак	Ограниченные возможности масштабирования при увеличении числа элементов

Модели дублирования подсистем являются важным инструментом повышения надежности и безопасности информационных систем. Их применение оправдано там, где необходима высокая степень бесперебойности и устойчивости к внешним воздействиям. Грамотное проектирование и правильная реализация обеспечивают значительную выгоду для организаций любого масштаба.

Список использованных источников:

1. Исмагилова А.С. Количественная оценка рекомпозиционной системы защиты информации / А.С. Исмагилова, И.А. Шагапов, И.В. Салов // Инженерный вестник Дона. 2024. № 8 (116). С. 273–281.

2. Давлетова Д.Р. Дублирование в защите информации / Д.Р. Давлетова, И.А. Шагапов // Естественные и технические науки. 2024. № 12 (199). С. 266–304.

3. Шагапов И.А. Рекомпозиционный подход в защите информации / И.А. Шагапов, А.С. Исмагилова, И.В. Салов // Международный форум KAZAN DIGITAL WEEK – 2021: сборник материалов, Казань, 21–24 сентября 2021 г. Том Часть 1. Казань: ГБУ «НЦБЖД», 2021. С. 275–282.

4. Шагапов И.А. К механизму переключения состояний системы защиты информации при использовании рекомпозиционного подхода / И.А. Шагапов // Естественные и технические науки. 2023. № 12 (187). С. 300–304.

Davletova D.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A
Ufa University of Science and Technology, Ufa

BUILDING A MODEL OF SUBSYSTEM DUPLICATION IN INFORMATION SECURITY

Abstract. Information protection is a critically important task in many areas of human activity, from business to public administration. One of the ways to increase the reliability of information security is the duplication of subsystems that ensure the security of information resources. This work is devoted to the construction of a model of duplication of subsystems in information security.

Keywords: information protection, subsystem duplication, model construction.

УДК 004

Давлетшина Э.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Фатхелисламов А.Ф.
Уфимский университет науки и технологий, Уфа

ИСПОЛЬЗОВАНИЕ RSA-КЛЮЧЕЙ ДЛЯ АВТОРИЗАЦИИ

Аннотация. В данной статье рассматривается концепция RSA-ключей, их сущность и значение, а также роль RSA-ключей в процессе авторизации. В рамках исследования будут рассмотрены практические аспекты использования RSA-ключей для авторизации. RSA (Rivest-Shamir-Adleman) представляет собой один из наиболее распространенных алгоритмов асимметричного шифрования, который обеспечивает безопасность передачи данных и аутентификацию пользователей. Статья освещает основные принципы работы RSA, его применение в современных системах безопасности и значимость для защиты информации.

Ключевые слова: авторизация, RSA, RSA-ключи, информационная безопасность.

Безопасность информации является одной из важнейших задач в XXI в. Многие специалисты ИТ-отрасли ежедневно разрабатывают различные методы и способы защиты информации, а хакеры, напротив, с каждым днем создают все новые вредоносы, эксплоиты и другие инструменты для взлома системы и кражи данных. Своеобразная гонка между хакерами и «защитниками информации» приводит к необходимости развития развитием информационных технологий. При развитии информационных технологий происходит и увеличением объема передаваемых данных. Таким образом, возрастает необходимость в надежных методах аутентификации и защиты информации. Один из методов защиты информации является ее шифрование, т. е. приведине информации в такое состояние, в котором хакер не сможет ее понять или как-либо использовать. В рамках данной статьи будет рассматриваться в основном асимметричное шифрование, а в частности алгоритм RSA. Данный алгоритм стал основой для многих современных систем безопасности. Под системой безопасности в данной статье рассматривается комплекс программно-технических и/или аппаратных инструментов, которые помогают защитить цифровую информацию - базы данных, текстовую информацию и другие виды. Итак, RSA-ключи, это часть криптографического алгоритма шифрования. Они состоят из пары открытого и закрытого ключей, обеспечивают безопасный обмен данными

и аутентификацию пользователей, что делает их важным инструментом в области кибербезопасности.

Алгоритм RSA имеет свои принципы работы, которые позволяют обеспечить защиту информации, путем использования вычислительных мощностей цифровой техники. Алгоритм RSA основан на математических свойствах больших простых чисел и сложности задачи факторизации [1]. Процесс генерации RSA-ключей включает следующие этапы:

Первый – это выбор двух больших простых чисел: Пусть p и q – два больших простых числа, которые должны быть выбраны случайным образом. Размер этих чисел определяет уровень безопасности ключа. Например, для обеспечения достаточной безопасности в текущем году рекомендуется использовать ключи длиной не менее 2048 бит.

Второй – это вычисление модуля, так модуль n вычисляется как $n=p\times q$. Этот модуль используется как основа для шифрования и дешифрования.

Третий этап – это вычисление функции Эйлера. Функция Эйлера

$\phi(n)=(p-1)(q-1)$ используется для определения количества чисел, меньших n, которые взаимно просты с n.

Четвертым этапом будет являться как раз выбор открытого ключа. Алгоритм выбирает целое число e, такое что $1<e<\phi(n)$ и e взаимно просто с $\phi(n)$. Обычно выбирается стандартное значение $e = 65537$, так как оно обеспечивает хороший баланс между безопасностью и эффективностью.

Последний этап – это вычисление закрытого ключа. В таком виде закрытый ключ d вычисляется как мультипликативная обратная к e по модулю $\phi(n)$, то есть $d\cdot e \equiv 1 mod \phi(n)$. Это можно сделать с помощью алгоритма Евклида.

Пара ключей (e,n) и (d,n) образует открытый и закрытый ключи соответственно. Открытый ключ может быть свободно распространен, в то время как закрытый ключ должен храниться в секрете.

Рассмотрим практическое применение RSA-ключей для авторизации.

RSA-ключи находят широкое применение в различных аспектах авторизации и аутентификации. Основные области их использования включают: шифрование данных, цифровые подписи, аутентификацию пользователей и безопасный обмен ключами.

Рассмотрим каждую область:

Шифрование данных – открытый ключ используется для шифрования сообщений, которые могут быть расшифрованы только с помощью соответствующего закрытого ключа. Это обеспечивает конфиденциальность передаваемой информации.

Цифровые подписи – RSA позволяет создавать цифровые подписи, которые подтверждают подлинность и целостность сообщения. Отправитель шифрует хэш-сумму сообщения с помощью своего закрытого ключа, а получатель может проверить подпись, расшифровав ее открытым ключом отправителя. Для создания хэш-суммы обычно используются криптографические хэш-функции, такие как SHA-256.

Аутентификация пользователей – в системах, требующих аутентификации, RSA-ключи могут использоваться для подтверждения личности пользователя. При входе в систему пользователь может предоставить свой открытый ключ, а сервер проверяет его подлинность, используя соответствующий закрытый ключ.

Безопасный обмен ключами – RSA может быть использован для безопасной передачи симметричных ключей, которые затем применяются для шифрования данных с использованием более быстрых симметричных алгоритмов, таких как AES [2]. Это позволяет комбинировать преимущества асимметричного и симметричного шифрования.

Использование RSA-ключей для авторизации имеет несколько ключевых преимуществ, например, безопасность, ведь RSA обеспечивает высокий уровень безопасности благодаря сложности задачи факторизации больших чисел. Это делает его устойчивым к атакам, что особенно важно в условиях современных угроз.

Примером будет являться гибкость использования данных ключей, ведь RSA-ключи могут быть использованы в различных сценариях, включая шифрование, цифровые подписи и аутентификацию, что делает их универсальным инструментом в области кибербезопасности.

Использование цифровых подписей и аутентификации на основе RSA способствует созданию доверительных отношений между пользователями и системами, что является важным аспектом в электронной коммерции и других областях. Также, RSA является стандартом в области криптографии и широко поддерживается различными протоколами и системами, такими как SSL/TLS, PGP и другие, что упрощает его интеграцию в существующие решения.

Рассмотрим практические кейсы, которые помогут подчеркнуть ценность RSA-ключей. Необходимо создать защищенный канал передачи данных - для этого отлично подойдет шифрование канала. В таком случае открытый ключ используется для шифрования сообщения, а закрытый ключ – для его расшифровки. То есть информация будет передаваться, но при этом, она будет полезна только тем, у кого есть закрытый ключ.

RSA также широко используется для создания цифровых подписей, которые подтверждают подлинность и целостность данных. Рассмотрим этот случай подробнее. Процесс цифровой подписи, путем использования RSA включает следующие шаги:

1. Создание подписи. Этап, когда отправитель создает хэш-сумму сообщения с помощью криптографической хэш-функции (например, SHA-256) и затем шифрует эту хэш-сумму своим закрытым ключом. Полученная подпись прикрепляется к сообщению.

2. Проверка подписи. Этап, в котором получатель может расшифровать подпись с помощью открытого ключа отправителя, чтобы получить хэш-сумму. Затем он сравнивает ее с хэш-суммой, вычисленной из полученного сообщения. Если они совпадают, это подтверждает, что сообщение не

было изменено и действительно было отправлено указанным отправителем.

Разумеется, при использовании данного шифрования в информационных системах, все операции происходят в автоматическом режиме, путем использования технических мощностей вычислительной техники.

Другой пример – RSA является основой для многих протоколов безопасности, таких как SSL/TLS, которые используются для защиты интернет-трафика. В этих протоколах RSA-ключи применяются для установления защищенного соединения и аутентификации сторон. При инициации соединения клиент и сервер обмениваются открытыми ключами и используют их для шифрования данных, что обеспечивает защиту от перехвата и подмены информации. После сервер может использовать свой закрытый ключ для создания цифровой подписи, подтверждающей его подлинность, что позволяет клиенту убедиться, что он подключается к правильному серверу.

Резюмируя, RSA-ключи представляют собой важный инструмент для обеспечения безопасности и аутентификации в цифровом мире. Их применение в шифровании данных, цифровых подписях и аутентификации пользователей способствует защите информации и созданию доверительных отношений между сторонами. В условиях растущих угроз кибербезопасности использование RSA-ключей становится необходимым для обеспечения конфиденциальности и целостности данных, что подчеркивает их значимость в современных информационных системах.

Список использованных источников:

1. Белоус А.И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения: учебник / А.И. Белоус. М.: Техносфера, 2021. 483 с. (дата обращения 28.03.2025). Текст: непосредственный.

2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. М.: ФОРУМ: ИНФРА-М, 2021. 416 с. (дата обращения 28.03.2025). Текст: непосредственный.

Davletshina E.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhelislamov A.F.
Ufa University of Science and Technology, Ufa

USE OF RSA KEYS FOR AUTHORIZATION

Abstract. This article discusses the concept of RSA keys, their essence and meaning, as well as the role of RSA keys in the authorization process. The study will consider the practical aspects of using RSA keys for authorization. RSA

(Rivest-Shamir-Adleman) is one of the most common asymmetric encryption algorithms that ensures the security of data transmission and user authentication. The article covers the basic principles of RSA, its application in modern security systems and its importance for information protection.
Keywords: authorization, RSA, RSA keys, information security.

УДК 004

Загидуллина А.У.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Фатхелисламов А.Ф.
Уфимский университет науки и технологий, Уфа

ШИФРОВАНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ ДЛЯ ЛИЧНОГО ПОЛЬЗОВАНИЯ

Аннотация. В эпоху цифровых технологий и повсеместного распространения интернета, защита личной информации становится одной из важнейших задач. Личная информация – это ценный ресурс, за обеспечение безопасности которого должен отвечать сам человек.

В данной статье рассматриваются методы шифрования электронной почты для личного пользования, их преимущества и недостатки, а также рекомендации по выбору подходящих инструментов. Особое внимание уделяется практическим аспектам внедрения шифрования в повседневное использование электронной почты.

Ключевые слова: шифрование, электронная почта, информационная безопасность, информация.

Под личной информацией может пониматься все что угодно, например, личная переписка, заметки, статьи (результаты интеллектуальной деятельности человека) и т. д. Соответственно, хранится личная информация может также в различных формах и источниках, будь то записная книжка, цифровые файлы в компьютере и даже электронная почта.

По данным исследований, более 90 % электронных писем содержат спам или фишинг-атаки, что подчеркивает необходимость защиты личной информации.

Защитить свою электронную почту можно различными методами и способами, начиная от организационных – установка сложного пароля и его изменение каждые 3 месяца, заканчивая техническими, куда можно отнести использование защищенного почтового агента, двухфакторную аутентификацию, услуги провайдера по защите электронной почты, а также шифрование.

Шифрование электронной почты позволяет защитить содержимое сообщений от несанкционированного доступа, обеспечивая конфиденциальность и целостность данных. Шифрование электронной почты может быть выполнено различными методами:

Первым методом будет являться полное шифрование любого исходящего письма, для этого пользователь должен использовать программу шифратор и ключ, для шифрования писем. Пользователь пишет необходимый текст в программу шифратор и при обработке текста получает не связанные символы, которые может отправить. Получатель письма копирует эти несвязанные символы, вставляет их в программу шифратор, указывает ключ и получает расширенное послание. Данный способ является очень редким, носит большое количество недостатков, а также является неудобным ни пользователю, ни получателю писем.

Вторым методом будет являться шифрование внутри клиента электронной почты, для этого пользователь и получатели электронных писем должны использовать единый клиент и единый ключ. Пользователь использует свою электронную почту, как и обычно, но через защищенной клиент, в таком случае, если злоумышленник входит в аккаунт электронной почты с обычного клиента он увидит лишь зашифрованные переписки. При этом получатели будут видеть реальный текст письма, только в том случае, если используют защищенный клиент и ввели необходимый ключ или установили необходимый сертификат

Третий метод – шифрование файла, содержащего письмо и отправка по обычному клиенту или веб-версии электронной почты. Пользователь пишет необходимый текст в файле (в word-файле), после чего шифрует этот файл и направляет получателю. Получатель скачивает данный файл и дешифрует его через указанное программное обеспечение или веб-ресурсы (при наличии ключа).

Далее следует рассмотреть сами методы шифрования, а именно симметричное и ассиметричное.

Асимметричное шифрование более безопасно, так как не требует передачи закрытого ключа, однако оно требует больше вычислительных ресурсов и может быть медленнее, чем симметричное шифрование [1].

Следует учитывать, что если шифрование настраивается на специальном клиенте или шифруется сам файл, то для выполнения автоматического шифрования используются особые протоколы.

Наиболее распространенные из них:

– PGP (Pretty Good Privacy [2];
– S/MIME (Secure/Multipurpose Internet Mail Extensions.

Определившись с методами и способами шифрования электронной почты, стоит рассмотреть целесообразность данной процедуры, для этого рассмотрим преимущества шифрования электронной почты.

Главное преимущество обеспечение конфиденциальности. Шифрование защищает содержимое сообщений от посторонних глаз, что особенно

важно для личной переписки. Это позволяет избежать утечек информации, которая может быть использована для мошенничества или шантажа.

Важным преимуществом является сохранение целостности данных. Шифрование гарантирует, что сообщение не было изменено в процессе передачи. Это особенно важно для юридически значимых документов или финансовых транзакций.

Третьим преимуществом является подтверждение, что пользователь, направивший письмо, является тем самым пользователем, т. е. аутентификация. Использование цифровых подписей позволяет подтвердить личность отправителя. Это помогает предотвратить атаки «человека посередине», когда злоумышленник пытается выдать себя за другого человека.

Разумеется, шифрование электронной почты используется и для защиты от утечек. В случае утечки данных, зашифрованные сообщения остаются недоступными для злоумышленников, что снижает риск компрометации личной информации.

Были выявлены недостатки при использовании шифрования электронной почты. Например, сложность использования. Необходимо понимать, что для многих пользователей настройка шифрования может показаться сложной задачей, что может привести к отказу от его использования. Необходимость в установке дополнительных программ и настройке ключей может отпугнуть менее технически подкованных пользователей.

Следующий недостаток – проблемы совместимости. Так как, современные технологии очень сильно развиты в данном вопросе, то не все почтовые клиенты поддерживают одни и те же протоколы шифрования, что может создать трудности при обмене зашифрованными сообщениями. Например, пользователь PGP не сможет отправить зашифрованное сообщение пользователю S/MIME без конвертации.

Пользователю всегда нужно помнить про «управление ключами». Необходимость в безопасном хранении и управлении ключами может стать дополнительной нагрузкой для пользователей. Потеря закрытого ключа может привести к невозможности доступа к зашифрованным сообщениям.

Отдельно стоит выделить проблему зависимости от инфраструктуры. Использование некоторых методов шифрования, таких как S/MIME, требует от пользователя наличие доступа к центрам сертификации, что может быть проблематично в некоторых регионах.

Разобравшись с перечнем достоинств и недостатков перейдем к рекомендации по выбору инструментов.

Выбор почтового клиента: Рекомендуется использовать почтовые клиенты, которые поддерживают шифрование, такие как Thunderbird с плагином Enigmail или Outlook с поддержкой S/MIME. Также стоит рассмотреть использование специализированных сервисов, таких как ProtonMail или Tutanota, которые предлагают встроенное шифрование.

После выбора инструмента пользователю необходимо поддерживать регулярное обновление программного обеспечения. Обновление почтовых клиентов и шифровальных программ поможет защититься от известных уязвимостей. Пользователи должны следить за обновлениями и устанавливать их своевременно.

Рекомендуется создавать резервные копии закрытых ключей и хранить их в безопасном месте. Это поможет избежать потери доступа к зашифрованным сообщениям.

Стоит обратить внимание, что для защиты электронной почты необходимо использование многофакторной аутентификации. Вне зависимости от того, защищенный вы используете клиент или нет. Для повышения безопасности рекомендуется использовать многофакторную аутентификацию при доступе к почтовым аккаунтам и шифровальным программам.

Подводя итог, шифрование электронной почты является важным инструментом для защиты личной информации в цифровом мире. Несмотря на некоторые недостатки, преимущества, которые оно предоставляет, делают его необходимым для обеспечения конфиденциальности и безопасности личной переписки. Пользователи должны быть осведомлены о доступных методах и инструментах шифрования, чтобы эффективно защищать свои данные. Внедрение шифрования в повседневное использование требует усилий, но эти усилия оправданы в условиях растущих угроз для информационной безопасности.

Список использованных источников:

1. Дунюшкина, К.С. Создание служебного канала для обмена информацией конфиденциального характера / К.С. Дунюшкина, А.Ф Фатхелисламов. Текст: непосредственный // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VI Всероссийской молодежной научно-практической конференции с международным участием. Уфа, 2023. Уфа: Уфимский университет науки и технологий, 2023. С. 83–86.

2. Сычев Ю.Н. Защита информации и информационная безопасность: учебное пособие/ Ю.Н. Сычев. М.: ИНФРА-М, 2021. 199 с. (дата обращения 29.03.2025). Текст: непосредственный.

Zagidullina A.U.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhelislamov A.F.
Ufa University of Science and Technology, Ufa

ENCRYPTING EMAIL FOR PERSONAL USE

Abstract. In the digital age and the ubiquity of the Internet, protecting personal information is becoming one of the most important tasks. Personal information is a valuable resource, for ensuring the security of which the person himself must be responsible.

This article discusses email encryption methods for personal use, their advantages and disadvantages, as well as recommendations for choosing appropriate tools. Special attention is paid to the practical aspects of implementing encryption in the daily use of e-mail.

Keywords: encryption, email, information security, information.

УДК 004

Зайнуллин Б.И., Масальский Н.В.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ КАК МЕТОД ЗАЩИТЫ

Аннотация. Обезличивание персональных данных представляет собой эффективный метод защиты конфиденциальной информации. Оно включает в себя такие техники, как перемешивание, введение идентификаторов и декомпозиция, позволяющие исключить возможность идентификации личности при обработке данных. Эти методы находят применение при сборе, хранении, поиске, актуализации и передаче персональных данных, обеспечивая соблюдение требований информационной безопасности и законодательства.

Ключевые слова: обезличивание, персональные данные, защита информации, идентификаторы, безопасность, конфиденциальность, метод перемешивания, декомпозиция, обработка данных, актуализация, хранение, поиск, информационные системы, идентификация, передача данных.

Обезличивание персональных данных – это действия, которые направлены на защиту информации от несанкционированного использования. В ходе процедуры персональные данные претерпевают значительные изменения, поэтому расшифровать их без использования дополнительной информации нет возможности.

Актуальность защиты персональных данных обусловлено тем, что с начала 2024 г. злоумышленники слили в сеть 286 млн телефонных номеров и 96 млн адресов электронных почт. Утечка информации с каждым годом увеличивается, так, например, в 2013 г. было слито 213 млн данных. В связи с этим был принят законопроект, который предусматривает максимальный штраф до трех процентов от годовой выручки компании за неправомерную передачу персональных данных третьим лицам.

Целью обезличивания является защита персональных данных при попытке несанкционированного доступа. Так как отсутствие ключа для восстановления базы усложнит работу мошенников.

Преимущества обезличивания данных:

– соответствие требованиям законодательства о персональных данных;
– снижение риска утечки личной информации;
– защита конфиденциальности.

Согласно приказу Роскомнадзора от 05.09.2013 № 996 существует несколько видов обезличивания персональных данных (рис. 1).

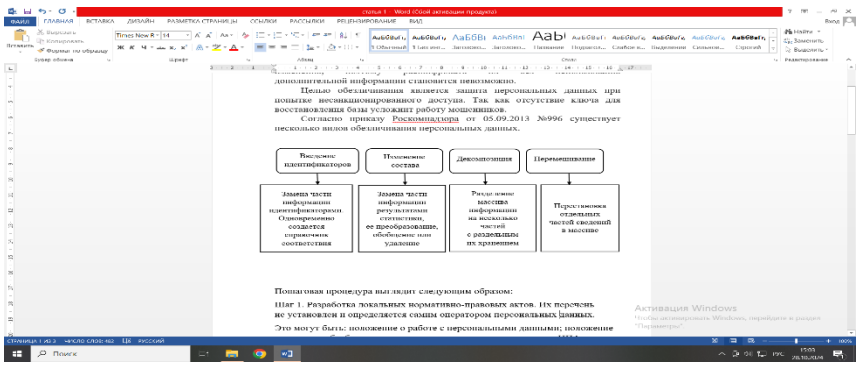

Рис. 1. Виды обезличивания персональных данных

При использовании метода обезличивания персональных данных, необходимо составлять план мероприятий. Примерная поэтапная структура:

1 этап. Необходимо разработать локальные нормативно-правовые акты.

В перечень нормативно-правовых актов могут включаться: положения о работе с персональными данными и положения о защите и обработке персональных данных.

2 этап. Назначить ответственных лиц.

3 этап. Провести обучение для ответственных лиц по правилам обработки персональных данных.

4 этап. Издать приказ о проведении обезличивании персональных данных.

5 этап. Проведение защиты персональных данных. По результатам составляется акт в произвольной форме.

В акте необходимо указать следующую информацию:

– проведенные процедуры;

– перечень персональных данных;

– ответственные лица.

Для того чтобы произвести выбор методов обезличивания персональных данных, необходимо учитывать класс задач. Данная классификация позволит ответственному лицу применить наиболее эффективные методы (табл. 1).

Таблица 1

Выбор методов обезличивания персональных данных

Класс задач	Задачи обработки	Метод обезличивания
Сбор и хранение персональных данных	внесение персональных данных в информационную систему на основе заявлений	метод перемешивания; метод введения идентификаторов
Обработка поисковых запросов	поиск информации и выдача документов, которые содержат персональные данные	метод перемешивания; метод введения идентификаторов; метод декомпозиции
Актуализация персональных данных	внесение изменений в базу персональных данных	метод перемешивания; метод введения идентификаторов; метод декомпозиции
Интеграция данных различных операторов	поиск информации ипередача данных смежным органам	метод перемешивания; метод введения идентификаторов; метод декомпозиции
Ведение учета субъектов персональных данны	ведение учета персональных данных и прием заявлений	метод перемешивания; метод введения идентификаторов; метод декомпозиции

Хэширование – это такой же способ защиты персональных данных, как обезличивание данных.

Криптографические хэш-функции являются одним из эффективных методов обезличивания персональных данных. Хэш-функции применяются для преобразования входных данных в выходные данные фиксированной длины, которые называются хэшем.

Преимущества использования хэш-функций:

– устойчивость к коллизиям (вероятность того, что два разных ввода выдадут одинаковый хэш очень низка);

– необратимость (невозможность получить исходные данные имея только хэш).

Использование хэш-функции в обезличивании персональных данных можно применять для замены идентификаторов на их хэш-значения. Вследствие этого, данные теряют прямую связь с конкретным человеком, но остаются в форме, которая пригодная для дальнейшего использования. Для того, чтобы применить замену можно использовать алгоритм SHA-256. В базе данных, где хранятся фамилия, имя, отчество и пароли, можно заменить фамилию, имя и отчество (рис. 2).

Фамилия, имя и отчество	Хэш-функция
Петров Петр Петрович	9f87d02365456
Иванова Мария Ивановна	efy548der2656

Рис. 2. Пример базы данных

Основным преимуществом использования алгоритма SHA-256 заключается в том, что даже при получении доступа к базе данных, злоумышленник не сможет узнать настоящие имена пользователей, так как хэш невозможно преобразовать в исходные данные. При необходимости аутентификации, пользователь может ввести свои данные, которые будут хэшированы по такому же принципу и система сравнит полученный хэш с хранимой хэш-функцией.

Обезличивание персональных данных с помощью применения хэш-функций является эффективным средством защиты информации. Оно обеспечивает высокий уровень безопасности данных. Для того, чтобы повысить надежность защиты, необходимо комбинировать данный метод с другими средствами защиты.

Список использованных источников:

1. Байдуллина В.В. К вопросу о защите персональных данных: учебное пособие / В.В. Байдуллина, И.А. Шагапов. Уфа: БашГУ, 2016. 28 с.

2. Ломакин С.Т. Информационная безопаность: учебное пособие / С.Т. Ломакин. Сургут: СиУт, 2021. 121 с.

3. Васильков А.В. Безопасность и управление доступом в информационных системах: учебное пособие / А.В. Васильков. М.: ФРуМ, 2021. 121 с.

Zainullin B.I., Masalsky N.V.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

DEPERSONALIZATION OF PERSONAL DATA AS A METHOD OF PROTECTION

Abstract. Depersonalization of personal data is an effective method of protecting confidential information. It includes techniques such as mixing, introducing identifiers, and decomposition to eliminate the possibility of personal identification during data processing. These methods are used in the collection, storage, retrieval, updating and transfer of personal data, ensuring compliance with information security requirements and legislation.

Keywords: depersonalization, personal data, information protection, identifiers, security, confidentiality, mixing method, decomposition, data processing, updating, storage, search, information systems, identification, data transmission.

УДК 004

Ибрагимова А.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Фатхелисламов А.Ф.
Уфимский университет науки и технологий, Уфа

АНАЛИЗ ЭФФЕКТИВНОСТИ И ПОВЫШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ ПРОВОДНОГО КАНАЛА ПЕРЕДАЧИ ДАННЫХ В КОМПЬЮТЕРНЫХ СЕТЯХ

Аннотация. В данной статье рассматриваются ключевые аспекты, влияющие на эффективность и производительность проводных каналов передачи данных в компьютерных сетях. Анализируются современные технологии, используемые для оптимизации передачи данных, а также предлагаются методы повышения производительности, включая использование новых протоколов, улучшение физической инфраструктуры и внедрение технологий управления трафиком.

Ключевые слова: передача данных, компьютерные сети, информация, информационная безопасность.

Сегодня эффективная передача данных играет ключевую роль в функционировании компьютерных сетей. Проводные каналы передачи данных, такие как Ethernet, остаются основным средством связи в локальных и глобальных сетях, обеспечивая высокую скорость, надежность и стабильность соединения. Несмотря на стремительное развитие беспроводных технологий, проводные каналы продолжают занимать важное место в инфраструктуре сетей благодаря своей способности обеспечивать большую пропускную способность и меньшую задержку.

Проводные каналы передачи данных используют различные физические среды, включая витую пару, коаксиальные кабели и оптоволокно, каждая из которых имеет свои преимущества и ограничения. Эффективность этих каналов зависит от множества факторов, таких как качество используемых материалов, протоколы передачи данных, а также методы управления трафиком. В условиях нынешних реалий и увеличения требований к скорости и надежности связи, становится необходимым анализировать и оптимизировать проводные каналы для достижения максимальной производительности.

В данной статье мы рассмотрим основные характеристики проводных каналов передачи данных, факторы, влияющие на их эффективность, а также методы повышения производительности. Целью исследования является выявление ключевых аспектов, которые могут помочь в оптимизации проводных каналов и обеспечении надежной передачи данных в современных компьютерных сетях.

В рамках исследования вначале стоит разобраться с основным термином. Компьютерная сеть – это совокупность взаимосвязанных устройств, таких как компьютеры, серверы, маршрутизаторы и другие сетевые компоненты, которые обмениваются данными и ресурсами друг с другом. Эти устройства могут находиться как в одном физическом пространстве, так и на значительном расстоянии друг от друга, объединяясь с помощью различных технологий передачи данных, включая проводные и беспроводные каналы.

Основная задача компьютерной сети заключается в обеспечении эффективной и надежной коммуникации между пользователями и устройствами, что позволяет обмениваться информацией, совместно использовать ресурсы (например, принтеры и файлы) и обеспечивать доступ к интернету. Компьютерные сети могут быть классифицированы по различным критериям, включая их масштаб (локальные, региональные, глобальные), архитектуру (клиент-серверные, пиринговые) и тип используемых технологий (Ethernet, Wi-Fi и др.).

В рамках анализа эффективности необходимо определить основные характеристики проводных каналов передачи данных.

1. Пропускная способность

Пропускная способность канала – это максимальная скорость передачи данных, которую он может обеспечить. Она измеряется в битах в секунду

(bps) и зависит от используемой технологии (например, Fast Ethernet, Gigabit Ethernet и т.д.) [1]. Современные проводные каналы могут обеспечивать пропускную способность до 100 Гбит/с и более.

2. Задержка

Задержка – это время, необходимое для передачи данных от источника к получателю. Она может быть вызвана различными факторами, включая физическое расстояние, обработку данных на маршрутизаторах и коммутаторах, а также время, необходимое для передачи данных по среде.

3. Ошибки передачи

Ошибки передачи могут возникать из-за помех, потерь пакетов и других факторов. Они могут значительно снизить эффективность канала, так как требуют повторной передачи данных.

Определившись с основными характеристиками каналов передачи информации в компьютерных сетях рассмотрим возможные способы их улучшения. Улучшение характеристик проводных каналов передачи данных может быть достигнуто с помощью различных методов и технологий. Вот несколько стратегий, которые направлены на повышение эффективности и надежности проводных каналов.

Во-первых, использование высококачественных кабелей, так выбор кабелей с высокой пропускной способностью, таких как категории 7, 6 или 6а для витой пары, или оптоволоконные кабели, может значительно увеличить скорость передачи данных и уменьшить потери.

Во-вторых, оптимизация топологии сети, ведь правильная проектировка сети, включая минимизацию длины кабелей и использование активных устройств (например, коммутаторов и маршрутизаторов) для уменьшения задержек, может улучшить общую производительность.

В-третьих, установка оборудования с высокой производительностью, так, например, использование современных маршрутизаторов, коммутаторов и сетевых карт, поддерживающих высокие скорости передачи данных и новые протоколы, может значительно повысить эффективность сети.

Также не стоит забывать об улучшении систем управления трафиком. В рамках этого способа можно инициировать внедрение технологий управления трафиком, таких как Quality of Service (QoS), что сможет помочь приоритизировать важные данные и уменьшить задержки для критически важных приложений.

Следующим способом улучшения эффективности будет использование технологий агрегации каналов. Агрегация нескольких соединений в одно логическое соединение может увеличить общую пропускную способность и обеспечить резервирование в случае сбоя одного из каналов.

Очевидно, что все эти способы так или иначе связаны с физической инфраструктурой и протоколами передачи данных.

Таким образом, факторы, влияющие на эффективность проводных каналов это и качество кабелей, разъемов и оборудования, используемого в сети, напрямую влияет на производительность и используемые протоколы.

Рассмотрим способы повышения производительности проводного канала передачи данных в компьютерных сетях.

Начнем с настройки параметров сети – MTU (Maximum Transmission Unit), нам необходимо оптимизировать размер MTU для уменьшения фрагментации пакетов и повышения эффективности передачи данных [2]. Следующим шагом будет внесение изменений в настройки, так в TCP/IP настройках, необходимо изменить параметры TCP, такие как размер пакета, для улучшения производительности при передаче больших объемов данных.

Также, необходимо проверить, что используются методы снижения помех, например, экранированные кабели. Используйте экранированные витые пары (STP) или оптоволоконные кабели для снижения влияния электромагнитных помех, также при прокладывании кабелей необходимо убедиться в отсутствии источников помех близ кабелей (например, электропроводкой, трансформаторами).

Используйте технологии агрегации каналов (например, LACP) для объединения нескольких физических соединений в одно логическое, что увеличивает общую пропускную способность. При использовании агрегации каналов несколько физических портов (например, Ethernet) на коммутаторе или маршрутизаторе объединяются в один логический порт. Это позволяет распределять трафик между всеми физическими соединениями, что увеличивает общую пропускную способность.

LACP автоматически управляет этими соединениями, обеспечивая их правильную конфигурацию и мониторинг состояния.

Настройка LACP обычно включает в себя следующие шаги - выбор физических портов, которые будут объединены, включение LACP на этих портах и настройка параметров агрегации, таких как режим балансировки нагрузки.

При этом важно – все порты, входящие в агрегацию, должны иметь одинаковые параметры (например, скорость и дуплексный режим).

Максимальное количество портов в одной агрегации может варьироваться в зависимости от оборудования, но обычно это от 2 до 8 портов.

Еще одним способом повышения эффективности проводного канала может являться протокол IPv6.

Применение современных протоколов передачи данных, таких как IPv6, имеет несколько важных причин и преимуществ, особенно в контексте развития компьютерных сетей и Интернета.

Автоконфигурация IPv6 поддерживает автоматическую конфигурацию адресов (Stateless Address Autoconfiguration, SLAAC), что позволяет

устройствам автоматически получать IP-адреса без необходимости ручной настройки или использования DHCP [3].

Упрощение маршрутизации: IPv6 имеет более простую иерархическую структуру адресации, что упрощает маршрутизацию и уменьшает размер таблиц маршрутизации

Заголовок IPv6 был упрощен по сравнению с IPv4, что позволяет ускорить обработку пакетов маршрутизаторами и улучшить общую производительность сети.

Так можно добиться повышения эффективности проводных каналов передачи данных в компьютерных сетях.

Таким образом, в рамках проведенного исследования удалось выявить методы и способы повышения эффективности, а также прийти к следующему выводу: эффективность и производительность проводных каналов передачи данных в компьютерных сетях зависят от множества факторов, включая физическую инфраструктуру, протоколы передачи и управление трафиком. Оптимизация этих аспектов может значительно повысить общую производительность сети. В условиях постоянного роста объема передаваемых данных и требований к скорости передачи, внедрение современных технологий и методов управления трафиком становится необходимым для обеспечения надежной и быстрой связи.

Список использованных источников:

1. Жук А.П. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. М.: РИОР: ИНФРА-М, 2021. 400 с. (дата обращения: 27.03.2025).

2. Кабанов А.С. Основы информационной безопасности: учебник / А.С. Кабанов, А.Б. Лось, А.В. Сорокин. М.: Академия, 2021. 238 с. (дата обращения: 27.03.2025).

3. Щербак А.В. Информационная безопасность: учебник / А.В. Щербак. М.: Издательство Юрайт, 2023. 259 с. (дата обращения: 27.03.2025).

Ibragimova A.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhielislamov A.F.
Ufa University of Science and Technology, Ufa

ANALYSIS OF EFFICIENCY AND INCREASING THE PERFORMANCE OF WIRED DATA TRANSMISSION CHANNEL IN COMPUTER NETWORKS

Abstract. This article discusses the key aspects affecting the efficiency and performance of wired data transmission channels in computer networks. Modern

technologies used to optimize data transmission are analyzed, and methods for increasing productivity are proposed, including the use of new protocols, improving the physical infrastructure and introducing traffic management technologies.

Keywords: data transmission, computer networks, information, information security.

УДК 004

Ибрагимова А.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

АКТУАЛЬНОСТЬ ПРИМЕНЕНИЯ СИСТЕМ КЛАССА DECEPTION ДЛЯ ЗАЩИТЫ ПРЕДПРИЯТИЯ ОТ СОВРЕМЕННЫХ КИБЕРУГРОЗ

Аннотация. В статье раскрыты особенности комплексной системы защиты информации с применением систем класса Deception. Рассматриваются и анализируются принципы работы данной системы, выделяются преимущества систем класса Deception.

Ключевые слова: информация, система защиты информации, Deception, виртуальные ловушки, эмулированная инфраструктура.

Современные информационные системы (ИС) каждый день сталкиваются с новыми и все более сложными атаками на систему безопасности. Зачастую такие атаки могут оказаться даже незамеченными, т. к. в системах могут применяться неактуальные средства и методы защиты информации, которые не зафиксируют сам факт атаки. В связи с этим особо актуальными становятся новые подходы к управлению рисками информационной безопасности (ИБ), которые имеют возможность опознавать кибератаки на ранних стадиях и предотвращать их дальнейшее воздействие на систему.

Ежегодно поставщики средств защиты информации (СЗИ) представляют клиентам обновленные и все более совершенные средства и инструменты для обеспечения информационной безопасности. Одним из таких инновационных решений является технология Deception - DDP (Distributed Deception Platform), относительно недавно появившаяся на рынке, но уже успевшая привлечь внимание специалистов в области защиты информации. Такие системы создают виртуальные приманки и имитируют слабые места (уязвимости), которые отвлекают внимание

злоумышленников. Это позволяет быстро обнаруживать попытки несанкционированного доступа в систему и снижать потенциальный ущерб от реализации угроз нарушения информационной безопасности [1].

Системы Deception, также называемые системами дезинформации или платформами обмана, представляют собой специализированное программное обеспечение, разработанное для создания ложных целей и сетей, предназначенных для привлечения потенциальных злоумышленников и выявления их тактик. Функционирование этих систем осуществляется путем развертывания фиктивных узлов, сервисов и данных, имитирующих настоящие активы компании, тем самым создавая привлекательные цели для злоумышленников.

Если рассматривать принцип работы Deception, то эта технология основывается на имитации информационной инфраструктуры, которая вводит в заблуждение злоумышленника относительно подлинности и конфигурации информационных ресурсов компании. После внедрения системы класса Deception, инфраструктура организации структурируется в виде двух уровней:

1. Первый уровень – это существующая инфраструктура организации.
2. Второй уровень – это имитированная среда, включающая в себя ловушки и приманки, размещенные на реальных устройствах. Любая активность злоумышленника в отношении этих ловушек немедленно раскрывает его присутствие, отправляя уведомление специалистам по защите информации.

Основными этапами работы Deception-систем являются:

1. Создание виртуальных ловушек: развертывание поддельных серверов, компьютеров, IoT-устройств и т.д., которые неотличимы от настоящих и служат для привлечения внимания злоумышленников.
2. Выявление отклонений: система регистрирует любое взаимодействие с созданными системой ресурсами, что позволяет обнаружить активность злоумышленников.
3. Получение информации об угрозах: анализ действий злоумышленников на виртуальных ловушках предоставляет ценные сведения о применяемых методах, инструментах и тактике нападающего, позволяя проактивно реагировать на угрозы ИБ.
4. Взаимодействие с системой безопасности: данные, полученные с помощью Deception-систем, интегрируются с основными инструментами мониторинга безопасности, обеспечивая комплексную защиту информации.

Система Deception обеспечивает точную регистрацию событий активации виртуальных ловушек и практически любых взаимодействий с созданной имитированной средой [2]. Это дает возможность определить весь путь злоумышленника и провести связь между его действиями с другими событиями, которые происходят в инфраструктуре. В случае обнаружения попыток НСД к основным ресурсам компании, центр

управления безопасностью (SOC) может оперативно предпринять шаги для их изоляции, блокировки подозрительной активности и даже имитировать дальнейшие действия злоумышленника, чтобы отвлечь его внимание от реальных целей.

Таким образом, система Deception не ограничивается только констатацией факта несанкционированного доступа в ИТ-инфрастуктуре, а предоставляет возможности для активного противодействия, обеспечивая анализ всех действий злоумышленника.

Преимуществами систем класса Deception являются:

– раннее предупреждение угроз безопасности на этапе вторжения в систему задолго до того, как атака достигнет критически важных активов, обнаружение подготовительных стадий сетевых атак;

– минимизация ущерба от атаки за счет раннего реагирования;

– обман злоумышленника путем создания ложных целей;

– повышение эффективности защитных мер безопасности информации путем анализа поведения злоумышленников и выявления новых методов атак.

Для успешного внедрения решений класса Deception необходима тщательная настройка имитируемой конфигурации. Поскольку каждая организация имеет уникальные особенности инфраструктуры, система должна быть адаптирована именно под конкретные условия эксплуатации [3]. Это позволит построить более эффективную систему для введения злоумышленника в заблуждение. Также необходима регулярная проверка работоспособности для своевременного обновления конфигураций и мониторинга. Это позволяет избежать уменьшения эффективности механизмов защиты информации.

Кроме того, системы Deception позволяют провести интеграцию с существующими системами мониторинга и управления инцидентами (SIEM, SOC) организации. Инструменты Deception могут стать частью общей экосистемы безопасности информации, эффективно дополняя традиционные меры защиты (антивирусные программы, межсетевые экраны), применяемые в организации.

Использование систем класса Deception способствует созданию дополнительного слоя защиты, повышая устойчивость организации перед современными киберугрозами. Таким образом, внедрение систем класса Deception становится важным элементом современной стратегии кибербезопасности, способствующим повышению защищенности информационных ресурсов предприятия.

Список использованных источников:

1. Вавилин Я.А. Информационные технологии в управлении качеством и защита информации: учебное пособие для вузов / Я.А. Вавилин, В.Г. Солдатов, И.Г. Манкевич. Санкт-Петербург: Лань, 2025. 196 с.

Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/447242 (дата обращения: 18.04.2025).

2. Прохорова О.В. Информационная безопасность и защита информации: учебник для СПО / О.В. Прохорова. 6-е изд., стер. СПб.: Лань, 2025. 124 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book /445250 (дата обращения: 18.04.2025).

3. Тумбинская М.В. Защита информации на предприятии: учебное пособие для вузов / М.В. Тумбинская, М.В. Петровский. 2-е изд., стер. Санкт-Петербург: Лань, 2025. 184 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book /463043 (дата обращения: 18.04.2025).

Ibragimova A.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.Yu.
Ufa University of Science and Technology, Ufa

THE RELEVANCE OF USING DECEPTION CLASS SYSTEMS TO PROTECT ENTERPRISES FROM MODERN CYBER THREATS

Abstract. The article reveals the features of a comprehensive information protection system using Deception class systems. The principles of operation of this system are considered and analyzed, the advantages of Deception class systems are highlighted.

Keywords: information, rights, information protection, information protection system, Deception, virtual traps, emulated infrastructure.

УДК 004

Ижболдина Т. К.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ УДАЛЕННОЙ РАБОТЫ

Аннотация. В условиях массового перехода на удаленный формат работы, вопросы информационной безопасности (ИБ) приобрели особую

важность и актуальность. В данной статье рассматриваются основные угрозы, возникающие при дистанционной работе, и предлагаются комплексные меры защиты информации. Дистанционный формат, при всей его гибкости и удобстве, создает множество уязвимостей: от использования ненадежных сетей и личных устройств до рисков фишинга и утечек данных. Особое внимание уделяется использованию VPN, многофакторной аутентификации, шифрованию данных и обучению сотрудников.

Ключевые слова: удаленная работа, фишинг, VPN, многофакторная аутентификация, DLP-система, кибербезопасность.

С переходом на удаленный формат работы многие компании и организации столкнулись с новыми инцидентами ИБ. По данным Xakep.ru, в 2023 г. доля целевых атак на организациях увеличилась на 78 % от общего числа [1]. Одной из причин такого роста стала неспособность традиционных средств защиты информации противодействовать атакам. Злоумышленники активно используют уязвимости в домашних сетях, фишинговые атаки и слабые пароли для доступа к корпоративным системам. В связи с этим организациям необходимо адаптировать свои стратегии защиты данных с учетом новых реалий.

К основным угрозам информационной безопасности при дистанционном формате работы относятся:

1. Небезопасные сети и устройства.

В офисной среде IT-отдел обеспечивает централизованный контроль над всей инфраструктурой: корпоративными компьютерами, серверами, маршрутизаторами и межсетевыми экранами. Однако при удаленной работе сотрудники часто подключаются к корпоративным ресурсам через личные устройства (ноутбуки, планшеты, смартфоны) и непроверенные сети, такие как: домашний Wi-Fi становится уязвимым, если роутер не обновлен или использует слабые настройки безопасности (например, устаревший протокол WPA2 или стандартный пароль администратора), что позволяет злоумышленникам перехватывать трафик; общедоступные точки доступа (кафе, аэропорты, коворкинги) представляют угрозу из-за отсутствия шифрования, что облегчает проведение атак типа Man-in-the-Middle (MITM) с перехватом логинов, паролей и конфиденциальных данных; кроме того, личные устройства сотрудников без защиты (отсутствие антивируса, файрвола или актуальных обновлений) превращаются в легкую мишень для вредоносного ПО.

2. Методы социальной инженерии и фишинг.

Социальная инженерия остается крайне опасным методом атак на удаленных сотрудников, особенно уязвимых из-за цифрового формата работы и отсутствия личного взаимодействия. Злоумышленники активно используют психологические манипуляции, поскольку удаленные работники не могут оперативно проверить подозрительные запросы у

коллег, а стресс и высокая нагрузка снижают их бдительность [2]. Наиболее распространены фишинговые письма, маскирующиеся под сообщения от руководства или ИТ-службы с просьбой «обновить данные», фейковые звонки от «техподдержки» с требованием передать пароли или установить вредоносное ПО, а также поддельные профили коллег в мессенджерах, рассылающие зараженные вложения. Эти методы особенно эффективны благодаря изолированности удаленных команд и повышенной доверчивости сотрудников в условиях стресса [6].

3. Организация контроля доступа.

При офисной работе ИТ-специалисты могут оперативно заблокировать уволенного сотрудника или отследить подозрительную активность, однако в удаленном формате контроль значительно усложняется: сотрудники часто используют слабые пароли (типа «123456» или «Password1»), которые легко подбираются брутфорс-атаками; отсутствие сегментации прав приводит к ситуации, когда все удаленные работники имеют одинаковый доступ к системам, что увеличивает риски при компрометации даже одной учетной записи; кроме того, многие сотрудники пренебрегают обновлением операционных систем и корпоративных приложений, оставляя уязвимости (например, в RDP-подключениях), которыми могут воспользоваться злоумышленники [3].

Для эффективной борьбы с названными угрозами безопасности предлагаются следующие методы защиты информации для сотрудников, работающих в удаленном формате:

1. Использование виртуальных частных сетей (VPN). Хороший VPN-сервис шифрует весь интернет-трафик, делая его недоступным для перехвата даже при подключении через ненадежные сети [4]. VPN-сервисы сами могут собирать и анализировать данные пользователей.

2. Внедрение DLP-систем для предотвращения утечек и обязательное шифрование корпоративной переписки.

3. Многофакторная аутентификация (MFA). Даже если злоумышленник получит логин и пароль сотрудника, без дополнительного кода из SMS или мобильного приложения он не сможет получить доступ к системе [5]. Этот простой метод уже предотвратил множество успешных атак по всему миру. Однако даже самые совершенные технические средства не помогут, если сотрудники не понимают основ кибербезопасности.

4. Регулярное обучение должно стать нормой. Необходимо повсеместно практиковать нескучные лекции и практические тренинги с примерами реальных атак. Полезно проводить тестовые фишинговые рассылки внутри компании, чтобы сотрудники на практике учились распознавать угрозы.

5. Для защиты конфиденциальных данных необходимо использовать шифрование как при передаче, так и при хранении информации. Современные решения позволяют шифровать электронную почту, файлы в облачных хранилищах и даже сообщения в корпоративных чатах [7].

Особенно это актуально для компаний, работающих с персональными данными клиентов или коммерческой тайной.

6. Мониторинг безопасности в условиях удаленной работы также требует особого подхода. Системы класса EDR (Endpoint Detection and Response) позволяют отслеживать угрозы на устройствах сотрудников в реальном времени и автоматически блокировать подозрительную активность. При этом важно найти баланс между безопасностью и приватностью, чтобы чрезмерный контроль не вызывал сопротивления у сотрудников.

7. Отдельного внимания заслуживает резервное копирование (back up) данных. Удаленные сотрудники могут случайно удалить или повредить важные файлы, а ransomware-атаки могут зашифровать данные на их устройствах. Регулярные back up в защищенное облачное хранилище или на корпоративные серверы помогут быстро восстановить информацию в случае инцидента.

Таким образом, переход на удаленную работу – это не просто смена рабочего места, а фундаментальное изменение подходов к информационной безопасности. Комплексные технические решения, обучение сотрудников и четкие регламенты должны работать в совокупности. Компании, которые смогут найти баланс между удобством удаленной работы и защитой данных, получат значительное конкурентное преимущество в современном цифровом мире [8].

Список использованных источников:

1. Хакер. Атаки и тренды Q2 2023: что нужно знать о киберугрозах последнего квартала // Xakep.ru. 2023. 30 августа. URL: https://xakep.ru/2023/08/30/q2-2023-attacks-and-trends/.

2. Козлов Д.В., Шестаков А.А. Современные угрозы информационной безопасности в условиях удаленной работы // Информационная безопасность. 2022. № 3(45). С. 56–62.

3. Мельников В.П. Кибербезопасность и защита данных. М.: Юрайт, 2021. 318 с.

4. NIST Special Publication 800-46r2 "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security". 2022. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf /.

5. ENISA Threat Landscape 2023 "Top Cyber Threats and Trends". European Union Agency for Cybersecurity, 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 /.

6. Скляров Д.В., Туманов В.Е. Защита информации в облачных сервисах. СПб.: БХВ-Петербург, 2020. 256 с. Электрон. версия. URL: https://books.4nmv.ru/books/iskusstvo_zashchity_i_vzloma_informatsii_3642868.pdf /.

7. ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection". 2022 / URL: https://www.iso.org/standard/27001 /.

8. Зыков А.И. Цифровизация как средство повышения эффективности предприятия / А.И. Зыков, Р.М. Яппаров // Взаимодействие вузов, научных организаций и учреждений культуры в сфере защиты информации и технологий безопасности: сборник статей по материалам V Международной научной конференции, посвященной памяти доктора технических наук, профессора А.А. Тарасова и доктора технических наук, старшего научного сотрудника О.В. Казарина, Москва, 24–26 апреля 2024 г. М.: Федеральное государственное автономное образовательное учреждение высшего образования «Российский государственный гуманитарный университет», 2024. С. 124-127.

Izhboldina T. K.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

FEATURES OF ENSURING INFORMATION SECURITY IN THE CONTEXT OF REMOTE WORK

Abstract. In the context of the massive transition to a remote work format, information security issues have become particularly important and relevant. This article examines the main threats posed by remote work and suggests comprehensive information protection measures. The remote format, for all its flexibility and convenience, creates many vulnerabilities: from the use of unreliable networks and personal devices to the risks of phishing and data leaks. Special attention is paid to the use of VPNs, multi-factor authentication, data encryption and employee training.

Keywords: remote work, phishing, VPN, multi-factor authentication, encryption, DLP system, cybersecurity.

УДК 004

Искужина Э.Р.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Фатхелисламов А.Ф.
Уфимский университет науки и технологий, Уфа

МЕТОДЫ И ПРОГРАММЫ ДЛЯ ВЫЯВЛЕНИЯ ПОДСЛУШИВАНИЯ СЕТЕВОГО ТРАФИКА

Аннотация. В статье раскрыты особенности работы с сетевым трафиком. Особое внимание уделяется проблемам защиты информации при подслушивании сетевого трафика и методам и программам (анализаторам) для выявления подслушивания сетевого трафика.

Ключевые слова: информация, информационная безопасность, сеть, сетевой трафик, анализатор, сетевой монитор, сниффер, сниффинг.

Актуальность темы подслушивания сетевого трафика является очень высокой в современном мире и тому есть ряд причин. Деятельность организаций и личная жизнь пользователей все сильнее зависят от стабильной и защищенной передачи информации. Увеличение объема передаваемой информации по сети открывает новые горизонты для киберпреступников.

Подслушивание сетевого трафика, также известное как сниффинг, представляет собой процесс перехвата и анализа данных, передаваемых по сети.

Подслушивание позволяет злоумышленнику или администратору сети наблюдать за всеми данными, которые передаются по сети. Получение доступа к сетевому трафику – это часто используемый метод для незаконного получения конфиденциальных данных, в том числе паролей, банковских реквизитов и личных переписок пользователей сети. Зачастую злоумышленники используют прослушивание и перехват трафика для проведения атак «человек посередине» (Man-in-the-Middle, MITM), внедрения вредоносного кода и кражи защищаемой информации. Также государственная власть и разведывательные органы могут прибегать к мониторингу сетевого трафика для обеспечения государственной безопасности и ведения разведки.

При этом в сфере информационной безопасности постоянно возникают новые средства и методы для перехвата и анализа сетевого трафика. Эти инструменты могут применяться как в законных целях (например, для мониторинга сети и контроля), так и для осуществления действий злоумышленников.

Различают несколько типов подслушивания:

1. Пассивное подслушивание: перехват трафика без активного взаимодействия с сетью. Злоумышленник при этом скрытно наблюдает за обменом данными без внесения изменений или активного вмешательства. Обнаружить подобную атаку особенно в коммутируемых сетях крайне затруднительно, так как передача данных не прерывается и функционирование сети остается в норме.

2. Активное подслушивание: включает в себя активное вмешательство в сетевой трафик, например, ARP-спуфинг или DNS-спуфинг, чтобы перенаправить трафик через машину злоумышленника. Легче обнаружить, но может быть более эффективным, т. к. дает возможность изменять информацию, а это чревато возникновением крайне неблагоприятных ситуаций для пользователей [1].

Стоит отметить, что прослушивание сетевого трафика применяется с целью:

– анализа сетевого трафика (диагностика проблем с сетью и анализ производительности);

– тестирования на проникновение (для выявления уязвимостей в сетевой безопасности);

– отладки сетевых приложений;

– злонамеренного использования (для кражи конфиденциальной информации, паролей и других ценных данных).

За всю историю анализа сетевого трафика было создано множество методов и программных средств для обнаружения прослушивания. К основным методам относятся:

1. Выявление «promiscuous mode»: сетевые адаптеры обычно принимают только предназначенный им трафик. Сниффер переводит карту в режим приема всего трафика. Обнаружить это можно с помощью:

– отправки ARP-запроса с неверным IP- и MAC-адресом;

– отправки ping-запросов на недействительные IP-адреса;

– отправки DNS-запросов с некорректными именами.

2. Анализ трафика: поиск дублирующихся пакетов, большого количества ARP-запросов или трафика, который не соответствует протоколам сети.

3. Выявление пассивных снифферов: анализ трафика может помочь выявить характерные признаки, указывающие на их присутствие.

4. Мониторинг производительности сети: сниффинг может замедлить работу сети, увеличивая нагрузку и др. [2].

Для отслеживания и расшифровки сетевого трафика в понятном виде с целью обнаружения неполадок или целевых объектов, представляющих интерес для сетевых специалистов, применяются сетевые анализаторы. Популярными сетевыми анализаторами являются: Wireshark и TCPdump. Рассмотрим более подробно каждый.

Wireshark – это один из самых популярных и мощных анализаторов трафика. Он позволяет захватывать и интерактивно просматривать сетевой

трафик. Поддерживает множество протоколов и имеет богатый набор фильтров.

Wireshark обладает рядом преимуществ, включая богатый набор функций и гибкость в использовании. Пользователи могут настраивать фильтры для фокусировки на интересующих пакетах, преобразовывать информацию в различные форматы для последующего изучения и применять Wireshark для отслеживания сетевого трафика в текущем времени.

Вместе с тем Wireshark обладает и недостатками. Прежде всего, его использование требует определенной квалификации в сфере сетевых технологий и протоколов. Кроме того, при обработке больших объемов информации Wireshark может оказывать существенное влияние на производительность системы, что может привести к замедлению других программ [3].

TCPdump – это консольная утилита для захвата и анализа сетевого трафика. Как и Wireshark, может использоваться для выявления аномалий, указывающих на сниффинг [4].

Главное преимущество TCPdump заключается в его простоте и скорости работы. Работая через командную строку, TCPdump способен оперативно обрабатывать значительные потоки информации, предъявляя минимальные требования к ресурсам системы. Также TCPdump предоставляет возможность сохранения информации в формате pcap, что обеспечивает совместимость с другими приложениями, например, Wireshark.

В числе недостатков TCPdump следует выделить ограниченный интерфейс, подразумевающий владение командной строкой и понимание правил фильтрации. Это снижает удобство использования для тех, кто не имеет опыта работы с Unix-подобными системами. Так же, как и с работой в Wireshark, для полноценного использования возможностей TCPdump необходимо хорошее знание сетевых протоколов.

Wireshark и TCPdumpм – два популярных инструмента для анализа сетевого трафика. Оба позволяют «перехватывать» сетевые пакеты, отфильтровывать ненужные данные и тщательно их анализировать. Однако, несмотря на общую цель, они отличаются друг от друга, что делает их более подходящими для решения разных задач.

Несмотря на растущую популярность шифрования трафика, киберпреступники активно ищут и разрабатывают способы обхода и взлома криптографической защиты. В свою очередь, технологии искусственного интеллекта и машинного обучения находят применение в автоматизации процесса анализа трафика и обнаружении аномальной активности, что повышает эффективность защиты от угроз [5].

В заключение стоит отметить, что обнаружение сниффинга требует комплексного подхода, который включает использование специализированного программного обеспечения, анализ трафика и соблюдение лучших практик безопасности. Важно понимать, что наиболее эффективный метод борьбы со сниффингом – это его упреждение.

Список использованных источников:

1. Басыня Е.А. Сетевая информационная безопасность: учебник / Е.А. Басыня. М.: НИЯУ МИФИ, 2023. 224 с.
2. Воробьев С.П. Компьютерные сети и сетевая безопасность: учебное пособие / С.П. Воробьев, С.Н. Широбокова, Р.К. Литвяк. Новочеркасск: ЮРГПУ (НПИ), 2022. 216 с.
3. Гаврилова А.А. Генерация пакетов трафика для моделирования сетевых атак / А.А. Гаврилова // Информационные технологии обеспечения комплексной безопасности в цифровом обществе. 2024. С. 72–74. Электрон. версия. URL: https://elibrary.ru/ item.asp?id=75117750 (дата обращения: 01.04.2025).
4. Дунюшкина, К.С. Причины и источники сетевых аномалий / К.С. Дунюшкина, А.Ф. Фатхелисламов // Информационная безопасность цифровой экономики. 2023. С. 223–231. Электрон. версия. URL: https://elibrary.ru/item.asp?id=54127454 (дата обращения: 01.04.2025).
5. Назаров М.В. Анализ различных типов подключений на безопасность с помощью программы / М.В. Назаров, Д.М. Акмырадов, Р.М. Насибуллин // Информационные технологии обеспечения комплексной безопасности в цифровом обществе. 2024. С. 96–99. Электрон. версия. URL: https://elibrary.ru/ item.asp?id=75117758 (дата обращения: 01.04.2025).

Iskuzhina E.R.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhielislamov A.F.
University of Science and Technology, Ufa

METHODS AND PROGRAMS FOR DETECTING NETWORK TRAFFIC EAVESDROPPING

Abstract. the article describes the features of working with network traffic. Special attention is paid to the problems of information protection during eavesdropping on network traffic and methods and programs (analyzers) for detecting eavesdropping on network traffic.

Keywords: information protection rights, information security, network, network traffic, analyzer, network monitor, sniffer, sniffing.

УДК 004

Набиева А.И.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Яппаров Р.М.
Уфимский университет науки и технологий, Уфа

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. В условиях постоянного роста объемов данных увеличения числа киберугроз, защита информации стала одной из главных задач для организаций. В данной работе рассмотрены основы технической защиты информации, проведен анализ современных методов и технологий защиты данных, а также разработаны рекомендации по совершенствованию системы технической защиты информации организации. Особое внимание уделено комплексному подходу, включающему аппаратные, программные и организационные меры.

Ключевые слова: техническая защита информации, уязвимости, киберугрозы, системы обнаружения вторжений, аудит безопасности.

Комплексная система защиты информации (КСЗИ) – совокупность организационных, правовых, инженерно-технических (физических), программно-аппаратных, криптографических мероприятий, направленных на обеспечение защиты информации от разглашения, утечки и несанкционированного доступа [1].

Система технической защиты информации (СТЗИ) – это совокупность специальных технических средств, персонала его эксплуатирующего и их использование для защиты информации. Выбор технических средств защиты зависит от выбранного уровня защищенности информации, который необходимо обеспечить.

Мероприятия, проводимые для технической защиты информационной инфраструктуры организации, могут включать в себя: использование защищенных подключений и межсетевых экранов, средств шифрования и защиты от несанкционированного доступа, а также разграничение потоков информации между сегментами сети. При этом они неразрывно связаны с инженерно-техническими (физическими) – установкой систем контроля управления доступом (СКУД), средствами видеонаблюдения, датчиков охранной сигнализации, металлических ворот и др. Отдельные помещения также могут быть оборудованы средствами защиты от утечки акустической (речевой) информации.

В целом, многие организации сталкиваются с угрозами информационной безопасности, которые можно классифицировать на

четыре категории: внешние кибератаки, внутренние угрозы, технические уязвимости и методы социальной инженерии [2].

К внешним угрозам относятся: фишинг, DDoS-атаки, эксплуатация уязвимостей программного обеспечения. Внутренние угрозы включают в себя как умышленные действия инсайдеров (злоупотребление доступом), так и непреднамеренные нарушения (ошибочные отправки конфиденциальной информации). Технические уязвимости проявляются в слабом шифровании данных (использование устаревших алгоритмов), ошибках конфигурации облачных сервисов.

Опасность представляют методы социальной инженерии, позволяющие злоумышленникам обходить технические средства защиты через манипуляции с персоналом. Последствия перечисленных угроз представляют комплексный характер: от прямых финансовых потерь, до репутационного ущерба и юридических рисков, что подтверждает необходимость внедрения многоуровневой системы защиты, включающей регулярный аудит уязвимостей, сочетание технологических решений и обучение сотрудников [3].

В цифровой среде защита информации требует особого подхода, сочетающего несколько взаимодополняющих технологий. Основой являются криптографические методы: передаваемые данные защищаются протоколами SSL/TLS, которые обеспечивают безопасное соединение, а для хранения конфиденциальной информации применяются алгоритмы шифрования (AES-256 для симметричного шифрования и PGP для асимметричного).

Одним из главных элементов защиты являются системы обнаружения и предотвращения вторжений (IDS/IPS), которые анализируют сетевой трафик, используя сигнатурный анализ для выявления известных угроз и поведенческий анализ для обнаружения аномальной активности, автоматически блокируя потенциально опасные действия. Для предотвращения утечек данных применяются DLP-системы, которые производят глубокий контент-анализ и мониторинг всех каналов передачи информации (электронная почта, мессенджеры, съемные носители), а также отслеживающие поведение пользователей для выявления подозрительных действий. Доступ к критическим системам защищается многофакторной аутентификацией, требующей не только пароль, но и дополнительное подтверждение через SMS-коды или биометрические данные. Систематическое обновление программного обеспечения помогает своевременно закрывать уязвимости, а стратегия резервного копирования по принципу 3-2-1 (три копии данных на двух разных типах носителей, одна из которых хранится географически обособленно) дает возможность быстрого восстановления после инцидентов [4].

В целях совершенствования СТЗИ организации необходимо произвести комплекс взаимосвязанных мер, основанных на современных подходах к информационной безопасности. Главной задачей является проведение

регулярного комплексного аудита безопасности, включающего анализ уязвимостей и оценку соответствия международным стандартам (ISO 27001, PCI DSS). Основным элементом модернизации СТЗИ должно стать внедрение SOC (Security Operations Center) с использованием платформ SIEM (например, IBM QRadar или Splunk), обеспечивающего оперативное выявление инцидентов и координацию реагирования. Также необходимо реализовать программу непрерывного обучения сотрудников, где будут не только базовые тренинги по кибергигиене, но и специализированные курсы по распознаванию фишинга и социальной инженерии [5]. Архитектурные улучшения должны включать в себя логическую сегментацию сети с применением технологий микросегментации, что позволит минимизировать зону поражения при компрометации. Обязательным требованием является разработка детальных политик безопасности, регламентирующих все аспекты работы с данными – от классификации информации, до процедур реагирования на инциденты. В качестве технологической основы рекомендовано использовать защищенные облачные решения, такие как Microsoft Azure Sentinel для мониторинга угроз или Kaspersky Endpoint Security для защиты рабочих станций, которые обеспечивают масштабируемость и доступ к современным средствам защиты. Реализация данных мер поможет создать адаптивную СТЗИ, которая качественно противостоит современным киберугрозам.

В заключение необходимо выделить, что разработка эффективной СТЗИ подразумевает комплексный подход, умещающий современные технологические решения (криптографическую защиту, системы обнаружения вторжений, DLP-системы, многофакторную аутентификацию) с организационными мерами (регулярный аудит безопасности, создание SOC, обучение персонала, разработку регламентирующих документов). Одним из главных является принцип многоуровневой защиты, предполагающий не только внедрение отдельных средств защиты, но и их системную интеграцию, обеспечивающую синергетический эффект. Соблюдение предложенных рекомендаций поможет организациям создать адаптивную систему информационной безопасности, которая сможет противостоять киберугрозам, минимизировать риски утечек данных и обеспечить непрерывность бизнес-процессов.

Список использованных источников:

1. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. Электрон. версия. URL: https://books.ifmo.ru/file/pdf/2006.pdf /.

2. Николаева К.А, Шабурова А.В. Совершенствование политики информационной безопасности в организации. Электрон. версия. URL:https://cyberleninka.ru/article/n/sovershenstvovanie-politiki-informatsionnoy-bezopasnosti-v-organizatsii /.

3. Солодянников А.В. Информационная безопасность автоматизированных систем: учебное пособие. Электрон. версия. URL: https://infosec.spb.ru/wp-content/uploads/2020/08/solodjannikov.pdf /.

4. Исмагилова А.С. Количественная оценка рекомпозиционной системы защиты информации / А.С. Исмагилова, И.А. Шагапов, И.В. Салов // Инженерный вестник Дона. 2024. № 8(116). С. 273–281.

5. Ахмадиева В.Ф. Обучение персонала с использованием платформы по осуществлению симуляции кибератак / В.Ф. Ахмадиева, В.Ф. Ахмадиева // Вопросы эффективного применения научного потенциала общества: сборник статей по итогам Международной научно-практической конференции, Екатеринбург, 09 апреля 2025 г. Стерлитамак: Агентство международных исследований, 2025. С. 110–114.

Nabieva A.I.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Yapparov R.M.
Ufa University of Science and Technology, Ufa

ON THE ISSUE OF IMPROVING THE SYSTEM OF TECHNICAL PROTECTION OF INFORMATION

Abstract. With the constant growth of data volumes and the increasing number of cyber threats, information protection has become one of the main tasks for organizations. In this paper, the basics of technical information protection are considered, an analysis of modern methods and technologies of data protection is carried out, and recommendations for improving the system of technical information protection (TPI) of organizations are developed. Special attention is paid to an integrated approach, including hardware, software and organizational measures.

Keywords: technical information protection, vulnerabilities, cyber threats, intrusion detection systems, security audit.

УДК 004

Тактаев Т.У.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

ПРИВАТНОСТЬ В МЕССЕНДЖЕРАХ: НАСКОЛЬКО ЗАЩИЩЕНЫ НАШИ ПЕРЕПИСКИ?

Аннотация. В статье рассматриваются современные угрозы приватности в мессенджерах, методы их защиты, включая сквозное и постквантовое шифрование, а также концепция мессенджера нового поколения. Отдельное внимание уделено проблеме сбора метаданных и децентрализации. Представлены предложения по созданию мессенджера, обеспечивающего максимальную безопасность и конфиденциальность общения.

Ключевые слова: приватность, мессенджеры, шифрование, метаданные, безопасность.

Современные мессенджеры применяют E2EE как стандарт шифрования, но метаданные остаются уязвимыми. Signal считается самым безопасным, тогда как Telegram критикуется за непрозрачность. TLS защищает передачу данных, но не исключает их хранения. Даже защищенные мессенджеры, такие как Signal или Briar, собирают метаданные, позволяющие анализировать поведение пользователей. Централизованные серверы создают риски взломов и утечек, что подтверждают случаи с Telegram и WhatsApp.

Развитие квантовых технологий ставит под угрозу текущие алгоритмы шифрования, требуя перехода на постквантовые решения. Приватность одновременно защищает пользователей от внешних угроз и может использоваться злоумышленниками для сокрытия противоправной деятельности. Необходим баланс между безопасностью и контролем.

Приватные каналы могут быть использованы для координации преступных схем, распространения запрещенного контента или даже террористических действий, поскольку отсутствие контроля и прозрачности создает пространство для злоупотреблений.

Найти оптимальный баланс между защитой персональных данных и предотвращением злоупотреблений – сложная, но необходимая задача. Вот несколько ключевых направлений для решения данной проблемы:

1. Технологическая гибкость: Разработка мессенджеров и систем связи, которые позволят пользователю самостоятельно регулировать уровень приватности в зависимости от ситуации. Например, возможность выбора

между режимами высокой анонимности и режимами, где предусмотрено определенное логирование для оперативного реагирования на угрозы.

2. Интеграция аналитических инструментов: Использование искусственного интеллекта для выявления аномалий в поведении пользователей без нарушения их приватности. Такие системы могут предупреждать о подозрительной активности, не раскрывая личную информацию законопослушных пользователей.

3. Децентрализация: Разработка децентрализованных архитектур, где контроль над данными остается у пользователя, а не централизованных сервисов, что минимизирует риск их незаконного использования, но при этом затрудняет злоумышленникам организацию скрытых групповых сетей.

4. Регуляция и стандартизация: Формирование нормативных актов, устанавливающих границы допустимой приватности в цифровых коммуникациях. Законодательное регулирование может помочь в определении рамок, в которых приватность остается инструментом защиты, а не средством для укрытия преступной деятельности.

Для обеспечения истинной приватности необходимо:

- минимизация сбора данных: отказ от логирования активности пользователей;
- защита метаданных: использование луковой маршрутизации и микс-сетей;
- полный контроль пользователя: гибкие настройки конфиденциальности;
- постквантовое шифрование: защита от будущих угроз;
- децентрализованные идентификаторы: отказ от привязки к телефонным номерам.

Такая архитектура обеспечит максимальную приватность, устойчивость к цензуре и защиту от потенциальных атак.

Для защиты метаданных предлагаются следующие решения:

- луковая маршрутизация – передача сообщений через несколько узлов, скрывающая отправителя и получателя;
- обфускация трафика – создание фонового трафика, затрудняющего анализ данных;
- децентрализованная серверная архитектура – устранение единой точки отказа.

Для защиты от квантовых атак необходимо внедрение постквантовой криптографии. Среди перспективных алгоритмов – Kyber и хеш-базированные подписи. Важно учитывать их эффективность на мобильных устройствах.

Пользовательский контроль будет включать:

- гибкую настройку анонимности в зависимости от уровня риска;
- опции самоуничтожающихся сообщений с различными таймерами;
- интуитивные индикаторы уровня безопасности в чатах;

- использование блокчейна и AI для повышения безопасности.
- блокчейн обеспечит децентрализованную идентификацию без телефонных номеров и прозрачность хранения данных;
- AI может анализировать аномалии в доступе к данным, выявлять утечки и повышать безопасность, не нарушая приватности.

Эти технологии помогут создать мессенджер, обеспечивающий беспрецедентный уровень конфиденциальности и безопасности.

Существующие децентрализованные мессенджеры (Signal, Session, Briar, Matrix) предлагают частичную защиту приватности, но сталкиваются с проблемами удобства, масштабируемости и защиты метаданных.

Для создания максимально защищенного мессенджера необходимо объединить их сильные стороны:

- децентрализация – устранение единых точек отказа;
- постквантовое шифрование – защита от будущих угроз;
- луковая маршрутизация и микс-сети – скрытие метаданных;
- AI для обнаружения утечек – предотвращение атак в реальном времени;
- гибкие настройки конфиденциальности – контроль над уровнями защиты.

PrivacyGuard – мессенджер нового поколения

Предлагаемая инновация – PrivacyGuard, мессенджер с акцентом на приватность. Его ключевые характеристики:

- полностью децентрализованная архитектура;
- сквозное шифрование с постквантовой защитой;
- минимальный сбор данных и защита от анализа метаданных;
- гибкие настройки для пользователей с разными уровнями риска;
- интеграция с блокчейном для аутентификации без номеров телефонов.

Конфиденциальность в мессенджерах – важная необходимость в цифровую эпоху. Даже при сквозном шифровании остаются уязвимыми метаданные. Безопасные мессенджеры часто неудобны, а популярные – недостаточно защищены. Решение – в новых технологиях: децентрализации, постквантовом шифровании, AI и блокчейне. Идея PrivacyGuard – шаг к балансу между безопасностью, удобством и свободой общения.

Список использованных источников:

1. Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ.
2. ГОСТ Р 59407-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных».
3. Ашманов И.С., Касперская Н.И. Цифровая гигиена. СПб.: Питер, 2021. 256 с.

4. Гуриков С.Р. Интернет-технологии: учебное пособие. М.: Форум: ИНФРА-М, 2019. 184 с.
5. Binance Academy. Что такое сквозное шифрование (E2EE)? URL: https://academy.binance.com/ru/articles/what-is-end-to-end-encryption-e2ee (дата обращения: 26.03.2025).
6. Anti-Malware.ru. Сравнительный анализ безопасности и приватности мессенджеров. URL: https://www.anti-malware.ru/compare/Messengers-security-and-privacy (дата обращения: 26.03.2025).
7. Blockchain-Enabled End-to-End Encryption for Instant Messaging Applications // arXiv. URL: https://arxiv.org/ abs/2104.08494 (дата обращения: 26.03.2025).
8. Сквозное шифрование: что это и почему это так важно? // SecurityLab.ru. URL: https://www.securitylab.ru/analytics/543882.php (дата обращения: 26.03.2025).
9. Практика применения постквантовых криптографических алгоритмов // Futurecrew.ru. URL: https://futurecrew.ru/blog/praktika-primeneniya-postkvantovyh-kriptograficheskih-algoritmov (дата обращения: 26.03.2025).

Taktaev T.U.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

PRIVACY IN MESSENGERS: HOW SECURE ARE OUR CHATS?

Abstract. The article discusses current privacy threats in messengers, protection methods including end-to-end and post-quantum encryption, and a concept of the next-generation messenger. Special attention is given to metadata protection and decentralization. The paper proposes ideas for developing a secure communication platform ensuring maximum confidentiality and user control.

Keywords: privacy, messengers, encryption, metadata, security.

УДК 004

Хафизова А.Э.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Фатхелисламов А.Ф.
Уфимский университет науки и технологий, Уфа

ИССЛЕДОВАНИЕ И ОЦЕНКА ЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ СЕТЕВЫХ СОЕДИНЕНИЙ

Аннотация. В статье раскрыты особенности исследования и оценки защищенности беспроводных сетевых соединений, в частности сети Wi-Fi. Особое внимание уделяется проблемам защиты информации при использовании сети Wi-Fi и средствам безопасности при работе с беспроводными сетями.

Ключевые слова: информация, информационная безопасность, сеть, беспроводные сети, беспроводные сетевые соединения, Wi-Fi.

Применение беспроводных технологий дает огромные преимущества и возможности для современного пользователя. Преимуществом беспроводных решений можно отметить мобильность, т. к. пользователи спокойно могут перемещаться и оставаться на связи, не используя провода, чтобы с кем-то связаться. Использование беспроводных сетей зачастую выходит дешевле, чем сети, использующие провода. А также одним из основных преимуществ является масштабируемость: новые устройства способны без труда интегрироваться в уже работающие сети без специальной установки дополнительных коммуникаций.

Преимущества беспроводных сетей для пользователей и компаний весьма значительны, но при этом они создают и новые риски для информационной безопасности пользователей и организаций. Стоит отметить, что наиболее уязвимыми отраслями являются: гостиничный бизнес, аэропорты, вокзалы, офисные центры, торговые центры, а также другие места с большой проходимостью [1, с. 15]. Рассмотрим основные современные угрозы, которые связаны напрямую с данными, передаваемыми через беспроводные сети:

– перехват злоумышленником конфиденциальной информации, которая передается через беспроводные сети. Такой перехват возможен с применением специальных устройств, которые улавливают радиосигнал, расшифровывают его и ретранслирует, при этом злоумышленника физически можно не заметить, т. к. он может быть далеко от объекта перехвата;

– нарушение доступности данных, передаваемых через беспроводные сети, может быть вызвано как специальными помехами в канале связи, так и атаками хакеров, которые направлены на узлы беспроводной сети;

– перехват идентификационной информации пользователей в процессе ее передачи по беспроводному соединению, например, даже при компрометации мобильного устройства. Полученные данные позволяют выдавать себя за законного владельца при подключении к беспроводной сети [2, с. 22].

К числу потенциальных злоумышленников относятся как конкурирующие организации, так и обычные пользователи, которые действуют умышленно или в связи с низкой осведомленностью. Проникнув в сетевой периметр, злоумышленник получает возможность атаки на конфиденциальную информацию и несанкционированный доступ к важным корпоративным системам.

Атаки на беспроводные сети грозят утечкой персональных данных пользователей, скрытым нахождением злоумышленников в течение времени, пока они не будут обнаружены, сбоями в работоспособности информационных активов, перехватом исходящего трафика и др.

Сегодня существуют проверенные методы обеспечения информационной безопасности в беспроводных сетях, чтобы защитить конфиденциальную информацию от злоумышленников. В частности, будет рассмотрена беспроводная сеть Wi-Fi, для которой разработаны разнообразные подходы к созданию систем, устойчивых к несанкционированному доступу.

В процессе работы по исследованию беспроводных сетевых соединений специалисты применяют подходы к оценке степени безопасности беспроводных сетей и придерживаются нормам, содержащихся в передовых международных стандартах, касающихся анализа безопасности, таких как: ISECOM OSSTMM, PTES и PCI DSS.

Чтобы провести оценку безопасности беспроводных сетевых соединений требуется выполнить ряд шагов:

1. Обнаружение действующих WiFi-точек доступа (стандартов 802.11a/b/g/n) с последующей классификацией на две группы: принадлежащие пользователю/компании и неавторизованные сети.
2. Исследование применяемых методов шифрования.
3. Изучение уязвимостей устройств пользователя/компании в исследуемой беспроводной сети.
4. Поиск и проверка паролей от беспроводной сети WiFi.
5. Проверка использования возможности несанкционированного доступа (НСД) к сети.
6. Мониторинг трафика без активного вмешательства и оценка рисков информационных атак на протоколы канального уровня (ARP, STP и др.).
7. Осуществление перенаправления и перехвата сетевого трафика с целью обнаружения конфиденциальных данных.

Стоит отметить, что в настоящее время существует большое количество специальных анализаторов Wi-Fi, которые способны повысить защиту, стабильность и производительность беспроводной сети. Рассмотрим более подробно несколько популярных программ: NetSpot, inSSIDer и Acrylic Wi-Fi.

Среди обширного количества программ для Wi-Fi анализа NetSpot выделяется своей доступностью и простотой использования. Программа предлагает широкий функционал, начиная от обычного сканирования беспроводных сетей и заканчивая созданием карт покрытия Wi-Fi сигнала (тепловых карт). Важная функция NetSpot – режим «Site Survey», который позволяет визуализировать мощность сигнала и зону покрытия Wi-Fi на плане помещения. Можно загрузить план офиса или квартиры и, перемещаясь с ноутбуком, записывать параметры сигнала в разных точках. Программа создаст подробную карту с цветовой индикацией уровня сигнала. Это особенно актуально для больших офисов, где важно обеспечить стабильное и равномерное покрытие. В дополнение к визуализации силы сигнала, NetSpot предоставляет данные об уровне помех, потенциальных источниках интерференции, а также подробную статистику по каждому каналу и диапазону частот (2.4 ГГц и 5 ГГц) [3, с. 104].

Также среди программ особой популярностью пользуется inSSIDer. Этот инструмент выделяется глубоким изучением характеристик Wi-Fi, предоставляя информацию о точках доступа, мощности сигнала, используемом шифровании, скорости передачи и прочих параметрах. Ключевым достоинством inSSIDer является его визуализация данных и углубленный анализ каналов. Для экспертов в сетевой сфере программа предоставляет расширенные настройки и показатели, позволяющие тщательно мониторить изменения сигнала в динамике.

Acrylic Wi-Fi – еще один достойный внимания анализатор Wi-Fi. Бесплатная версия предлагает основные возможности: сканирование каналов, сбор данных о ближайших сетях, отображение уровня сигнала и протокола безопасности (WEP, WPA и т. д.). Расширенный функционал доступен в платных версиях. Главное преимущество Acrylic Wi-Fi – мониторинг в реальном времени с высокой детализацией. Программа отслеживает изменения сигнала каждую секунду, что позволяет выявлять внезапные ухудшения или источники помех. Кроме того, инструмент предоставляет информацию о стандарте связи (802.11b/g/n/ac/ax), BSSID и поддерживаемых скоростях передачи данных. Версия Heatmaps предназначена для создания тепловых карт Wi-Fi сигнала. Она особенно полезна в крупных помещениях, где важно обеспечить равномерное покрытие [4, с. 53].

Подбор Wi-Fi анализатора обусловлен вашими задачами, уровнем подготовки и финансовыми возможностями. Для детального изучения сети с наглядной визуализацией тепловой карты пространства стоит рассмотреть NetSpot или Acrylic Wi-Fi. Если приоритетом является проверенное решение с широким функционалом, inSSIDer будет отличным

выбором. Для домашнего применения подойдут простые и понятные Wi-Fi Analyzer (из Microsoft Store) и WifiInfoView от NirSoft.

В любом случае, правильный анализ и оптимизация беспроводной сети способны значительно улучшить скорость и стабильность соединения. Анализаторы помогут выявить перегруженные каналы, зоны слабого сигнала и оптимальные настройки роутера. NetSpot, Acrylic Wi-Fi и inSSIDer помогают пользователям и профессионалам выявлять проблемы покрытия, оптимизировать размещение точек доступа и устранять источники помех.

Список использованных источников:

1. Басыня Е.А. Сетевая информационная безопасность: учебник / Е.А. Басыня. М.: НИЯУ МИФИ, 2023. 224 с.

2. Лозовецкий В.В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей: учебное пособие для вузов / В.В. Лозовецкий, Е.Г. Комаров, В.В. Лебедев; под ред. В.В. Лозовецкий. 2-е изд., стер. СПб.: Лань, 2024. 488 с.

3. Файзуллина А.С. Угрозы открытых сетей беспроводной передачи данных / А.С. Файзуллина // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VII Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 24–25 мая 2024 г. Уфа: Уфимский университет науки и технологий, 2024. С. 103–106.

4. Фатхелисламов А.Ф. Беспроводная сеть как уязвимое место в периметре защиты / А.Ф. Фатхелисламов // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов VII Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 24–25 мая 2024 г. Уфа: Уфимский университет науки и технологий, 2024. С. 52–54.

Khafizova A.E.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Fatkhelislamov A.F.
Ufa University of Science and Technology, Ufa

RESEARCH AND ASSESSMENT OF SECURITY OF WIRELESS NETWORK CONNECTIONS

Abstract. The article reveals the features of research and assessment of security of wireless network connections, in particular Wi-Fi networks. Particular attention is paid to the problems of information protection when using Wi-Fi networks and security tools when working with wireless networks.

Keywords: rights, information protection, information security, network, wireless networks, wireless network connections, Wi-Fi.

СЕКЦИЯ 5. ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ИНФОРМАЦИОННЫХ ВОЙН

УДК 004

Бильданов С.З., Попов А.А.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

Научный руководитель:
Новикова Д.Д.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

СОВРЕМЕННЫЕ ВЫЗОВЫ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В настоящей работе представлен анализ актуальности вызовов в области информационной безопасности, возникающих в направлениях обеспечения информационной безопасности в условиях информационных войн, обеспечения ИБ в сфере, обеспечение безопасности органов исполнительной власти, а также актуальность применения ИИ в сфере обеспечения ИБ.

Ключевые слова: информационная безопасность, искусственный интеллект.

Согласно Стратегии национальной безопасности РФ обеспечение информационной безопасности является одним из ключевых направлений обеспечения национальной безопасности [1]. Таким образом, тема нашей работы актуальна.

Целью нашей работы мы видим освещение основных вызовов информационной безопасности в различных областях. Мы решили рассмотреть следующие направления: обеспечение информационной безопасности в период информационных войн, обеспечение ИБ в сфере экономики, а также информационная безопасность органов исполнительной власти и применение ИИ в рамках обеспечения ИБ.

Постепенное развитие цифровых технологий несет за собой колоссальные риски и угрозы. В связи с этим в условиях геополитических изменений и цифровизации всех сфер жизнедеятельности человека, в правовой сфере необходимо проведение полномасштабных исследований и проработки современных подходов к систематизации информационного права.

На 2022 г. в информационном законодательстве существовал ряд проблем при обеспечении безопасности, такие как факт существования кибератак, как таковых, общественно-опасные деяния с использованием информационных средств, использование искусственного интеллекта и

робототехники в преступных целях. [1] В наше же время, на 2025 г.д вступил ряд изменений, направленных на усиление ответственности в области информационной безопасности, такие как повышение мер наказания по ст. 272–274 УК РФ [2], также повысилась мера ответственности за распространение ложной информации по ст. 207.3 УК РФ [3]. На основании приведенных сведений можно сделать вывод, что актуальность вызовов обеспечения информационной безопасности в условиях информационной войны снизилась, но не исчезла.

Прежде чем обеспечивать информационную безопасность, необходимо определить список угроз защищаемого субъекта. Информационная безопасность органов исполнительной власти включает в себя обеспечение их информационных потребностей в рамках их ответственности и в объемах, необходимых для выполнения возложенных задач, полноту, своевременность и достоверность информации, необходимой для принятия решений; безопасность информации и информационных ресурсов; безопасность информационного обмена [4].

В наше время возможно обеспечить безопасность информационного обмена, за счет построения защищенных информационных телекоммуникационных систем, с применением технических средств, сертифицированных ФСТЭК. Также стандартной процедурой является постановление соответствующего правового режима применяя различные политики безопасности, положения и прочее.

Однако, даже несмотря на серьезное покрытие законодательством проблем информационной безопасности субъектов и объектов КИИ, тем не менее некоторые проблемы до сих пор не урегулированы, например защита информации с грифом «Для служебного пользования». Несмотря на федеральные законы и указы Президента, регулирующие защиту информации для служебного пользования, ответственность за ее разглашения законодательно не регулируется. Следовательно, данный вопрос по-прежнему остается актуальным.

Стремительная информатизация и интеллектуализация общества породили вопрос применения систем на основе искусственного интеллекта, причем данное направление очень популярно с экономической точки зрения, так, с 2019 по 2025 г. мировой рынок технологий обеспечения информационной безопасности, использующей искусственного интеллекта, непрерывно рос и достиг оценочного показателя более 30 млн долларов [5].

Основными факторами, обуславливающими необходимость применения искусственного интеллекта, являются необходимость оперативного реагирования и нехватка квалифицированного персонала, а также факт использование злоумышленниками искусственного интеллекта при проведении атак на системы.

В рамках атаки зачастую применяют отвлекающие маневры, такие как сетевое сканирование или атаки типа «Отказ в обслуживании». Такие

атаки позволяют отвлечь сотрудников на их решение, «растягивая» фронт обороны и позволяя незаметно реализовать более серьезную атаку. В таких условиях, все более актуальна идея применения искусственного интеллекта, который способен обрабатывать значительные объемы информации и реагировать на инциденты даже в нерабочее время.

Для гарантии обеспечения требуемого уровня защиты информации внедряемой системой, необходимо ее корректно реализовать, внедрить и настроить. Причем в процессе настройки модели подвержены угрозам отравления данных и атаки уклонения.

Обе эти угрозы связаны с искажением данных для обучения модели, при отравлении данных переданная выборка искажена до момента обучения системы, во второй угрозе искажение данных происходит в процессе обучения путем незаметных видоизменений корректных входящих данных. В процессе таких атак система обучается некорректно и может работать в пользу третьих лиц, значительно понижая уровень защищенности информации.

Классические интеллектуальные системы, используемые в области информационной безопасности сконструированы на основе анализа отклонений объема специфического трафика, неуспешных попыток аутентификации, шаблонов работы пользователей, идентификации скомпрометированных учетных записей.

Список использованных источников:

1. Дубень А.К. Аспекты и угрозы информационной безопасности в эпоху современных информационных войн // Вестник Удмуртского университета. Серия «Экономика и право». 2022. № 6. URL: https://cyberleninka.ru/article/n/aspekty-i-ugrozy-informatsionnoy-bezopasnosti-v-epohu-sovremennyh-informatsionnyh-voyn (дата обращения: 29.04.2025).

2. КонсультантПлюс: УК РФ Глава 28. Преступления в сфере компьютерной информации: сайт / Региональный центр правовой информации Информправо. М., 1997–2020. URL: http://www.consultant.ru/ (дата обращения: 29.04.2025).

3. КонсультантПлюс: УК РФ Статья 207.3. Публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий, оказании добровольческими формированиями, организациями или лицами содействия в выполнении задач, возложенных на Вооруженные Силы Российской Федерации или войска национальной гвардии Российской Федерации: сайт / Региональный центр правовой информации Информправо. М., 1997–2020. URL: http://www.consultant.ru/ (дата обращения: 29.04.2025).

4. Терещенко Л.К., Тиунов О.И. Информационная безопасность органов исполнительной власти на современном этапе // Журнал

российского права. 2015. № 8 (224). URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-organov-ispolnitelnoy-vlasti-na-sovremennom-etape (дата обращения: 29.04.2025).

5. Шананин В.А. Применение систем искусственного интеллекта в защите информации // Инновации и инвестиции. 2022. № 11. URL: https://cyberleninka.ru/article/n/primenenie-sistem-iskusstvennogo-intellekta-v-zaschite-informatsii (дата обращения: 29.04.2025).

Bildanov S.Z., Popov A.A.
Volga Region State University of
Telecommunications and Informatics, Samara

Scientific supervisor:
Novikova D.D.
Volga Region State University of
Telecommunications and Informatics, Samara

CONTEMPORARY CHALLENGES IN THE FIELD OF INFORMATION SECURITY

Abstract. This paper presents an analysis of the relevance of challenges in the field of information security arising in the areas of ensuring information security in the context of information wars, ensuring information security of executive authorities, as well as the relevance of the use of AI in the field of ensuring information security.

Keywords: information security, artificial intelligence.

УДК 004.8

Ларичев Р.С.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

Научный руководитель:
Козырева Н.И.
Поволжский государственный университет
телекоммуникаций и информатики, Самара

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ИНФОРМАЦИОННЫХ ВОЙНАХ: УГРОЗЫ И ВОЗМОЖНОСТИ ДЛЯ ГОСУДАРСТВ

Аннотация. Статья посвящена анализу роли искусственного интеллекта (ИИ) в современном противоборстве. Рассматриваются ключевые направления применения ИИ как в наступательных, так и в

оборонительных целях. Особое внимание уделено технологиям третьего поколения (нейросетям), которые кардинально меняют методы ведения информационных войн через создание фейкового контента, автоматизированную пропаганду и адаптивные кибератаки. Показано, как ИИ применяется на разных уровнях власти для анализа данных, обработки обращений граждан и оптимизации госуслуг.

Ключевые слова: искусственный интеллект, кибератаки, информационные войны, информационная безопасность, манипуляции, национальная безопасность.

Информационная война – это борьба за влияние на аудиторию с помощью информации. Основными целями войны являются манипуляция сознанием населения, формирование искаженного общественного мнения об определенных событиях и явлениях. На сегодняшний день каждое государство имеет развитую информационную систему и оборудование. В 1950 г. была ИИ первого поколения, которая заключалась на символической логике [1]. В конце 1990-х появился ИИ второго поколения, он был сделан на основе вычислительной мощности первых компьютеров [1]. К новому, третьему поколению ИИ относятся нейросети (Deepfake, ChatGPT, DeepSeek).

Основой систем ИИ являются алгоритмы, которые предоставляют набор инструкций и правил, которым компьютер должен следовать. Машинное обучение- вид системы ИИ, она создает свои собственные правила и инструкции, анализируя входные данные, в которой работает. Это может служить проблемой, так как при известных входных данных, машина может повести себя иначе, что иногда приводит к большим рискам.

Кроме того, некоторые страны мира масштабно инвестируют в системы ИИ. Уже есть примеры их применения на поле боя для информационного обеспечения военных операций или в составе различных систем вооружений [3]. Использование ИИ в военно-стратегических целях предусматривает объединение знаний специалистов в сфере информационных технологий и профессионалов военного дела. Таким образом система обеспечивает максимальную эффективность разведывательной и оборонительной деятельности на поле киберпространства.

Ключевые инструменты любой информационной войны стали:

1. Генерация фейков – нейросети создают убедительные тексты, изображения и видео, которые трудно отличить от реальных.
2. Автоматизированная пропаганда – боты и алгоритмы распространяют дезинформацию в социальных сетях, влияя на общественное мнение.
3. Кибератаки с использованием ИИ – адаптивные вирусы и системы взлома, способные обходить традиционные средства защиты.
4. Анализ Big Data для таргетированных атак – ИИ помогает выявлять уязвимые группы населения для точечного психологического воздействия.

Так, к примеру, в 2020 г. появилось Deepfake-видео, где присутствовали несколько главных политиков РФ [2]. Видео оказали большой резонанс на общества, что даже активно обсуждались во время избирательной компании в США. Этот пример дипфейка вида видеомонтажа, при которой с помощью ИИ создается впечатление для общества, что кто-то сделал или сказал то, чего нет на самом деле.

Основные угрозы для государств:

1. Дестабилизация общества – массовые фейки могут провоцировать протесты, панику и раскол в обществе.
2. Подрыв доверия к институтам власти – имитация голосов и образов политиков дискредитирует официальные источники информации.
3. Кибершпионаж и саботаж – ИИ ускоряет взлом критической инфраструктуры (энергосети, банки, госучреждения).

Несмотря на все угрозы, ИИ превращает государственное управление в хорошо работающий автономный аппарат, предоставляя инструменты и полезные советы для повышения эффективности государственных учреждений.

По словам российского премьер-министра в 2024 г., искусственный интеллект повысил в полтора раза средний уровень использования в отраслях экономики и госуправления [4]. Применение ИИ открывает огромные перспективы для государственного управления, что уже находит практическое подтверждение на разных уровнях власти, от федерального до муниципального.

На федеральном уровне ИИ помогает анализировать огромные объемы государственных документов и готовить экспертные заключения по их эффективности. На региональном уровне ИИ используется для автоматической обработки обращений граждан и составления ответов. А на муниципальном уровне ИИ оптимизирует процессы городского управления.

Особенно востребованы решения, направленные на взаимодействие с гражданами (Госуслуги). Чат-боты и «умные» голосовые помощники (робот Макс в Госуслугах) способны оперативно отвечать на часто задаваемые вопросы, помогают в заполнении документов и заявлений. Такие решения положительно меняют качество государственных услуг, сокращая время обслуживания за счет мгновенной обработки запросов.

В заключении хочется сказать, что искусственный интеллект стал неотъемлемым элементом современного информационного противоборства, с одной стороны, он усиливает угрозы в виде дезинформации, кибератак и манипуляций общественным сознанием, а с другой – служит мощным средством защиты национальных интересов. Технологии третьего поколения, такие как нейросети и генеративный ИИ, уже сегодня трансформируют методы ведения информационных войн, делая их более изощренными и масштабными.

Список использованных источников:

1. Международная безопасность: вызовы и угрозы технологий искусственного интеллекта: статья // ИНТЕРНЕТ ПОРТАЛ СНГ: [сайт] URL: https://e-cis.info/news/566/110242 (дата обращения: 25.04.2025).
2. В Сети появился вирусный ролик с дипфейками Лаврова, Проценко и Шойгу. Технологию все чаще используют в рекламе и политической агитации: статья // Московские новости: [сайт]. URL: https://www.mn.ru/smart/v-seti-poyavilsya-virusnyj-rolik-s-dipfejkami-lavrova-proczenko-i-shojgu-dipfejki-vse-chashhe-ispolzuyut-v-reklame-i-politicheskoj-agitaczii (дата обращения: 25.04.2025).
3. Что нужно знать о роли искусственного интеллекта в вооруженных конфликтах: статья // Международный Комитет Крастного Креста: [сайт]. URL: https://www.icrc.org/ru/document/chto-nuzhno-znat-o-roli-iskusstvennogo-intellekta-v-vooruzhennyh-konfliktah (дата обращения: 25.04.2025).
4. Как компьютерный разум служит государству: статья // РБК ОТРАСЛИ: [сайт]. URL: https://www.rbc.ru/industries/news/680f4a1b9a7947f3fd62bb99 (дата обращения: 28.04.2025).

Larichev R.S.
Volga Region State University of
Telecommunications and Informatics, Samara

Scientific director:
Kozyreva N.I.
Volga Region State University of
Telecommunications and Informatics, Samara

ARTIFICIAL INTELLIGENCE IN INFORMATION WARFARE: THREATS AND OPPORTUNITIES FOR STATES

Abstract. The article is devoted to the analysis of the role of artificial intelligence (AI) in the modern confrontation. The key areas of AI application for both offensive and defensive purposes are considered. Special attention is paid to third-generation technologies (neural networks), which radically change the methods of information warfare through the creation of fake content, automated propaganda and adaptive cyber-attacks. It shows how AI is used at different levels of government to analyze data, process citizens' requests, and optimize public services.

Keywords: artificial intelligence, cyber-attacks, information wars, information security, manipulation, national security.

При подготовке электронного издания использовались следующие программные средства:

- Adobe Acrobat − текстовый редактор;
- Microsoft Word – текстовый редактор.

Все права защищены. Книга или любая ее часть не может быть скопирована, воспроизведена в электронной или механической форме, в виде фотокопии, записи в память ЭВМ, репродукции или каким-либо иным способом, а также использована в любой информационной системе без получения разрешения от издателя. Копирование, воспроизведение и иное использование книги или ее части без согласия издателя является незаконным и влечет уголовную, административную и гражданскую ответственность.

Научное издание

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ В ЦИФРОВОМ ОБЩЕСТВЕ

Материалы
VIII Всероссийской молодежной научно-практической конференции с международным участием
(г. Уфа, 23–24 мая 2025 г.)

Электронное издание сетевого доступа

За достоверность информации, изложенной в статьях, ответственность несут авторы.
Статьи публикуются в авторской редакции

Подписано к использованию 06.10.2025 г.
Гарнитура «Times New Roman». Объем 4,68 Мб.
Заказ 147.

ФГБОУ ВО «Уфимский университет науки и технологий»
450008, Башкортостан, г. Уфа, ул. Карла Маркса, 12.

Тел.: +7-908-35-05-007
e-mail: ric-bdu@yandex.ru