МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное
учреждение высшего образования
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ПЕРСПЕКТИВА – 2025

Сборник трудов

Двенадцатой всероссийской молодежной школы-семинара
по проблемам информационной безопасности

Таганрог, 19–22 мая 2025 г.

Ростов-на-Дону – Таганрог
Издательство Южного федерального университета
2025

УДК 004.56(063)
ББК 16.8 я431
П27

П27 **ПЕРСПЕКТИВА – 2025** [Электронный ресурс] : сборник трудов Двенадцатой всероссийской молодежной школы-семинара по проблемам информационной безопасности (Таганрог, 19–22 мая 2025 г.) ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2025. – Электрон. текстовые дан. (1 файл: 11,7 Мб). – 1 электрон. опт. диск (CD-R). – Системные требования: процессор с тактовой частотой 1,5 ГГц и выше, 2 Гб оперативной памяти, Windows 7 SP1/8, 8.1/10 (32- и 64-разрядные версии), Windows 11 (64-разрядная версия), Acrobat Reader, привод DVD-ROM. – Загл. с экрана. – 381 с.
ISBN 978-5-9275-5087-6

В сборник трудов Двенадцатой всероссийской молодежной школы-семинара по проблемам информационной безопасности «ПЕРСПЕКТИВА – 2025» вошли статьи по следующим направлениям: «Методические основы информационной безопасности»; «Программно-аппаратные средства защиты информации»; «Технические средства защиты информации»; «Правовые и организационные вопросы защиты информации»; «Криптографические методы и средства защиты информации»; «Информационная безопасность в сфере цифровой экономики, блокчейна и криптовалют»; «Управление информационной безопасностью»; «Машинное обучение в информационной безопасности»; «Безопасность телекоммуникационных систем»; «Технологии, методы и средства кибеpразведки»; «Развитие кадрового потенциала в области информационной безопасности»; «Обеспечение безопасности критической информационной инфраструктуры»; «Первые шаги исследований информационной безопасности для студентов СПО и школьников 10-11 классов «Начинающие исследователи» (очно-заочная)».

Материалы публикуются в авторской редакции

ISBN 978-5-9275-5087-6

УДК 004.56(063)
ББК 16.8 я431

ПРОГРАММНЫЙ КОМИТЕТ

Сопредседатели

Веселов Г.Е. – д.т.н., доцент, директор ИКТИБ ЮФУ, г. Таганрог.

Попов А.М. – д.ф.-м.н., профессор, директор Института информатики и телекоммуникаций Сибирского государственного университета науки и технологий имени академика М.Ф. Решетнева (СибГУ им. М.Ф. Решетнева), г. Красноярск.

Заместители председателя

Ищукова Е.А. – к.т.н., доцент, доцент кафедры БИТ им. О.Б. Макаревича ИКТИБ ЮФУ, г. Таганрог;

Золотарев В.В. – к.т.н., доцент, заведующий кафедрой безопасности информационных технологий (БИТ) Института информатики и телекоммуникаций (ИИТ) СибГУ им. М.Ф. Решетнева, г. Красноярск.

ЧЛЕНЫ ПРОГРАММНОГО КОМИТЕТА

Абрамов Е.С. – к.т.н., доцент, заведующий кафедрой БИТ им. О.Б. Макаревича ИКТИБ ЮФУ, г. Таганрог;

Архипова А.Б. – к.т.н., доцент Новосибирского государственного технического университета, г. Новосибирск;

Бабенко Л.К. – д.т.н., профессор, профессор кафедры БИТ им. О.Б. Макаревича ИКТИБ ЮФУ, г. Таганрог;

Жукова М.Н. – к.т.н., доцент, доцент кафедры БИТ ИИТ СибГУ им. М.Ф. Решетнева, г. Красноярск;

Карпова Н.Е. – к.т.н., доцент, заведующая кафедрой электронных систем и информационной безопасности Самарского государственного технического университета, г. Самара;

Касимова А.Р. – старший преподаватель кафедры информационной безопасности Казанского национального исследовательского технологического университета, г. Казань;

Лапина М.А. – к.ф.-м.н., доцент, доцент кафедры вычислительной математики и кибернетики факультета математики и компьютерных наук имени профессора Н.И. Червякова СКФУ, г. Ставрополь;

Маро Е.А. – к.т.н., доцент кафедры БИТ им. О.Б. Макаревича ИКТИБ ЮФУ, г. Таганрог;

Паротькин Н.Ю. – к.т.н., доцент кафедры БИТ ИИТ СибГУ им. М.Ф. Решетнева, г. Красноярск.

УДК 336.74

В.А. Агапов

Финансовый университет при Правительстве Российской Федерации, Россия, г. Москва

ФОРМИРОВАНИЕ ИНФРАСТРУКТУРЫ ДОВЕРИЯ К СИСТЕМЕ ЦИФРОВОГО РУБЛЯ: НОРМАТИВНО-ПРАВОВОЙ АНАЛИЗ И РЕКОМЕНДАЦИИ

В данной статье исследуется ключевая проблема успешного внедрения цифрового рубля (СЦР) в России: необходимость создания инфраструктуры доверия. В статье подчеркивается, что эффективное и безопасное функционирование СЦР напрямую зависит от доверия к системе со стороны как граждан, так и кредитных организаций. Исследование начинается с детального анализа текущего российского законодательства, регулирующего цифровой рубль, что позволяет выявить проблемы и потенциальные риски. Для получения более широкого контекста также изучается международный опыт нормативно-правового регулирования цифровых валют центральных банков (CBDC), что позволяет перенять лучшие практики и избежать возможных ошибок. Важным аспектом исследования является сравнительный анализ цифровых валют, представленных в мире. Выявляются ключевые характеристики и анализируются ограничения их применения в условиях российской финансовой системы, учитывая ее специфические особенности и существующую инфраструктуру. Особое внимание уделено потенциальным проблемам и перспективам, которые возникают при переходе российской банковской системы на расчеты в цифровых рублях. Рассматриваются вопросы совместимости с существующими платежными системами, кибербезопасности, защиты персональных данных и влияния на денежно-кредитную политику. На основе проведенного анализа предлагается ряд конкретных рекомендаций по формированию надежной инфраструктуры доверия к СЦР. Эти рекомендации направлены на обеспечение безопасности, устойчивости и эффективности использования цифрового рубля в Российской Федерации. Они могут касаться усиления нормативно-правового регулирования, внедрения передовых технологий защиты, повышения финансовой грамотности населения и установления четких правил взаимодействия между участниками системы.

***Ключевые слова**: цифровой рубль, цифровые валюты центральных банков (CBDC), инфраструктура доверия, правовое регулирование, цифровая экономика, финансовая стабильность, цифровизация платежных систем, блокчейн, Центральный банк РФ.*

This article examines the key problem of the successful implementation of the digital ruble in Russia: the need to create a trust infrastructure. It emphasizes that the effective and safe functioning of the SEC directly depends on the trust in the system on the part of both citizens and credit institutions. The study begins with a detailed analysis of the current Russian legislation governing the digital ruble, which allows us to identify problems and potential risks. To gain a broader context, the international experience of regulatory regulation of central bank digital currencies (CBDCs) is also being studied, which allows us to adopt best practices and avoid possible mistakes. An important aspect of the study is the comparative analysis of digital currencies represented in the world. The key characteristics are identified and the limitations of their application in the Russian financial system are analyzed, taking into account its specific features and the existing infrastructure. Special attention is paid to potential problems and prospects that arise during the transition of the Russian banking system to settlements in digital rubles. The issues of compatibility with existing payment systems, cybersecurity, personal data protection and the impact on monetary policy are considered. Based on the analysis, a number of specific recommendations are proposed for the formation of a reliable infrastructure of trust in the CC. These recommendations are aimed at ensuring the security, sustainability and efficiency of the use of the digital ruble in the Russian Federation. They may relate to strengthening regulatory and legal regulation, introducing advanced protection technologies, improving financial literacy of the population, and establishing clear rules for interaction between system participants

Keywords: *digital ruble, central bank digital currencies (CBDC), trust infrastructure, legal regulation, digital economy, financial stability, digitalization of payment systems, blockchain, Central Bank of the Russian Federation.*

Введение

В современном мире цифровая трансформация проникает во все сферы экономики, включая финансовый сектор. Одним из ключевых трендов современного мира является развитие цифровых валют центральных банков (CBDC), представляющих собой новый вид денег, эмитируемых центральными банками в цифровой форме. В Российской Федерации в настоящее время активно разрабатывается концепция и реализуется пилотный проект цифрового рубля (ЦР), призванного стать третьей формой национальной валюты наряду с наличными и безналичными деньгами.

Внедрение цифрового рубля в российскую экономику несет в себе значительный потенциал для повышения эффективности расчетов, снижения транзакционных издержек, расширения доступа к финансовым услугам, развития инновационных финансовых продуктов и услуг, а также повышения прозрачности финансовых операций. Однако успешная реализация этого потенциала во многом зависит от формирования инфраструктуры доверия, обеспечивающей безопасность, устойчивость и эффективность функционирования цифрового рубля.

Инфраструктура доверия – это комплекс организационных, правовых и технологических мер, направленных на обеспечение уверенности всех участников системы цифрового рубля в надежности и безопасности проводи-

мых операций, а также в соблюдении их прав и интересов. Ключевыми элементами инфраструктуры доверия являются нормативно-правовая база, определяющая юридические права пользования и ответственность участников, механизмы идентификации и аутентификации пользователей, средства защиты от киберугроз и мошенничества, а также система разрешения споров и защиты прав потребителей.

В статье представлен первый этап исследования, посвященного обоснованию необходимости формирования инфраструктуры доверия для успешного внедрения системы цифрового рубля. В рамках работы проанализировано действующее российское законодательство в области цифрового рубля и международный опыт регулирования цифровых валют. Систематизированы сравнительные характеристики различных цифровых валют центральных банков и сформулированы ограничения их использования в контексте российской финансовой системы. Выявлены потенциальные проблемы и перспективы, связанные с переходом российской банковской системы на расчеты в цифровых рублях. Результаты исследования включают аналитическую оценку законодательной базы, описание сравнительных характеристик цифровых валют и анализ рисков и возможностей, возникающих при внедрении цифрового рубля. Полученные материалы лягут в основу дальнейшей разработки монографии по данной тематике.

Методология

Настоящее исследование проведено с использованием комплекса взаимодополняющих методов, обеспечивающих всесторонний и объективный анализ проблематики создания инфраструктуры доверия для системы цифрового рубля (СЦР). В качестве основных методов исследования были применены:

1. Анализ нормативно-правовой документации: проведен детальный анализ российского законодательства, регулирующего сферу цифрового рубля, включая федеральные законы, подзаконные акты Центрального банка Российской Федерации (Банка России) и другие нормативные документы. В рамках анализа исследовались вопросы эмиссии, обращения и использования цифрового рубля, защиты прав потребителей, предотвращения отмывания доходов, полученных преступным путем, и финансирования терроризма (ПОД/ФТ). Также был проведен анализ международного законодательства в области цифровых валют, включая нормативные акты и рекомендации международных организаций, таких как Банк международных расчетов (BIS) и Международный валютный фонд (МВФ).

2. Сравнительный анализ: выполнен сравнительный анализ характеристик различных цифровых валют центральных банков (CBDC), реализуемых в разных странах. Сравнение проводилось по следующим параметрам:

архитектура, функциональность, технологические особенности, модели распространения, меры безопасности, механизмы обеспечения конфиденциальности, а также регуляторные подходы.

3. Системный анализ: применен для выявления взаимосвязей и взаимозависимостей между различными элементами системы цифрового рубля, включая технологическую инфраструктуру, правовую базу, участников рынка и потребителей. Системный анализ позволил оценить потенциальные риски и возможности, связанные с внедрением цифрового рубля в российскую банковскую систему.

4. Метод обобщения: применен для систематизации результатов анализа нормативно-правовой документации и сравнительного анализа. Метод обобщения позволил сформулировать выводы о необходимости создания инфраструктуры доверия для системы цифрового рубля, а также разработать предложения по ее формированию.

В качестве информационных источников использовались официальные документы органов государственной власти и Центрального банка Российской Федерации, отчеты международных организаций, научные публикации в рецензируемых журналах, материалы конференций, а также данные аналитических агентств и консалтинговых компаний.

При проведении исследования соблюдались принципы объективности, достоверности и обоснованности полученных результатов.

Результаты

Введение цифрового рубля в Российской Федерации – масштабный проект, требующий детальной проработки правовых аспектов и создания надежной инфраструктуры. Основным регулятором и оператором платформы цифрового рубля выступает Центральный банк Российской Федерации (Банк России), который определяет правила функционирования платформы, требования к участникам и пользователям, а также порядок совершения операций. Правовой основой для функционирования платформы цифрового рубля является Федеральный закон «О национальной платежной системе» и другие нормативные акты Банка России, в частности, «Положение о платформе цифрового рубля».

Ключевая особенность платформы – централизованный характер управления. Банк России контролирует работу системы, минимизируя риски. Участниками выступают операторы по переводу денег и пользователи (физические и юридические лица). Они обеспечивают доступ к цифровому рублю, обрабатывают распоряжения клиентов и взаимодействуют с Банком России.

Безопасность обеспечивается строгими требованиями к защите информации и обязательной идентификацией пользователей через государственную систему. Для операций используются специализированные ЭСП.

Для обеспечения безопасности и соответствия требованиям законодательства, к участникам и пользователям платформы предъявляются строгие требования. Участники платформы обязаны соблюдать требования к обеспечению защиты информации, устанавливаемые Банком России. Пользователи платформы должны пройти обязательную процедуру идентификации и аутентификации, включая регистрацию в федеральной государственной информационной системе и получение ключа простой электронной подписи. Это позволяет обеспечить прозрачность операций и противодействовать незаконной деятельности. Для совершения операций пользователи должны использовать электронные средства платежа (ЭСП) на основе специализированного программного обеспечения, установленного на их устройствах.

На платформе открываются счета цифрового рубля различных типов: счета операторов по переводу денежных средств, счета физических лиц и счета юридических лиц. Важно отметить, что филиалам кредитных организаций счета цифрового рубля не открываются. Открытие счетов осуществляется Банком России на основании обращений участников и пользователей платформы. Процедура закрытия счетов также строго регламентирована Банком России и может происходить как по инициативе участника/пользователя, так и в случаях, предусмотренных законодательством, например, при нарушении правил платформы или при банкротстве пользователя. Банк России осуществляет учет и хранение информации об остатках цифровых рублей и совершенных операциях, обеспечивая тем самым надежность и прозрачность системы.

Доступ к платформе регулируется «Положением о цифровом рубле», и в определенных ситуациях может быть приостановлен. Причины для приостановления или прекращения доступа включают нарушение требований к защите информации, возникновение чрезвычайных ситуаций, ограничение права распоряжения цифровыми рублями, отзыв лицензии у кредитной организации и другие. Эти меры направлены на обеспечение стабильности и безопасности функционирования платформы.

Основные операции на платформе – переводы, пополнение и вывод средств. Все операции контролируются на нескольких уровнях, чтобы избежать ошибок и мошенничества. Банк России постоянно следит за соблюдением правил и применяет санкции в случае нарушений.

Платформа цифрового рубля тесно интегрирована с платежной системой Банка России, что обеспечивает ее взаимодействие с другими участниками финансового рынка. Взаимодействие осуществляется с использованием форматов электронных сообщений, предусмотренных Альбомом электронных сообщений. Основные операции, осуществляемые в рамках взаимодействия, включают пополнение счетов цифрового рубля, вывод средств и получение нормативно-справочной информации.

Постановление Центрального Банка Российской Федерации № 833-П вводит строгие требования к обеспечению информационной безопасности для всех участников системы цифрового рубля (ЦР), включая кредитные учреждения. Особое значение придается защите данных транзакций, средствам криптографической защиты и электронной подписи. Документ предписывает применение сертифицированных средств криптографической защиты информации (СКЗИ) и строгое следование процедурам обеспечения безопасности. Ключевое место занимает защита прав пользователей, особенно в контексте операций, совершенных без их ведома.

Инструкция Центрального Банка Российской Федерации № 6928-У регламентирует меры противодействия несанкционированным операциям, возлагая на участников обязанность проверки подозрительных распоряжений, приостановление их исполнения и взаимодействие с клиентами для верификации их намерений. Оператор платформы осуществляет дополнительную проверку, повышая уровень защищенности. Клиентские счета могут подвергаться блокировке при выявлении фактов неправомерной деятельности.

Данная система направлена на укрепление доверия к цифровому рублю, однако требует непрерывного совершенствования алгоритмов выявления мошеннических действий, оптимизации взаимодействия с клиентами и повышения уровня безопасности используемых приложений.

Чтобы проанализировать текущую ситуацию вокруг цифрового рубля, необходимо сравнить, насколько его платформа отражает современные тренды в использовании цифровых валют, согласно международным исследованиям, а также выделить важнейшие аспекты в развитии цифровых валют в других странах.

Отчеты Банка международных расчетов (BIS) предоставляют всесторонний анализ правовых аспектов и тенденций развития цифровых валют центральных банков (CBDC). В центре внимания находятся вопросы юридической классификации CBDC, трансграничные операции, обеспечение конфиденциальности и меры противодействия отмыванию денег. Разнообразие юрисдикций изучают возможные варианты правового статуса CBDC, зачастую основываясь на двухуровневой модели. Среди рисков выделяются операционные, финансовые, репутационные и юридические аспекты. Наиболее значимые тенденции включают усиление кооперации между центральными банками, разработку нормативной базы, активную вовлеченность частного сектора и поддержание конфиденциальности.

Документы BIS фокусируются на технических стандартах и архитектуре CBDC, интеграции технологий блокчейн и распределенных реестров, вопросах регулирования и защиты конфиденциальности. Потенциальные последствия внедрения CBDC включают изменения в структуре финансовой системы и снижение роли коммерческих банков.

Международный валютный фонд (МВФ) подчеркивает значительный интерес центральных банков к CBDC, особенно к розничным проектам, таким как цифровой евро, китайский цифровой юань (e-CNY) и другие. Основные вызовы связаны с кибербезопасностью, правовой базой и международным сотрудничеством. Эффективная интеграция CBDC требует стратегического подхода, учитывающего интересы всех участников финансового рынка и адаптированного к динамике рыночных условий.

Для определения уровня развития цифровых валют (CBDC), проведем сравнительный анализ самых популярных и продвинутых цифровых валют разных стран, а также сопоставим данный анализ с данными по цифровому рублю и сделаем выводы (табл. 1).

Таблица 1

Сравнительный анализ CBDC*

Параметр	**Россия (ЦР)**	**Китай (e-CNY)**	**Япония (цифровая йена)**	**Великобритания (Digital Pound)**	**Швейцария (CBDC)**	**США (Цифровой доллар)**
Архитектура	Централизованная (платформа ЦБ)	Централизован-ная (двухуровневая)	Гибридная (рассматривается)	Гибридная (рассматривается)	Централизованная (рассматривает-ся)	Централизованная (рассматривается)
Функциональность	Розничные платежи, платежи между организациями, смарт-контракты (перспектива)	Розничные платежи, международные платежи (тестирование)	Розничные и оптовые платежи, офлайн платежи (исследования)	Розничные и оптовые платежи, программируемые деньги, смарт-контракты (исследования)	Оптовые и, возможно, розничные платежи	Розничные и оптовые платежи, международные платежи (рассматривается)
Технологии	Платформа ЦБ (не блокчейн)	Распределенный реестр (частично), централизован-ная база данных	Распределен-ный реестр (рассматривает-ся), платформа ЦБ	Распределенный реестр (рассматривается) платформа ЦБ	Платформа ЦБ (возможно с элементами DLT)	Платформа ЦБ (возможно с элементами DLT)
Модель распространения	Двухуровневая ЦБ -> банки -> потребители/ бизнес	Двухуровневая ЦБ -> авторизованные коммерческие банки -> потребители/ бизнес	Двухуровневая ЦБ -> посредники (банки, платежные системы) -> потребители/ бизнес	Двухуровневая ЦБ -> частные поставщики платежных услуг -> потребители/ бизнес	Оптовая ЦБ -> банки (рассматривается)	Двухуровневая (предположительно) ЦБ -> авторизованные посредники -> потребители/бизнес

Окончание табл. 1

Параметр	Россия (ЦР)	Китай (e-CNY)	Япония (цифровая йена)	Великобритания (Digital Pound)	Швейцария (CBDC)	США (Цифровой доллар)
Меры безопасности	Шифрование, многофакторная аутентификация, антифрод	Шифрование, управление доступом, KYC/AML	Шифрование, цифровые подписи	Шифрование, кибербезопасность, защита данных	Шифрование, управление рисками	Шифрование, кибербезопасность, соответствие регуляторным требованиям
Конфиденциальность	Контролируемая (ЦБ имеет доступ к транзакциям)	Контролируемая анонимность: ограниченные транзакции без идентификации, большие транзакции требуют KYC/AML	Баланс между анонимностью и прозрачностью (исследования)	Баланс между анонимностью и прозрачностью (исследования)	Баланс между анонимностью и прозрачностью (исследования)	Обсуждается; необходимость соответствия требованиям безопасности и борьбы с отмыванием денег
Регулярные подходы	Новое законодательство, регулирование ЦБ	Новое законодательство, регулирование ЦБ	Регулирование ЦБ, изменения в существующих законах	Новое законодательство (предполагается) консультации с регуляторами	Регулирование ЦБ, адаптация существующего законодательства	Рассмотрение Конгрессом, консультации с регуляторами, изучение влияния на финансовую систему

** таблица составлена автором*

В ходе анализа можем сделать вывод, что большинство рассматриваемых CBDC (Россия, Китай, Швейцария, США) склоняются к централизованной архитектуре на платформе ЦБ. Это обеспечивает более высокий уровень контроля и безопасности, но может ограничивать инновации и гибкость. В свою очередь Япония и Великобритания изучают гибридные модели, сочетающие элементы централизации и децентрализации. Этот подход может позволить объединить преимущества обеих архитектур.

Если говорить про функциональность, то практически все CBDC ориентированы на поддержку розничных платежей, хотя Китай уже тестирует международные платежи. Оптовые платежи, особенно межбанковские расчеты, также рассматриваются как важная область применения CBDC, но требуют отдельной разработки.

Технологии у стран тоже разнообразные: Россия, США и Швейцария позволяют Центральному банку полностью контролировать платежи и функционирование цифровой валюты, в то время, как Япония, Китай и Великобритания рассматривают возможность использования распределённых реестров, что может повысить устойчивость и прозрачность, но усложняет управление цифровой валютой.

Двухуровневая модель является наиболее распространенной. ЦБ взаимодействует с банками или другими авторизованными посредниками, которые, в свою очередь, предоставляют услуги конечным потребителям и бизнесу. Это позволяет использовать существующую инфраструктуру финансового сектора и избежать нагрузки на ЦБ. Однако стоит отметить, что Швейцария рассматривает оптовую модель, которая направлена исключительно на оптовые платежи.

В контексте безопасности CDBC шифрование является обязательным элементом. Различия возникают в подходах к дополнительным мерам безопасности (Россия – многофакторная аутентификация, Китай – KYC/AML, Великобритания – кибербезопасность, Япония – цифровые подписи, Швейцария – управление рисками и другие), которые отражают приоритеты различных юрисдикций.

Конфиденциальность является одним из самых сложных вопросов. Россия и Китай склоняются к контролируемой анонимности, где ЦБ имеет доступ к информации о транзакциях, но для небольших операций может быть обеспечена ограниченная анонимность. Япония, Великобритания и Швейцария находятся в поиске баланса между анонимностью и прозрачностью, проводя соответствующие исследования.

Большинство стран разрабатывают новое законодательство для регулирования CBDC. Швейцария и США рассматривают возможность адаптации существующего законодательства.

На основе изученных параметров для CBDC разных стран, можно выделить, что Российской Федерации и цифровому необходимо изучать возможность внедрения гибридной архитектуры, сочетающей централизованный контроль с элементами децентрализации, а также обеспечивать взаимодействие с другими финансовыми системами, в том числе, возможно, и с зарубежными CBDC. Кроме того, следует продолжить поиск оптимального баланса между контролируемостью транзакций и соблюдением принципов KYC/AML, исследовать и изучать различные дополнительные меры по обеспечению безопасности цифрового рубля, а также постоянно совершенствовать меры безопасности с учетом новых и актуальных угроз.

Проведенное исследование позволило выявить ряд ключевых проблем, возникающих при переходе на расчеты в цифровых рублях и формировании инфраструктуры доверия к СЦР:

- Риски, связанные с внедрением цифрового рубля. Основными угрозами являются проблемы кибербезопасности, операционные риски, риски ликвидности, а также опасность отмывания денег и финансирования терроризма. Центральный банк Российской Федерации (Банк России) должен обеспечить высокий уровень защиты платформы цифрового рубля, включая применение сертифицированных средств криптографической защиты информации (СКЗИ) и механизмов двухфакторной аутентификации.
- Проблемы интеграции с банковской инфраструктурой. Цифровой рубль должен быть совместим с действующими платежными системами и обеспечивать бесперебойное взаимодействие между коммерческими банками, государственными учреждениями и частными пользователями. Однако его внедрение требует модернизации IT-инфраструктуры банков, что может потребовать значительных финансовых вложений.
- Влияние на денежно-кредитную политику и финансовую стабильность. Одним из ключевых вызовов является возможность оттока ликвидности из коммерческих банков в пользу цифрового рубля, что может привести к снижению объемов кредитования и изменению структуры денежного обращения. Необходимы механизмы регулирования, позволяющие минимизировать эти риски.
- Защита персональных данных и конфиденциальность. Контролируемая анонимность цифрового рубля должна учитывать баланс между защитой конфиденциальности пользователей и необходимостью государственного надзора за финансовыми потоками. Опыт международных CBDC показывает, что наиболее перспективным вариантом является внедрение системы дифференцированного доступа к данным в зависимости от объемов и типов транзакций.

Несмотря на выявленные проблемы, внедрение цифрового рубля может принести значительные преимущества для российской экономики и банковской системы:

- Повышение эффективности расчетов и снижение издержек. Использование цифрового рубля позволит снизить затраты на обработку транзакций, ускорить проведение платежей и повысить прозрачность финансовых операций.
- Развитие инновационных финансовых продуктов и услуг. Цифровой рубль может быть использован для программируемых платежей, смарт-контрактов и автоматизированных расчетных механизмов, что создаст новые возможности для бизнеса и государственных сервисов.

- Повышение конкуренции в банковском секторе. Введение цифрового рубля может стимулировать конкуренцию среди банков и финтех-компаний, что приведет к созданию новых цифровых сервисов, улучшению клиентского опыта и снижению стоимости финансовых услуг.

Для успешного внедрения цифрового рубля и обеспечения его безопасности, устойчивости и эффективности необходимо:

- Совершенствовать разработанную систему защиты цифрового рубля. Необходимо с помощью массового тестирования цифрового рубля выявить основные проблемы, связанные с кибербезопасностью, а также модернизировать и внедрять новые меры безопасности, которые используются в других странах и на основе их отчетов создавать свои. национальные нормы к международным стандартам.
- Повышать финансовую грамотность населения. Важно проводить информационные кампании и образовательные программы, разъясняющие принципы работы цифрового рубля, его преимущества и меры безопасности для пользователей.
- Развивать механизмы защиты персональных данных. Необходимо внедрение технологий дифференцированного доступа к информации и использование передовых методов шифрования, чтобы предотвратить несанкционированное использование личных данных граждан.
- Создать платформу взаимодействия мировых Центральных Банков по вопросам цифровых валют для обмена статистическими показателями, практиками по повышению защиты цифровых валют, а также для более удобного анализа отчетности для массового внедрения цифровых валют в мировую экономику.

Выводы

Исследование подтвердило необходимость создания инфраструктуры доверия для цифрового рубля, обеспечивающей безопасность, прозрачность и эффективность финансовых операций. Были выявлены ключевые проблемы, связанные с внедрением цифрового рубля, а также обозначены перспективные направления его развития.

Поставленная цель исследования – обоснование необходимости формирования инфраструктуры доверия для системы цифрового рубля – была достигнута. На основе анализа международного опыта и нормативно-правовой базы разработаны рекомендации по устранению потенциальных рисков и повышению эффективности цифрового рубля.

Перспективными направлениями дальнейших исследований являются разработка технологических решений для повышения безопасности цифровых платежей, анализ влияния цифрового рубля на денежно-кредитную политику в долгосрочной перспективе, исследование сценариев интеграции цифрового рубля в международные платежные системы.

Результаты исследования обладают высокой практической значимостью и могут быть использованы государственными органами, финансовыми учреждениями и разработчиками финтех-решений при создании и модернизации инфраструктуры цифрового рубля.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (ред. от 04.08.2023).
2. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (ред. от 14.07.2023).
3. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» (ред. от 28.04.2023).
4. Положение Банка России от 03.08.2023 № 820-П «О платформе цифрового рубля».
5. Указание Банка России от 12.07.2024 № 6804-У «О внесении изменений в Положение Банка России от 03.08.2023 № 820-П “О платформе цифрового рубля”» (рег. в Минюсте России № 79208 от 20.08.2024, опубл. 31.10.2024).
6. Указание Банка России от 07.12.2023 № 833-П «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля» (рег. в Минюсте России № 76729 от 29.12.2023, опубл. 29.12.2023).
7. Постановление Центрального банка Российской Федерации от 11.10.2023 № 833-П «О требованиях к обеспечению информационной безопасности системы цифрового рубля».
8. Инструкция Центрального банка Российской Федерации от 12.12.2023 № 6928-У «О мерах противодействия несанкционированным операциям с цифровыми рублями».
9. О порядке противодействия совершению операций с цифровыми рублями, соответствующих признакам осуществления перевода денежных средств без добровольного согласия клиента, установленным Банком России в соответствии с частью 3.3 статьи 8 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (рег. в Минюсте России № 80506 от 09.12.2024, опубл. 24.12.2024).
10. Регламент взаимодействия Финансового посредника и Банка России при управлении криптографическими ключами Платформы Цифрового рубля. 29.12.2023.
11. Регламент по операционно-техническому взаимодействию Финансового посредника и Банка России при осуществлении операций на Платформе цифрового рубля.
12. Стандарт платформы цифрового рубля «Требования операционно-технологического взаимодействия на платформе цифрового рубля» версия 2.0 (вступает в силу 17.03.2025, утвержден 03.12.2024).
13. Стандарт платформы цифрового рубля «Спецификация на программный модуль». 29.11.2024.
14. Стандарт платформы цифрового рубля «Требования и рекомендации к пользовательским интерфейсам при совершении операций с цифровым рублем» версия 3.0 (вступает в силу 01.01.2025, утвержден 21.11.2024).

15. Стандарт платформы цифрового рубля «Порядок проведения работ по оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование программного модуля Банка России, на выполнение предъявленных к входящему в его состав средству криптографической защиты». 29.12.2023.
16. Стандарт платформы цифрового рубля «Требования операционно-технологического взаимодействия на платформе цифрового рубля» версия 1.0 (вступает в силу 01.03.2024, утвержден 05.02.2024).
17. Стандарт платформы цифрового рубля «Порядок подключения участника платформы к платформе цифрового рубля» версия 1.3 (вступает в силу 01.03.2024, утвержден 08.08.2023).
18. ЦВЦБ. Стандарт. Порядок подключения Финансового посредника к Платформе цифрового рубля. Версия 1.2 (действовал с 08.08.2023 по 29.02.2024 включительно, утвержден 29.12.2023).
19. Стандарт платформы цифрового рубля «Требования и рекомендации к пользовательским интерфейсам при совершении операций с цифровым рублем» версия 2.0 (вступает в силу 01.03.2024, утвержден 29.12.2023).
20. Стандарт платформы цифрового рубля «Требования и рекомендации к пользовательским интерфейсам при совершении операций с цифровым рублем» версия 1.0 (действовал с 20.07.2023 по 29.02.2024 включительно).
21. Bank for International Settlements. Central Bank Digital Currencies: executive summary. BIS Report, 2021.
22. Bank for International Settlements. Central Bank Digital Currencies: Foundational Principles and Core Features. BIS Report, 2020.
23. Bank for International Settlements. E-CNY: main objectives, guiding principles and inclusion considerations. BIS Report, 2021.
24. Bank for International Settlements. The Future Monetary System: Digital Currencies and Beyond. BIS Report, 2023.
25. Bank for International Settlements. Faster digital payments: global and regional perspectives. BIS Report, 2024.
26. Bank for International Settlements. Legal aspects of retail CBDCs. BIS Report, 2024.
27. International Monetary Fund. The Rise of Central Bank Digital Currencies: Drivers, Approaches and Technologies. IMF Working Paper, 2022.
28. International Monetary Fund. Central Bank Digital Currency Adoption Inclusive Strategies for Intermediaries and Users. IMF Working Paper, 2024.
29. International Monetary Fund. Digital Money and Central Bank Digital Currencies: The Role of Regulation. IMF Policy Paper, 2023.
30. International Monetary Fund. Central Bank Digital Currency--Progress and Further Considerations. IMF Working Paper, 2024.
31. The People’s Bank of China. White Paper on China’s Digital Yuan. PBOC, 2021.
32. Financial Services Agency of Japan. Framework for the Digital Yen. FSA Japan, 2023.
33. Bank of England. The Digital Pound: A New Form of Money for Households and Businesses? BoE Report, 2023.
34. Swiss National Bank. Wholesale CBDC for the Swiss Financial System. SNB Report, 2023.

35. Board of Governors of the Federal Reserve System. Money and Payments: The U.S. Dollar in the Age of Digital Transformation. Federal Reserve Report, 2022.
36. *Гаврилов С.А., Петрова Е.В.* Регулирование цифровых валют центральных банков: мировой опыт и перспективы для России // Финансы и кредит. – 2022. – № 11 (839). – С. 2243-2257.
37. *Смирнова И.Н.* Влияние цифрового рубля на банковскую систему РФ: риски и возможности // Вопросы экономики. – 2023. – № 5. – С. 115-130.
38. *Иванов Д.А., Сидоров А.Н.* Кибербезопасность цифровых валют центральных банков: ключевые вызовы и способы защиты // Журнал экономической теории. – 2023. –Т. 50, № 2. – С. 78-92.
39. *Кузнецов В.А.* Цифровая трансформация денежно-кредитной политики: роль цифровых валют центральных банков // Банковское дело. – 2022. – № 9. – С. 37-50.
40. *Лебедева Н.Ю., Назаренко Г.В., Седракян Л.К.* Цифровая валюта центрального банка: перспективы и риски эмиссии // Государственное и муниципальное управление. Ученые записки. – 2020. – № 2. – С. 147-153. – DOI: 10.22394/2079-1690-2020-1-2-147-153.
41. *Ларина О.И., Акимов О.М.* Цифровые деньги на современном этапе: ключевые риски и направления развития // Финансы: теория и практика. – 2020. – Т. 24, № 4. – С. 18-30. – DOI: 10.26794/2587-5671-2020- 24-4-18-30.
42. *Ситник А.А.* Цифровые валюты центральных банков // Вестник Университета имени О.Е. Кутафина (МГЮА). 2020. № 9(73) – С. 180-186. – DOI: 10.17803/2311-5998.2020.73.9.180-186.
43. *Кочергин Д.А.* Цифровые валюты центральных банков: опыт внедрения цифрового юаня и развитие концепции цифрового рубля // Экономическая политика. – 2023. – Т. 18б № 4. – С. 92-108.
44. *Чеканов П.Е.* Перспективы и риски эмиссии цифрового рубля Банком России // Вестник Финансового университета. – 2024. – Т. 30, № 2. – С. 45-60.

УДК 004.056:004.421.5

З.Х. Ахмедова, А.Х. Асхабов

ПРИМЕНЕНИЕ ГЕНЕРАТИВНЫХ НЕЙРОСЕТЕЙ ДЛЯ АТАКИ НА КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ: ВОЗМОЖНОСТИ И МЕТОДЫ ЗАЩИТЫ

Статья посвящена проблемам использования генеративных нейросетей для атак на криптографические протоколы, а также применению методов защиты протоколов от атак. Целью статьи является исследование возможного потенциала генеративных нейросетей в атаке на криптографические протоколы. В работе анализируется принцип работы генеративных нейросетей, основные их виды и модели. Проведено исследование сущности атак на криптографические протоколы и их эффективность, применяя различные метрики, такие как скорость атаки и точность предсказания и восстановления данных. Особое внимание уделено анализу успешных примеров и их применению к современным подходам защиты криптографических протоколов. На основе проведённого анализа статья раскрывает современные подходы к защите криптографических протоколов, включая усиление алгоритмов шифрования. Авторы дают обобщенную характеристику способам защиты от атак по побочным каналам с использованием адаптивных систем, интегрирующих машинное обучение. В качестве исследовательской задачи авторами была определена попытка предложить способы улучшения криптографических протоколов, такие как динамическое шифрование, обфускация алгоритмов и внедрение постквантовых методов защиты. Основное внимание в работе авторы акцентируют на исследование современных подходов к защите криптографических систем и принципов работы предложенных подходов. Авторами статьи предложены такие улучшения, как использование постквантовых алгоритмов шифрования, введение динамических протоколов шифрования, интеграция методов машинного обучения в протоколы шифрования и сокрытие информации о потреблении энергии для предотвращения атак по побочным каналам. В заключение авторы приводят примеры уже улучшенных криптографических протоколов и алгоритмов, обосновывают основные вызовы и проблемы введения улучшенных методов, а также раскрывают дальнейшие перспективы развития исследуемой области. В будущем авторы предлагают использовать гибридный подход, который объединит классическую криптографию с методами машинного обучения, минимизирует количество побочных каналов и будет основан на самонастраивающихся системах зашиты. Данная проблема мало изучена и требует дальнейших исследований. Настоящая статья призвана не только привлечь внимание к потенциальным угрозам, но и способствовать развитию методов противодействия, обеспечивая устойчивость криптографических систем в условиях активного использования нейросетевых технологий. Такой взгляд будет интересен специалистам в области защиты информации, а также исследователям в области нейрокриптографии.

Ключевые слова: *генеративные нейросети, криптографические протоколы, нейросетевые атаки, постквантовая криптография, методы защиты, машинное обучение.*

The article is devoted to the problems of using generative neural networks for attacks on cryptographic protocols, as well as the use of methods to protect protocols from attacks. The purpose of the article is to study the possible potential of generative neural networks in attacking cryptographic protocols. The paper analyzes the principle of operation of generative neural networks, their main types and models. A study of the nature of attacks on cryptographic protocols and their effectiveness has been conducted, using various metrics such as attack speed and accuracy of data prediction and recovery. Special attention is paid to the analysis of successful examples and their application to modern approaches to protecting cryptographic protocols. Based on the analysis, the article reveals modern approaches to protecting cryptographic protocols, including strengthening encryption algorithms. The authors provide a generalized description of ways to protect against side channel attacks using adaptive systems that integrate machine learning.

Keywords: *generative neural networks, cryptographic protocols, neural network attacks, post-quantum cryptography, security methods, machine learning.*

Введение

Современная криптография представляет собой одну из ключевых областей защиты данных в цифровом мире. С развитием технологий как защита, так и методы атак на криптографические системы претерпевают значительные изменения. Одним из наиболее перспективных направлений в области киберугроз стало использование генеративных нейросетей, которые демонстрируют высокую эффективность в решении сложных задач, включая анализ и взлом криптографических протоколов.

Генеративные нейросети – это тип нейронных сетей, которые используются для создания новых данных на основе полученной при обучении информации [1–3]. Генеративные нейросети, такие как вариационные автокодировщики (VAE) и генеративно-состязательные сети (GAN), способны не только создавать искусственные данные, но и находить уязвимости в защищенных системах. Это открывает новые возможности для атак, делая их более точными и адаптивными. Одновременно с этим возникает необходимость разработки надежных методов защиты, способных противостоять угрозам, связанным с нейросетями.

Основы генеративных нейросетей

Генеративные нейросети представляют собой класс алгоритмов машинного обучения, которые обучаются создавать новые данные, схожие с теми, что использовались при их обучении. В отличие от дискриминативных моделей, направленных на классификацию или предсказание данных, генеративные модели сосредоточены на моделировании распределения данных и их генерации.

Рассмотрим основные виды генеративных нейросетей и принцип их работы.

Вариационные автокодировщики (VAE). Вариационные автокодировщики – это модели, которые используют вероятностный подход для генерации новых данных. Они работают, сжимая входные данные в скрытое представление (латентное пространство) и затем восстанавливая их обратно. При этом латентное пространство организовано таким образом, чтобы новые, сгенерированные точки могли быть интерпретированы как достоверные образцы данных [4].

Генеративно-состязательные сети (GAN). Генеративно-состязательные сети состоят из двух частей: генератора и дискриминатора. Генератор создает данные, пытаясь обмануть дискриминатор, который, в свою очередь, учится отличать реальные данные от сгенерированных. Этот состязательный процесс приводит к созданию данных, которые максимально приближены к реальным. GAN широко используются для генерации изображений, текста, звуков и других видов данных.

Потоковые модели (Flow-based Models). Потоковые модели, такие как Glow, представляют данные через обратимые преобразования. Это позволяет вычислять плотности вероятности для данных, что делает их полезными как для генерации, так и для анализа.

Модели авторегрессии. В авторегрессионных моделях, таких как PixelCNN и GPT, каждый элемент данных предсказывается на основе предыдущих элементов. Эти модели часто применяются для задач последовательной генерации, таких как создание текста или временных рядов.

Главное преимущество генеративных нейросетей заключается в их способности учиться на больших объемах данных и находить сложные зависимости, которые трудно выявить традиционными методами. Эта способность делает их чрезвычайно мощным инструментом для различных приложений, включая моделирование, симуляцию, восстановление поврежденных данных и анализ аномалий.

В контексте криптографии генеративные нейросети открывают новые горизонты. Они могут использоваться для восстановления утраченных ключей, анализа слабостей в шифрах или даже создания фальсифицированных данных для обхода систем защиты. Однако эти возможности также ставят новые вызовы перед специалистами по кибербезопасности, требуя разработки методов защиты от подобных угроз.

Как известно [3], конфиденциальность информации обеспечивается в основном за счет использования алгоритмов зашифрования/расшифрования. Среди возможных способов реализации существуют такие, которые реализуются на основе нейронных сетей, составляющих основу искусственного интелекта. Эти методы объединены в один раздел криптографии, называемый *нейрокриптографией.* Это название было предложено в 1995 году С. Дурленсом (S.Dourlens) в работе по криптоанализу DES.

Иерархическая структура экосистемы нейрокриптографии представлена на рис. 1.

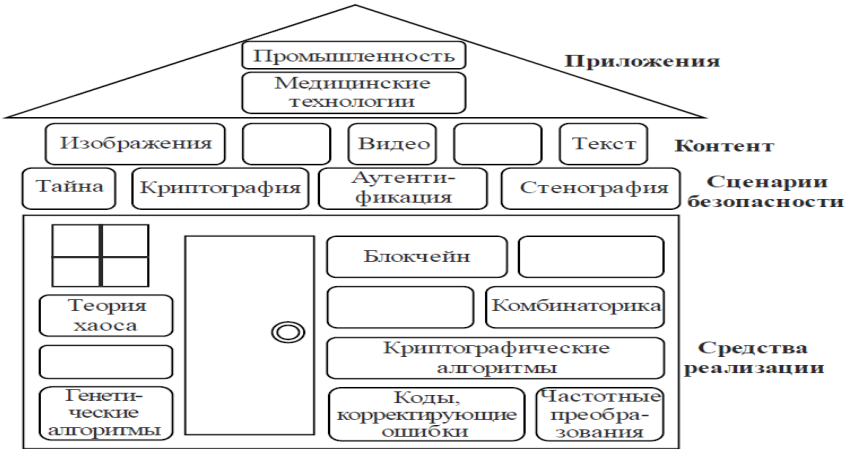


Рис. 1. Иерархическая структура экосистемы нейрокриптографии

Применение нейросетей для взлома криптографических протоколов

С развитием генеративных нейросетей (GAN, VAE и других) появилось множество новых подходов к анализу и атаке на криптографические протоколы. В результате использования таких моделей происходит поиск скрытых закономерностей в данных, что делает их удобным инструментом для взлома самых сложных криптографических систем.

Разберем способы взлома, наиболее часто используемые злоумышленниками.

Одной из главных задач злоумышленников является вычисление криптографических ключей с помощью анализа побочных каналов. Нейросети способны анализировать утечки данных, такие как время выполнения алгоритма, электромагнитные излучения устройств, и даже потребление электроэнергии [5; 12]. Генеративные модели помогают воспроизводить недостающие или скрытые данные, чтобы точно восстанавливать ключи.

Действие многих криптографических протоколов основано на псевдослучайных простых числах. Генеративные нейросети могут выявлять слабости в генераторах псевдослучайных чисел (ГПСЧ), создавая данные, которые могут взломать шифры или подменить сообщения в системах.

Генеративные нейросети очень часто используются для обхода систем аутентификации [6]. К примеру, GAN могут генерировать поддельные цифровые подписи, биометрические данные (отпечатки пальцев, изображения лиц) или голосовые записи. Эти биометрические данные воспринимаются системами как подлинные, что приводит к взлому системы.

Нейросети также применяются для анализа уязвимостей в асимметричных протоколах(RSA, эллиптические кривые). Эти сети способны моделировать сложные математические зависимости и предсказывать ключи на основе ограниченного числа данных или утечек [7].

Большинство программных средств и систем защищены системой обнаружения вторжений. Но ИИ может сотворить материал, который никак не отличить от настоящего. Это позволяет атакующим обходить системы обнаружения вторжений (IDS) и проникать в защищенные сети.

Анализ эффективности разрабатываемых атак

Для оценки эффективности атак на криптографические протоколы, необходимо учитывать несколько основных факторов, таких как точность предсказаний, скорость выполнения атак, сложность реализации и универсальность подхода. Генеративные нейросети предлагают новые возможности, но также имеют свои ограничения, которые важно учитывать при разработке и анализе атак.

Для анализа эффективности атак применимы *критерии оценки*. Наиболее популярным и часто используемым является **Точность предсказаний и восстановления данных.** Одним из основных показателей эффективности является вероятность успешного взлома криптографического протокола. Например, при атаке на криптографические ключи с использованием анализа побочных каналов точность модели измеряется процентом корректно восстановленных ключей. Исследования показывают, что генеративные нейросети, такие как GAN и VAE, способны достигать высокой точности даже при наличии шумов в данных или ограниченном объеме обучающих выборок.

Также нужно учитывать **Скорость атаки.** Генеративные модели, обученные заранее, позволяют значительно ускорить процесс атаки. Вместо полного перебора возможных значений ключа или анализа методом статистического моделирования, нейросети могут мгновенно выдавать результаты на основе латентного пространства. Это делает атаки более практичными в реальных условиях, где время является критически важным фактором.

Генеративные нейросети обладают высокой гибкостью и могут адаптироваться к новым условиям или изменениям в криптографических протоколах. Это особенно важно для атак, направленных на динамически изменяющиеся системы, где традиционные методы анализа могут оказаться неэффективными.

Атаки на основе нейросетей часто оказываются универсальными, поскольку они могут применяться к широкому спектру криптографических протоколов [8, 9]. Например, один и тот же подход может быть использован для анализа различных алгоритмов шифрования или систем аутентификации. Это снижает затраты на разработку новых методов атак.

Также, использование нейросетей для анализа выходных последовательностей **ГПСЧ (Генераторов псевдослучайных чисел)** показали способность выявлять слабости в алгоритмах ГПСЧ, которые ранее считались стойкими [10].

Генеративно-состязательные сети (GAN) продемонстрировали высокую эффективность при подделке биометрических данных, таких как отпечатки пальцев и лица. В некоторых экспериментах поддельные данные успешно проходили проверку в системах защиты с точностью до 95%.

Минусы использования нейросетей для атак

Несмотря на высокую эффективность, использование генеративных нейросетей для атак сталкивается с рядом ограничений:

Требования к обучающим данным: генеративные модели нуждаются в больших объемах данных для обучения, что может быть затруднительно в реальных сценариях [11].

Чувствительность к шумам: данные, содержащие значительный уровень шума, могут снижать точность атак.

Выбор архитектуры: для каждой задачи требуется индивидуальный подбор архитектуры нейросети, что увеличивает сложность разработки.

Зависимость от вычислительных ресурсов: обучение и применение генеративных моделей требуют мощного оборудования, что может ограничивать их использование.

Для дальнейшего повышения эффективности атак с использованием нейросетей исследователи предлагают оптимизировать архитектуру генеративных моделей для задач криптоанализа, применить методы трансферного обучения для снижения зависимости от больших объемов данных или использовать гибридные подходы, объединяющие генеративные нейросети с традиционными методами криптоанализа [12].

Таким образом, анализ эффективности разрабатываемых атак на основе генеративных нейросетей показывает их высокий потенциал в криптоанализе, но также подчеркивает необходимость дальнейших исследований для преодоления существующих ограничений.

Текущие подходы к защите криптографических систем

В условиях развития технологий генеративных нейросетей и их использования для атак на криптографические протоколы возникает острая необходимость в совершенствовании подходов к защите. Современные ме-

тоды защиты нацелены на выявление, предотвращение и минимизацию последствий таких атак. Эти подходы строятся на принципах усиления устойчивости криптографических систем, анализа потенциальных уязвимостей и разработки защитных механизмов, способных противостоять моделям на основе нейросетей.

Основные направления защиты

Усиление криптографических алгоритмов. Одним из ключевых направлений является повышение устойчивости шифров и протоколов к атакам по побочным каналам, анализу шаблонов и моделированию данных. Для этого можно применить усложнение генераторов псевдослучайных чисел (ГПСЧ) для минимизации предсказуемости их выходов; Увеличение длины ключей и использование алгоритмов с высокой криптостойкостью, такие как алгоритмы постквантовой криптографии; Использование дополнительных источников энтропии для генерации случайных чисел.

Обфускация данных и алгоритмов. Обфускация подразумевает изменение структуры данных или алгоритмов таким образом, чтобы они оставались функциональными, но становились труднодоступными для анализа [9, 13–15]. Генеративные нейросети часто обучаются на паттернах в данных, поэтому обфускация затрудняет их обучение. Это включает шумозащиту (добавление случайного шума в данные для повышения их защищенности) и размывание временных и энергетических характеристик, которые могут быть использованы для атак по побочным каналам.

Обеспечения защиты можно добиться с помощью адаптивных систем. Они изменяют свои параметры в зависимости от активности атакующих [13]. Такие системы могут динамически изменять алгоритмы генерации ключей или шифрования.

Человеческий фактор также играет ключевую роль в обеспечении защиты любой информации. Проведение регулярных обучений и повышение квалификации специалистов по информационной безопасности положительно скажется на защищенности сети и системы.

Улучшение протоколов для защиты от нейросетевых атак

Современные угрозы, связанные с применением генеративных нейросетей для атак на криптографические протоколы, требуют разработки и внедрения новых защитных механизмов. Улучшение протоколов заключается в повышении их устойчивости к анализу и взлому нейросетевыми моделями, а также в обеспечении способности адаптироваться к новым атакам.

Основные стратегии улучшения

Использование постквантовых алгоритмов. Протоколы постквантовой криптографии разрабатываются с учётом угроз не только со стороны квантовых компьютеров, но и со стороны генеративных нейросетей [14].

Такие алгоритмы, как NTRU, Kyber и другие, обладают устойчивостью к анализу зависимостей, который активно используется нейросетями. Эти протоколы основаны на задачах, связанных с решётками, многомерными уравнениями и задачей скрытого подмножества (SIS), что делает их стойкими к моделированию и предсказанию.

Введение динамических протоколов шифрования. Традиционные криптографические протоколы используют статические параметры, что делает их уязвимыми к обучению нейросетей. Динамические протоколы, напротив, меняют ключи, алгоритмы шифрования или параметры генерации данных в реальном времени. Это затрудняет обучение нейросетей и проведение атак. Например, адаптивные системы могут генерировать уникальные параметры для каждого сеанса шифрования, основываясь на случайных данных или внешних источниках энтропии.

Защита от атак по побочным каналам. Генеративные нейросети широко применяются для анализа побочных каналов, таких как потребление энергии, временные задержки и электромагнитное излучение. Для защиты протоколов в этих случаях пользуются сглаживанием временных характеристик и сокрытием потребления энергии.

Интеграция методов машинного обучения для защиты

Внедрение собственных моделей машинного обучения в криптографические протоколы позволяет автоматически анализировать входные данные и выявлять признаки атак [16]. Например, системы обнаружения аномалий, обученные на данных об атакующих действиях, могут блокировать попытки взлома в реальном времени; Генеративные модели, интегрированные в протоколы, могут создавать уникальные схемы шифрования, которые адаптируются к поведению атакующего.

Усиление процесса генерации случайных чисел. Генерация псевдослучайных чисел является критически важной частью многих криптографических протоколов. Для повышения их стойкости к нейросетевому анализу предлагаются:

- Увеличение энтропии источников случайных чисел за счёт использования аппаратных генераторов;
- Применение криптографических хэш-функций для рандомизации выходных данных генераторов.

Примеры улучшенных протоколов

1. **TLS с динамическими параметрами.**

Современные версии TLS протокола (например, TLS 1.3) уже внедряют механизмы быстрой смены ключей для повышения безопасности, но дальнейшее развитие может включать динамическое обновление алгоритмов шифрования на основе поведения атакующего.

2. **Адаптивные системы аутентификации.**

В биометрических системах защиты используются методы динамической проверки подлинности, которые адаптируются к изменениям в данных (например, возрастные изменения лица) и затрудняют использование поддельных данных, созданных нейросетями.

3. **Многослойное шифрование**

Некоторые улучшенные протоколы используют подход, при котором данные шифруются несколькими алгоритмами, работающими параллельно или последовательно. Это усложняет нейросетевое моделирование и взлом.

Вызовы при внедрении улучшенных протоколов

1. **Увеличение вычислительных затрат**

Улучшение протоколов часто связано с повышением сложности алгоритмов и увеличением нагрузки на вычислительные мощности [17]. Это может стать проблемой для устройств с ограниченными ресурсами.

2. **Совместимость с существующими системами.**

Многие новые методы защиты требуют модернизации инфраструктуры, что может быть трудно реализовать в краткосрочной перспективе.

3. **Адаптация под новые угрозы**

Генеративные нейросети постоянно развиваются, что требует регулярного пересмотра протоколов и их модернизации для противостояния новым типам атак.

Перспективы развития

Для дальнейшего улучшения криптографических протоколов в условиях угроз со стороны генеративных нейросетей необходимо:

- Интеграция гибридных подходов, объединяющих преимущества классической криптографии и машинного обучения;
- Разработка протоколов с минимальным количеством побочных каналов;
- Повышение автоматизации обнаружения и предотвращения атак с использованием самонастраивающихся систем защиты.

Заключение

Использование генеративных нейросетей для атак на криптографические протоколы представляет собой серьёзную проблему для современных систем безопасности. Несмотря на существующие подходы к защите, нейросетевые технологии продолжают развиваться, что создаёт новые угрозы и требует постоянной адаптации защитных механизмов.

Остаётся нерешённой проблема создания универсальных криптографических протоколов, устойчивых к нейросетевому анализу, которые будут эффективны как против традиционных атак, так и против современных ме-

тодов, основанных на машинном обучении. Особенно остро стоит вопрос вычислительной эффективности защитных решений и их внедрения в системы с ограниченными ресурсами.

Дальнейшее развитие этой области должно быть сосредоточено на разработке гибридных методов защиты, объединяющих традиционную криптографию с возможностями адаптивных систем машинного обучения, а также на активном исследовании постквантовых алгоритмов и многослойных систем шифрования. Только комплексный подход и постоянный мониторинг новых технологий позволят обеспечить безопасность криптографических систем в условиях стремительного развития нейросетей и искусственного интеллекта.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Кан К.А.* Нейронные сети. Эволюция. [Б. м.]: Литрес Самиздат, 2018. – 380 с.
2. *Аннаев Г., Аннаева Г.* Прикладные возможности нейронной сети // Символ науки: международный научный журнал. – 2023. – №4-1. – С. 22-24. – URL: https://elibrary.ru (дата обращения: 17.12.2024).
3. *Урбанович П.П., Плонковски М.Д., Долецки М.* Нейросетевые технологии в криптографических приложениях: монография. – Минск: БГТУ, 2024. – С. 43-58.
4. *Мальцев Н.Д.* Структурные и филологические особенности текстовых генеративных нейронных сетей // Неофилология. – 2024. – Т. 10, № 2. – URL: https://neophilology.elpub.ru/jour/article/view/304 (дата обращения: 12.12.2024).
5. *Гольдвассер Ш., Беллар Л.* Криптография: наука о секретах и кодах. – М.: Техносфера, 2019. – С. 278-292.
6. *Евдокимов И.А., Солодовников В.И.* Ключевые особенности нейросетевого подхода в задаче криптографической защиты информации // Новые информационные технологии в автоматизированных системах. – 2019. – № 2.
7. *Баженов В.А., Смирнов Ю.Б.* Нейросетевые модели для анализа и взлома криптографических систем // Вестник информационной безопасности. – 2022. – Т. 18, № 1. – С. 44-52.
8. *Dourlens S.* Applied neuro-cryptography // Maotrise Informatique, Department of Microcomputers and Microelectronics, University of Paris, 1995. – DOI: 10.13140/RG.2.2.35476.24960.
9. *Урбанович П.П.* Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие. – Минск: БГТУ, 2016. – 218 с.
10. *Червяков Н.И. [и др.].* Применение искусственных нейронных сетей и системы остаточных классов в криптографии. – М.: ФИЗМАТЛИТ, 2012. – 280 с.
11. *Dowlim N. [et al.].* CryptoNets: applying neural networks to encrypted data with high throughput and accuracy // Proceedings of the 33rd international conference on machine learning, New York, June 2022, 2016. – New York, 2016. – Vol. 48. – P. 201-210.
12. *Иващенко А.С.* Постквантовые криптографические системы: вызовы и перспективы // Журнал криптографии и информационной безопасности. – 2021. – Т. 15, № 4. – С. 18-29.

13. *Мовчан А.В., Ковалёв Д.Л.* Построение устойчивых криптографических систем с использованием адаптивных методов защиты // Информационные технологии и безопасность. – 2023. – № 4. – С. 12-20.
14. *Альбов А.* Квантовая криптография. – СПб.: ООО «Страта», 2015. – 248 с.
15. *Ruttor A. [et al.]*. Genetic attack on neural cryptography // Physical Review E, Statistical, Nonlinear, and Soft Matter Physics. – Vol. 73. – P. 036121. – PMID 16605612. – DOI: 10.1103/Physreve.73.036121.
16. *Klimov A., Mityagin A., Shamir A.* Analysis of neural cryptography // Advances in cryptology – ASIACRYPT 2002 / Y. Zheng (eds). – Springer, 2003. – P. 288-289. – DOI: org/10.1007/3-540-36178-2_18.
17. *Плонковски М., Урбанович П.П.* Использование нейронных сетей в системах криптографического преобразования информации // Известия Белорусской инженерной академии. – 2004. – № 1 (17). – С. 13-15.

УДК 621.396

М.А. Балеев

Южный федеральный университет, Россия, г. Таганрог

БАЗА ПРИЗНАКОВ ИСПОЛЬЗОВАНИЯ РАДИОЧАСТОТНОГО ПРОСТРАНСТВА ДЛЯ ЭКСПЕРТИЗЫ НЕПРАВОМЕРНОГО ИСПОЛЬЗОВАНИЯ ДИАПАЗОНОВ ЧАСТОТ

В представленной работе рассматриваются вопросы формирования базы знаний о РЧ-пространстве для экспертизы неправомерного использования диапазонов частот. В работе предлагается два подхода к детекции аномалий: алгоритмический и на основе нейросетевых технологий. В работе проведен сравнительный анализ данных методов в рамках концепции ошибок I, II рода. Практическим результатом работы является представленное ПО для ОС Windows и Linux. Целью данной работы является формирование базы знаний о поведении РЧ-пространства для экспертизы неправомерного использования диапазонов частот. Для достижения это цели балы выдвинуты следующие задачи: 1. Сбор и анализ данных о различных ситуациях работы РЧ-пространства. 2. Разработка механизма, основанного на алгоритмическом подходе, для детекции аномалий. 3. Разработка механизма, основанного на алгоритмах машинного обучения, для детекции аномалий. 4. Создание пользовательского ПО, в качестве практического применения разработанных механизмов с добавлением дополнительных функциональных возможностей.

Ключевые слова: *алгоритм, РЧ-пространства, радиочастота, активность, алгоритмы машинного обучения.*

The paper discusses the formation of a knowledge base about RF space for the examination of the misuse of frequency bands. The paper proposes two approaches to the detection of anomalies: algorithmic and based on neural network technologies. A comparative analysis of these methods is carried out within the framework of the concept of errors of the I and II types. The practical result of the work is the presented software for Windows and Linux. The purpose of this work is to form a knowledge base on the behavior of RF space for the examination of the misuse of frequency bands. To achieve this goal, the following tasks are put forward: 1. Collection and analysis of data on various situations of RF space operation. 2. Development of a mechanism based on an algorithmic approach for detecting anomalies. 3. Development of a mechanism based on machine learning algorithms for detecting anomalies. 4. Creation of user software, as a practical application of the developed mechanisms with the addition of additional functionality.

Keywords: *algorithm, RF spaces, radio frequency, activity, machine learning algorithms.*

Введение

Использование РЧ-спектра на данный момент развития технологий является одним из ключевых аспектов современных телекоммуникационных технологий. Согласно информации, представленной в отчете Global Digital [1], в 2025 году порядка 70,5% населения Земли использует беспроводные каналы связи для передачи какой-либо информации, что делает вопросы правомерного использования РЧ-пространства особенно актуальным.

Использование РЧ-спектра в контексте правовых аспектов регулируются как законодательством, так и международными соглашениями. Так, согласно приказу Госкомсвязи РФ [2] на территории Российской Федерации проведение анализа эффективности использования РЧ-пространства проводится на базе результатов работ, направленных на измерение параметров излучения и приема радиоэлектронных средств.

Работа [3] демонстрирует, что около трети выделенного частотного ресурса используется с низким уровнем эффективности, что косвенно создает предпосылки для неправомерного использования диапазонов частот. Также о высоком спросе на рассматриваемый ресурс свидетельствует статистика исследования [4], в которой говорится о том, что в период с 2023 по 2032 год доля рынка использования радиочастот вырастет на 15%.

Проблема исследования в данной теме заключается в следующем – вопреки строгой правовой и технической базы регулирования использования РЧ-спектра, наблюдается значительное количество случаев неправомерного его использования (о чем свидетельствует исследование компании Kaspersky [5], в котором говорится о высокой доле атак с использованием беспроводных каналов связи – более 6% от общего числа кибератак), что в свою очередь приводит к неблагоприятным последствиям.

Согласно работе [6] одним из наиболее используемых диапазонов частот при передаче пользовательской информации служит диапазон 2,4 ГГц, исходя из чего, исследование, представленное в работе, будет опираться на указанный диапазон частот.

Формирование базы знаний о РЧ-пространстве

С целью определения базы признаков поведения РЧ-пространства в той или иной ситуации функционирования были сформированы датасеты, записанные в момент действия определенных деструктивных воздействий, а также в ситуации нормальной работы системы (табл. 1).

Таблица 1

Объемы записанных датасетов

Ситуация	Кол-во записанных пакетов информации
Нормальное поведение	7315
Атака Jamming	8313
Атака Spoofing	6556
Атака DoS/DDoS	8378

Датасет представляет собой csv-файл, содержащий два столбца:

- frame – массив активности частот, сформированный внешним сенсором;
- class_id – метка класса состояния, присвоенная в ручном режиме: метка 0 – нормальное поведение; метка 1 – атака Jamming; метка 2 – атака Spoofing; метка 3 – атака DoS/DDoS.

Сбор датасетов проводился с использованием специализированного сенсора РЧ-пространства, представленного на рис. 1.

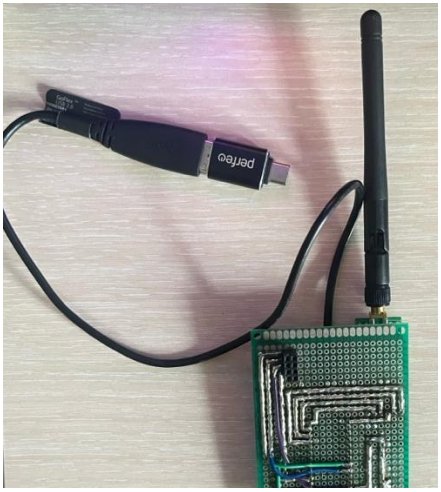


Рис. 1. Сенсор считывания состояния РЧ-спектра

Проведем полное сравнение всех упомянутых ситуаций по следующим метрикам (уже использованные метрики, дополнительные метрики):

- среднее арифметическое значение активности в ситуации;
- значение моды активности в ситуации;
- значение дисперсии активности в ситуации;

- значение стандартного отклонения активности в ситуации;
- значение выбросов по правилу 3-х сигм;
- значение коэффициента стабильности данных в ситуации.

Далее приведем некоторые графики изменения вышеуказанных величин и сделаем итоговые выводы по ним (рис. 2).

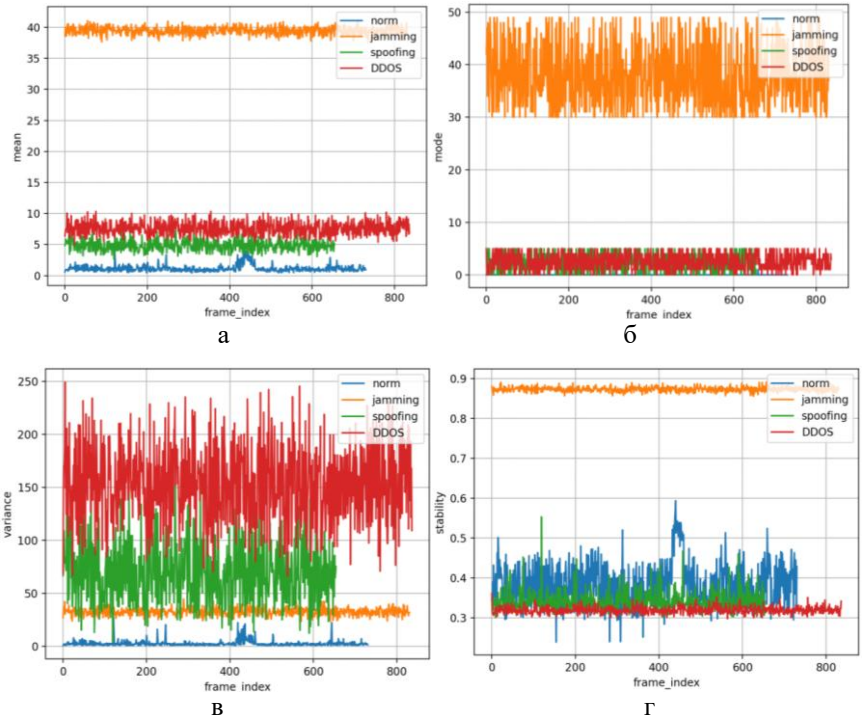


Рис. 2. Графики изменения некоторых величин состояния РЧ-пространства, где: а – график изменения среднего арифметического активности; б – график изменения моды активности; в – график изменения дисперсии активности; г – график изменения стабильности активности

Общие выводы по проведенному анализу собранных датасетов состояния РЧ-пространства в различных ситуациях:

1. Все ситуации можно четко проранжировать, используя значение среднего арифметического массива частот ситуации.
2. Ситуация “Jamming” обладает наиболее высоким показателем по метрикам стабильности, моды, среднего арифметического для массива частот ситуации.

3. Метрики дисперсии и стандартного отклонения массива частот активности ситуации удовлетворительно отражают уникальность ситуаций нормального поведения и “Jamming”.

4. Ситуации “DDoS/DoS”, “Spoofing” с неопределенной долей вероятности можно определить при помощи метрик дисперсии и стандартного отклонения, однако неравномерность полученных данных не позволяет с уверенностью использовать данные “следы”.

5. Ситуация без деструктивного воздействия также обладает сравнительно высоким уровнем стабильности, однако неравномерность данных не позволяет с уверенностью использовать данные “следы”. Данная особенность может быть связана с довольно низким уровнем шумов, на фоне которых любое активированное устройство в сети накладывает отчетливый отпечаток на весь РЧ-спектр.

6. Сопоставляя данные с графика на рисунке 6.21 и 6.22 (б), можно сделать вывод, что ситуация с деструктивным воздействием “DDoS/DoS” наиболее нестабильна относительно своих аналогов.

Исходя из полученных данных сформируем таблицу соответствия ситуации функционирования и ее поведенческому шаблону (табл. 2), на основании которого можно отделить одну ситуацию от другой согласно описанным метрикам.

Таблица 2

Значения метрик в ситуациях

Ситуация	Ориентировочное среднее значение активности	Диапазон значения активности	Диапазон значения стабильности
Без деструктивного воздействия	1.1406631601805242	от 0.41 до 4.67	от 0.24 до 0.59
Jamming	39.501817894984	от 37.54 до 41.28	от 0.86 до 0.89
Spoofing	4.889780994137442	от 2.66 до 7.6	от 0.3 до 0.55
DDoS/DoS	7.621153309975368	от 4.95 до 10.35	от 0.3 до 0.36

Алгоритмический подход к решению задачи

В основе реализации предлагаемого алгоритма лежит механизм расчета кратчайшего расстояния до объектов, расстояние рассчитывается между анализируемой точкой и объектами шаблонов, полученных заблаговременно при подготовке (табл. 2).

Общую идею алгоритма в простейшем виде можно продемонстрировать при помощи рис. 3.

Рис. 3. Расположения объектов шаблонов на оси среднего значения активности

В данном случае на оси абсцисс отображается значение активности РЧ-пространства, в свою очередь разноцветные прямоугольники – диапазоны значений средней активности шаблонов, где соответственно: желтый – ситуация без деструктивного воздействия, красный – “Jamming”, синий – “Spoofing”, зеленый – “DDoS/DoS”. Вертикальные линии на рисунке – ориентировочное среднее значение для каждой из соответствующих ситуаций. Суть алгоритма заключается в детекции попадания какой-либо входной точки в данных диапазоны, следовательно, если входная точка попала только в один диапазон, следует считать данную ситуацию искомой, однако, если точка попала в более чем 1 диапазон, необходимо рассчитать коэффициент, по которому можно будет сделать вывод о принадлежности точки к ситуации.

Коэффициент рассчитывается по следующей формуле:

$$Score = (dist\_mean/max\_dist\_mean) * (dist\_stab/max\_dist\_stab),$$

где соответственно: dist_mean – расстояние от точки среднего значения то ориентировочного значения ситуации (вертикальная линия на рис. 3), max_dist_mean – максимально имеющееся расстояние по среднему значению активности из всех, dist_stab – расстояние от точки стабильности массива до ближайшей границы диапазона значений стабильности ситуации, max_dist_stab – максимальное расстояние из расстояний стабильности.

Исходя из выдвинутого механизма селекции ситуаций, был реализован алгоритм, схема которого представлена на рис. 4.

Подход на основе алгоритмов машинного обучения

Данный подход использует методы машинного обучения для задач классификации. Перед непосредственным обучением нейросетевой модели собранные датасеты были разделены в отношении 1 к 4, то есть 20% каждого датасета было отделено от основной записи с целью будущего тестирования и определения точности обученной модели. Итого датасеты был и поделены по количеству пакетов, представленному в табл. 3.

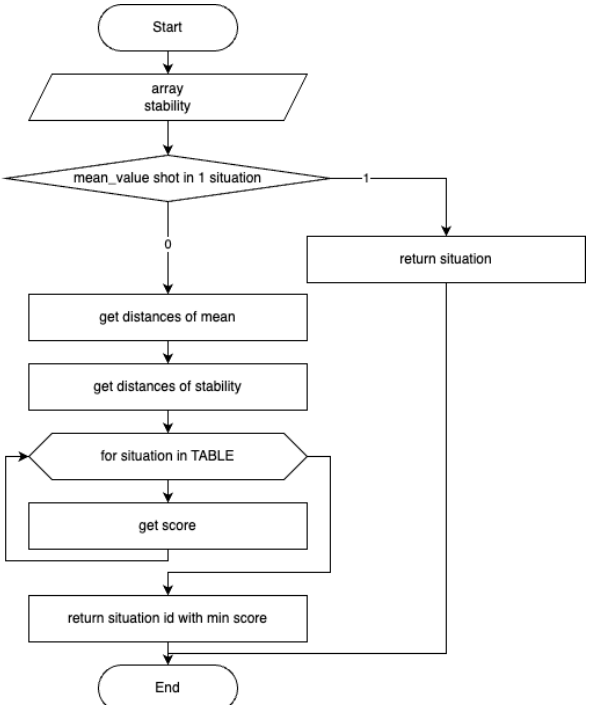


Рис. 4. Блок-схема алгоритма селекции ситуаций

Таблица 3

Разделение пакетов для обучения модели

Ситуация	Пакетов для обучения	Пакетов для тестов
Без деструктивного воздействия	5853	1462
Jamming	6652	1663
Spoofing	5241	1317
DDoS/DoS	6705	1672

Результатом работы обучения стала нейросетевая модель с рассчитанным коэффициентом точности – 0.859.

Оценим обученную модель исходя из информации, предоставленной ROC-кривой, матрицей ошибок и общим отчетом обучения. На рис. 5 представлен график ROC-кривой (кривая линия, демонстрирующая зависимость между TPR (True Positive Rate) и FPR (False Positive Rate) при изменении порогового значения вероятности. TPR – соотношение правильно-

классифицированных объектов к общему числу объектов, FPR – соотношение неправильно классифицированных объектов к общему числу объектов, AUC – площадь под ROC-кривой (1 – идеальная классификация, 0 – полностью некорректная классификация)).

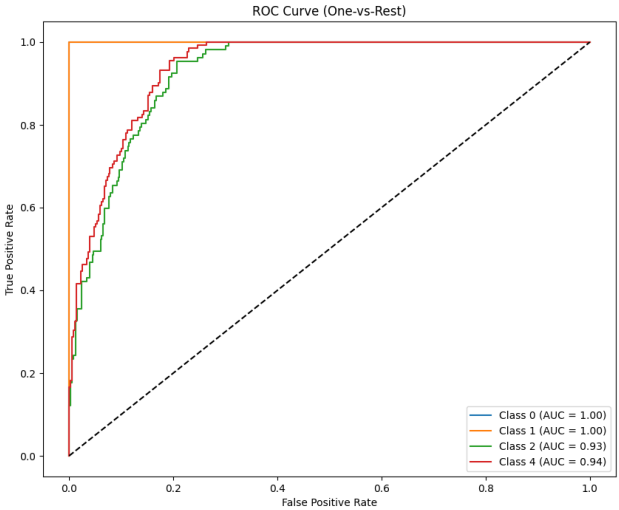


Рис. 5. График ROC-кривой

Исходя из графика ROC-кривой видно, что разделение классов для класса 0 (без деструктивного воздействия) и 1 (Jamming) оценилось по высшей оценке, оценка для разделения классов 2 (Spoofing) и 4 (DDoS/DoS) незначительно ниже, однако также высока.

На рис. 6 представлена матрица ошибок обученной модели. Данна матрица показывает сколько объектов были правильно или неправильно классифицированы. Здесь по диагонали показано количество объектов, которые были правильно классифицированы, ячейки, не находящиеся на диагонали – ситуации неправильной классификации.

Из матрицы ошибок видно, что модель отлично справляется с ситуациями отсутствия деструктивного воздействия и Jamming, однако с ситуациями Spoofing и DDoS/DoS справляется хуже (подтверждение результатов ROC-кривой). Видим, что точность (predicted) по всем классам находится на неплохом уровне, однако видно, что ситуации Spoofing, DDoS/DoS имеют более низкую точность, причиной чего является сравнительно близкое поведение в ситуациях (анализ состояний в п. 1). Однако данная ситуация не противоречит задаче детекции аномалий – система в состоянии обнаружить аномалию.

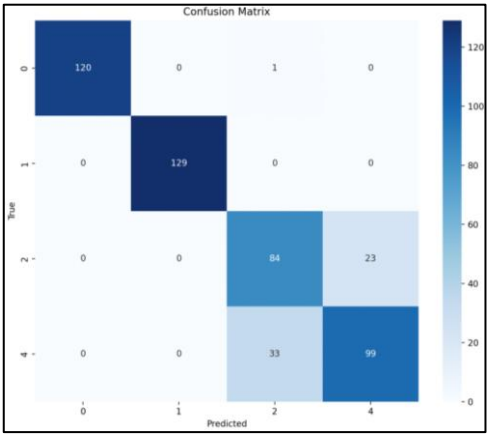


Рис. 6. Матрица ошибок обученной модели

Сравнение выдвинутых механизмов детекции

Для сравнения выдвинутых механизмов необходимо ввести два понятия:

1. Ошибка I рода – вероятность неверного отклонения нулевой гипотезы, т.е. отклонения нулевой гипотезы, когда она на самом деле верна («ложная тревога»). В данном случае речь идет о сигнализации об атаке, в то время, когда изменений, связанных с атакой, не наблюдается.

2. Ошибка II рода – вероятность остаться в рамках нулевой гипотезы, когда на самом деле она не верна («пропуск цели»). В данном случае речь идет о ситуации, когда на самом деле атака проводится, но система воспринимает состояние как нормальное.

Рассчитанные значения данных характеристик представлены в табл. 4.

Таблица 4

Значения ошибок I, II рода

Ситуация	Ошибка I рода		Ошибка II рода	
	Алгоритмический подход	Нейросетевой подход	Алгоритмический подход	Нейросетевой подход
Без воздействия	0.038	0.015	-	-
Атака Jamming	0.016	0.012	0.023	0.045
Атака Spoofing	0.238	0.153	0.002	0.011
Атака DDoS/DoS	0.08	0.132	0.012	0.037

Отметим, что ошибка II рода для ситуации без деструктивного воздействия не может быть посчитана, так ошибка данного рода подразумевает наличие деструктивного воздействия, однако концепция ситуации не предусматривает данного аспекта. Из таблицы видно, что общие результаты тестирования вполне удовлетворительны – средний уровень значения ошибки не превышает 4 процентов, однако результаты тестирования в ситуации “Spoofing” в данный момент находятся на довольно высоком уровне, что говорит о проблемах детекции данного класса событий. Как уже было сказано выше, нейросетевая модель сравнительно хорошо справилась с классификацией первых двух ситуаций, однако классификация ситуаций Spoofing и DDoS/DoS значительно упала по сравнению со своими аналогами.

Проведя анализ, каждой реализации механизма классификации аномалий в беспроводных каналах связи нельзя сделать однозначного вывода и доминировании того или иного способа получения результата – каждый метод обладает своими сильными и слабыми сторонами. Следовательно, было принято решение использовать оба подхода в итоговом продукте, так как только при таком взаимодействии общая система сможет с максимальной точностью классифицировать аномалию РЧ-пространства.

Практическое применения предложенных механизмов

В качестве практического применения разработанного алгоритма и обученной нейросетевой модели было разработано десктопное приложение для ОС Windows, ОС семейства Linux. Суть данного ПО – предоставление удобной программной прослойки между человеком (пользователем) и непосредственно механизмами детекции аномалий РЧ-пространства. Приложение использует клиент-серверную архитектуру, где сервер располагается непосредственно на пользовательском устройстве. Также стоит отметить, что модуль кроме диапазона 2.4 ГГц в состоянии обрабатывать информацию о диапазоне 915 МГц, что позитивно сказывается на возможности масштабирования системы.

Основными модулями разработанного продукта являются (рис. 7):

- модуль форматирования данных – модуль, предназначенный для приведения входного пакета информации в формате строки в формат JSON для дальнейшей работы с ним;
- модуль анализа собранных данных – модуль, использующий описанные выше механизмы детекции аномалий для получения класса ситуации;
- модуль записи собранны данных в лог-файл – модуль, предназначенный для формирования специального файла, который содержит снимки состояния РЧ-диапазона, а также полученный результат детекции;
- пользовательский интерфейс – клиентская часть ПО, отвечающая за взаимодействие с пользователем.

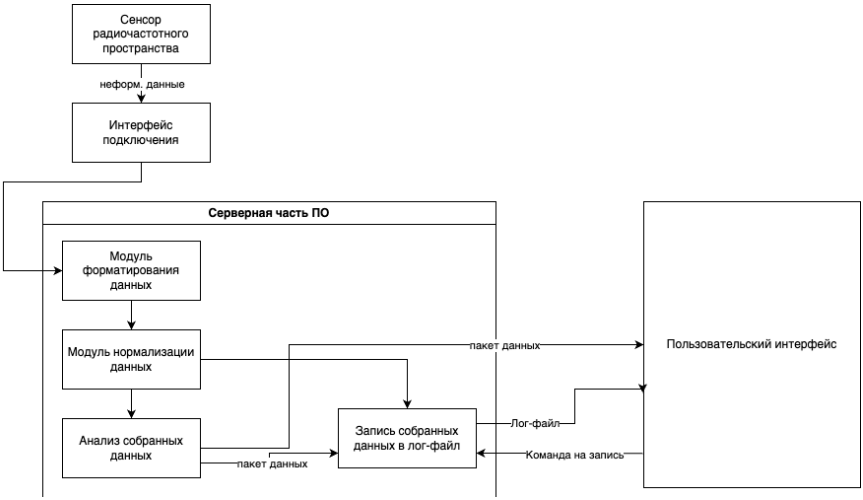


Рис. 7. Схема реализации пользовательского ПО

Разработанный продукт включает в себя следующий перечень функциональных возможностей:

- сбор информации о диапазоне 2.4 ГГц/915 МГц, как слитно, так и по раздельности (в зависимости от считывающего сенсора);
- упаковка информации о РЧ-диапазоне в файл-лог;
- возможность прикрепления текстовых комментариев к лог-записи для дальнейшего воспроизведения произошедших событий;
- анализ данных о диапазоне 2.4 ГГц на основе предложенных механизмов детекции, а также простейший базовый анализ диапазона 915 МГц на основе выборки выбросов;
- возможность чтения записанных лог-записей с возможностью построения графиков активности рассматриваемых диапазонов с возможностью выгрузки отчета в xlsx-таблицу.

Рассмотрим главный раздел предлагаемого ПО – анализ состояния РЧ-пространства в режиме реального времени (рис. 8).

В блоке № 1 расположена навигационная панель для переключения между разделами ПО: мониторинг состояния и просмотр лог-записей. В блоке № 2 расположены карточки РЧ-диапазонов, а именно наименование диапазона, график его активности (в данном случае подключен сенсор, работающий только с диапазоном 2.4 ГГц), а также результат от системы детекции аномалий пространства. В блоках № 3–4 расположены объекты для взаимодействия с картой – здесь пользователь может задать географическое расположение сенсора для определения области работы сенсора для более

точного визуального анализа (не играет роли в механизмах детекции), соответственно, в блоке № 3 пользователь может задать числовые значения координат, а в блоке № 4 пользователь может указать примерное положение на карте путем клика мыши по ней. В блоке № 5 расположены органы управления записью происходящих событий.

Рис. 8. Общий вид модуля анализа состояния РЧ-пространства

Также демонстрируемый продукт обладает системой валидации пользовательских действий – при неверном поведении пользователя система не будет выполнять заведомо ложные команды, показав пользователю модальное сообщение о названии и описании ошибки (рис. 9). В данном примере пользователь предпринял попытку инициализации соединения с внешним устройством без указания его COM-порта, соответственно, система в автоматическом режиме прервала цепочку пользовательских действий выводом соответствующего сообщения в интерфейс. Данная функциональная возможность позволит пользователю в наименьшие сроки обучиться работе с продуктом.

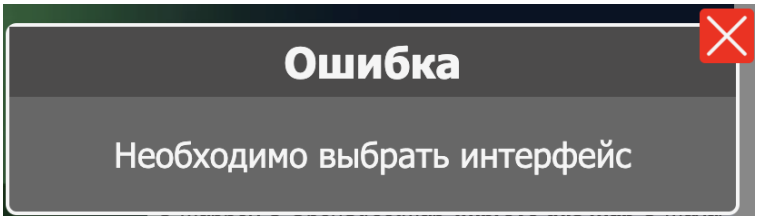


Рис. 9. Вид модального сообщения системы

Заключение

В рамках проведенного исследования были решены поставленные задачи по формированию базы знаний о поведении РЧ-пространства в различных ситуациях функционирования, которые включают в себя как нормальную работу системы, так и работу системы при каком-либо воздействии. При проведении работы были сформированы механизмы классификации аномалий поведения беспроводного канала связи, значения ошибок работы которых не превышает 4% в случае нейросетевого подхода и 25% в случае алгоритмического подхода.

Практическая реализация предложенных механизмов была выполнена в виде десктопного приложения, совместимого с несколькими ОС и охватывающего несколько диапазонов.

Таким образом, результаты работы подтверждают возможность создания эффективной системы для обнаружения аномалий в РЧ-пространстве, что соответствует выдвинутой проблеме. Перспективы дальнейших исследований и доработок существующих механизмов включают в себя совершенствование алгоритмов классификации, а также расширение массива исследуемых ситуаций за счет дополнительного сбора информации о функционировании в иных ситуациях, не описанных в работе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Бегин А.* Мобильный интернет в мире [Электронный ресурс] // ИНКЛИЕНТ: [сайт]. – 2025. – URL: https://inclient.ru/mobile-internet-stats/ (дата обращения: 25.04.2025).
2. Приказ Госкомсвязи РФ от 03.07.98 N 48.
3. *Солозобов С.А., Шевченко В.В., Щукин А.Н.* Децентрализованное использование частотного ресурса декаметрового диапазона волн в сложной помеховой обстановке // Техника средств связи. – 2020. – № 1 (149). – С. 28-36.
4. Размер и доля радиочастотного фронтового рынка 2023–2032 [Электронный ресурс] // Global Market Insights: [сайт]. – URL: https://www.gminsights.com/ru/industry-analysis/radio-frequency-front-end-market (дата обращения: 25.04.2025).
5. В первом полугодии 2024 года кратно выросло число атак на сферы телекоммуникаций и строительства / [Электронный ресурс] // kaspersky: [сайт]. – URL: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-v-pervom-polugodii-2024-goda-zafiksirovan-kratnyj-rost-atak-na-sfery-telekoma-i-stroitelstva (дата обращения: 02.04.2025).
6. *Polak L., Milos J.* Performance analysis of LoRa in the 2.4 GHz ISM band: coexistence issues with Wi-Fi // Telecommunication Systems. – 2020. – Vol. 74, No. 3. – P. 299-309.

УДК 004.056.5

А.А. Белоус, М.М. Адживапаев, М.А. Маслова

Севастопольский государственный университет, Россия, г. Севастополь

МЕТОД ВЫЯВЛЕНИЯ НЕТИПИЧНОГО ПОВЕДЕНИЯ В СЕТИ С ИСПОЛЬЗОВАНИЕМ В КАЧЕСТВЕ РАСЧЁТНОГО ИНТЕРВАЛА ПАКЕТНОЙ ВЫБОРКИ ФИКСИРОВАННОЙ ДЛИНЫ

В статье рассмотрены методы выявления нетипичного поведения в сети с использованием интеллектуальных моделей. Целью работы является поиск метода, обеспечивающего постоянный масштаб входных данных с учётом всего сетевого потока. Для достижения цели поставлены следующие задачи: выявить сильные и слабые стороны существующих исследований, предложить собственный метод, протестировать подход на различных сценариях атак. В результате подтверждена действенность предложенного метода, сформулированы направления дальнейших исследований.

***Ключевые слова**: анализ сети, нетипичное поведение, аномалии, пакетный интервал, пакетная выборка.*

The article discusses methods for detecting atypical behavior in the network using intelligent models. The aim of the work is to find a method that ensures a constant scale of input data, taking into account the entire luminous flux. To achieve this goal, the following tasks have been set: to identify the strengths and weaknesses of existing research, to propose our own method, and to test the method on various attack scenarios. As a result, the effectiveness of the proposed method has been confirmed, and directions for further research have been formulated.

***Keywords**: network analysis, atypical behavior, anomalies, batch interval, batch sampling.*

Введение

Исследования ЭАЦ InfoWatch [1] свидетельствуют о росте утечек конфиденциальной информации в мире в 2023 году более чем на 60%, при этом число скомпрометированных персональных данных удвоилось, а утечки (свыше 1 млн записей) увеличились почти на 50%. Более 94% инцидентов вызваны кибератаками, при этом 98% утечек осуществляются через сетевой канал.

По данным Positive Technologies [2], 55% российских компаний столкнулись с кибератаками в 2024 году, при этом 80% объектов атак составляли компьютеры, серверы и сетевое оборудование.

Отчёт ЭАЦ InfoWatch [3] показывает, что в 2024 году в России 76,9% зарегистрированных утечек информации произошло в результате действий внешних нарушителей, при этом основным каналом утечки остаётся сеть.

Для поддержания безопасного киберпространства применяются системы обнаружения вторжений (IDS), позволяющие обнаруживать и оперативно реагировать на потенциальные вторжения и подозрительную активность посредством мониторинга сетевого трафика. IDS могут реализовываться на основе сигнатур, аномалий или в виде гибридных систем. Сигнатурные IDS обнаруживают вторжения посредством сравнения наблюдаемого поведения с заранее определёнными шаблонами атак, что неэффективно против неизвестных, изменённых или гибридных угроз. IDS, основанные на поиске аномалий без использования сигнатур, строят представление о нормальном поведении сети и далее выявляют отклонения путём сравнения текущих значений с эталонным, однако при таком подходе велико число ложных срабатываний. В связи с этим, исследования в области построения эффективных методов выявления нетипичного поведения в сети остаются актуальными [4].

Анализ релевантных работ

В работах, посвящённых поиску метода оптимального анализа сети без использования баз сигнатур, оценка сети происходит на уровне потока или сессии, при этом под потоком понимается набор данных между отправителем и получателем, а под сессией – двунаправленный поток, включающий в себя трафик обоих направлений. Особо можно выделить следующие исследования:

1. В работе [5] авторы акцентируют разрабатывают требования к данным, которые могут быть использованы для машинного обучения, и производят их синтез, в результате чего создан датасет CIC-IDS2017. Также произведён анализа сетевых сессий посредством расчёта статистических параметров с последующим сравнением с эталонными значениями, обучены машинные модели. Однако исследование страдает отсутствием проверки предложенной методики в корпоративных сетях, что увеличивает риск ошибочного обнаружения аномалий из-за несоответствия характеристик синтетических данных реальным условиям.

2. Работа [6], являющаяся логическим продолжением предыдущего исследования, предлагает методику формирования обучающего набора для объектно-ориентированной модели обнаружения атак. Методика опирается на использование программных инструментов для моделирования трафика с учётом временных интервалов и дополнительных параметров, что является её отличительной особенностью. Недостатком является отсутствие предложений по оптимизации метода анализа трафика, предложенного в [5].

В работе [7] представлен альтернативный подход к выявлению аномалий, основанный на анализе самоподобия с использованием показателя Херста. Преимущество данного метода заключается в применении нового аналитического критерия. С другой стороны, выбор фиксированного 120-секундного интервала для анализа остаётся не обоснованным с точки зрения сравнения с другими временными отрезками, что может приводить к задержкам в обнаружении аномальных событий.

Работа [8] предлагает подход к подготовке входных данных, при котором первые n пакетов потока приводятся к фиксированной длине (обрезаются или дополняются до 100 байт), нормализуются и объединяются в единый вектор фиксированной длины в $100 \cdot n$ байт. Такой подход обеспечивает единообразие масштаба входных данных, однако теряет информацию, содержащуюся в обрезанной части пакетов или целой сессии, что может негативно сказаться на точности анализа.

На основании рассмотренных выше подходов к формированию признаков для анализа сети можно выделить следующие логические группы:

1. Выделение заранее определённых статистических признаков из сетевых потоков или сессий. Преимуществом этого метода является простота реализации и экономичность в использовании вычислительных ресурсов. Однако ограничением является необходимость определения временных интервалов потока или сессии. Длина этих интервалов может варьироваться в зависимости от нагрузки на сеть, что приводит к изменению масштаба данных, подаваемых на вход анализатора, и снижает качество обработки.

2. Анализ фиксированного набора байт. Этот подход обеспечивает сохранение неизменного масштаба признаков между различными итерациями пересчёта. Однако он требует выбора оптимального объёма байтов: слишком малый объём приводит к необходимости дополнения данных искусственными значениями, а слишком большой – к их обрезке. Оба случая могут искажать результаты анализа.

В настоящем исследовании предложен альтернативный метод формирования признаков, основанный на анализе двунаправленного сетевого потока, разбитого на фиксированные интервалы по числу пакетов. Признаки пересчитываются через каждые p пакетов, что избавляет от необходимости разделять трафик на сессии и учитывает весь объём данных. Для реализации метода требуются дампы легитимного и вредоносного трафика, собранного в одной и той же сетевой инфраструктуре, что обеспечивает качественную измеримость результатов обучения машинных моделей.

Основная часть

Предлагаемый в работе метод можно описать следующим образом:

1. Выбираются три базовых интервала для анализа, например, 10, 1 000 и 10 000 пакетов. Формируется нормальный, затем – вредоносный трафик. Для каждого из интервалов на дампах нормального и аномального

трафика формируются векторы статистических признаков (потоковых и временных), пересчитываемых через каждые *p* пакетов. Эти векторы аннотируются как "норма" или "аномалия" соответственно. Таким образом, создаются три датасета, соответствующие выбранным интервалам, каждый из которых содержит пары нормального и вредоносного трафика.

2. Полученные датасеты поочерёдно используются для обучения машинных моделей: Gradient Boosting (GB), K-Nearest Neighbors (KNN), Logistic Regression (LR), Random Forest (RF) и Support Vector Machine (SVM). Результаты обучения оцениваются по метрикам точности, прецизионности и полноты. Затем выбираются два интервала, на которых модели продемонстрировали наилучшие показатели, и вычисляется их арифметическое среднее. На основе этого среднего значения формируется новая тройка интервалов, после чего процесс повторяется.

3. Алгоритм завершается, когда идентифицирована пара интервалов, результаты обучения на которых лучше, чем при дроблении в последующих итерациях. Интервал с наименьшей длиной из этой пары признаётся оптимальным для анализа сетевого трафика в рассматриваемой инфраструктуре.

Исследование действенности метода проходило в два этапа: работа с общедоступным датасетом, а также работа с собственными данными, собранными в рамках данной работы.

Для проведения первой части исследования был выбран набор CIC-IDS2017 [9] ввиду хорошего разнообразия данных: нормальный трафик, а также семь классов кибератак. В начале эксперимента были посчитаны статистические параметры на трёх базовых интервалах для нормального трафика, а также для дампов всех вредоносных сценариев. Далее обучались машинные модели. Исходя из качества датасета, указанные выше машинные модели решали задачу множественной классификации. Качество обучения оценивалось на метриках точности, прецизионности и полноты как внутри классов, так и в среднем. При необходимости тройка интервалов корректировалась. В первой части исследования получены следующие результаты:

1. На выборке в 500 пакетов модели GB, KNN и RF показали среднюю точность 0.841, 0.797 и 0.851 соответственно.

2. Среднюю точность 0.8 показали остальные модели для 1 000 пакетов.

3. Значения прецизионности и полноты сравнимы с точностью для всех моделей.

Таким образом, модель случайного леса демонстрирует средние значения метрик, близкие к 0.9, при решении задачи множественной классификации кибеугроз на выборке в 500 пакетов.

Во второй части исследования эффективность разработанного метода проверялась в условиях, когда количество пакетов, передаваемых в секунду на протяжении определённого временного интервала (например, в течение одного

часа), подчиняется заданному статистическому распределению. В эксперименте были выбраны три типа распределений: нормальное, гамма и распределение Коши.

Для реализации эксперимента был разработан собственный генератор трафика на языке Python с использованием библиотеки NumPy. Генератор имитирует TCP/UDP-сессии между двумя хостами в течение заданного временного интервала. Сначала определяется общее число секунд *s* для данного интервала, после чего формируется массив *r* из *s* чисел, распределённых согласно выбранному статистическому закону. При этом параметры каждого распределения подбирались таким образом, чтобы математическое ожидание количества пакетов в секунду стремилось к значению 1 000.

Сохранив характеристики распределения сетевого трафика, генератор каждую секунду, в соответствии с очередным числом из массива *r*, формирует соответствующий набор пакетов (90% TCP, остальное – UDP) и отправляет их на целевой хост. Начало и конец сессии определяется случайно. Такой подход позволяет смоделировать реалистичные условия передачи данных с учётом случайных вариаций нагрузки на сеть, но при этом обеспечивает подчинённость трафика выбранному закону на протяжении всего эксперимента.

Работа проводилась с использованием среды GNS3. Схема лабораторного стенда, эмулирующего небольшую компьютерную сеть с потенциалом масштабирования, представлена на рис. 1.

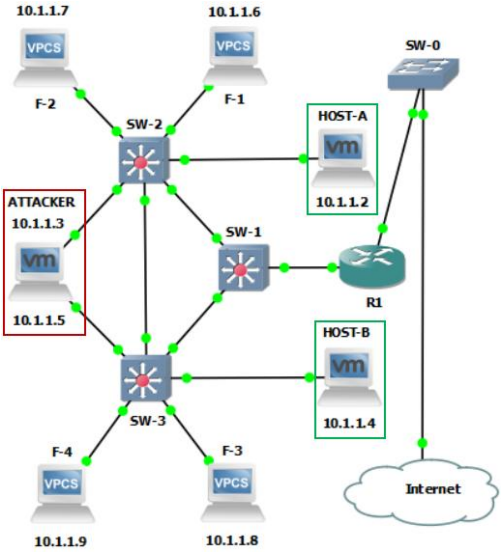


Рис. 1. Топология киберполигона, используемого в исследовании

На рис. 1 обозначено следующее оборудование:

1. R1 – маршрутизатор, образ c3725-adventerprise [10], настроены NAT и DHCP.
2. SW-0—SW-3 – коммутаторы, образ i86bi-linux-l2-adventerprise [10].
3. F-1—F-4 – хосты, предустановлены в GNS3, предназначены для имитации разнообразных сетевых взаимодействий и нагрузки на оборудование.
4. HOST-A, HOST-B – хосты, между которыми снимался трафик, виртуальные машины Kali Linux и Parrot HTB на базе VMware соответственно.
5. ATTACKER – машина злоумышленника, Parrot OS на базе VMware.

В рамках исследования для каждого рассматриваемого статистического закона были собраны два дампа сетевого трафика продолжительностью в 1,5 часа: один отражал нормальное взаимодействие между хостами A и B, а второй – аномальное. Для компрометации сети была смоделирована атака типа "Человек по середине" с использованием уязвимостей протоколов ARP и STP. При этом скомпрометированный трафик не был разделён на временные интервалы, фиксирующие начало и окончание атаки, поскольку он практически непрерывно проходил через узел злоумышленника.

В данной части эксперимента решалась задача бинарной классификации, или определение состояния сети: происходит ли атака в настоящий момент времени, или нет. Аналогично первой части исследования, проводился поиск оптимальной длины для пакетной выборки. Выбранные модели обучались на дампах трафика, влияние длины пакетной выборки на качество классификации оценивалось по точности, прецизионности и полноте. Во второй части исследования получены следующие результаты:

1. Для нормально распределённого трафика модели GB и RF показали значения метрик, близкие к 0.95 на выборке в 5 000 пакетов.

2. При гамма-распределении результаты, близкие к 0.98, показали также модели GB и RF, а остальные – чуть выше 0.9; при этом оптимальная длина выборки для всех моделей составила 1 000 пакетов.

3. В случае, когда трафик распределён по Коши, каждая модель показала значения метрик около 0.98, как на выборках в 1 000, так и в 5 000 пакетов.

Таким образом, модель случайного леса также показала лучший результат при минимальной длине пакетного интервала. Метод с использованием фиксированной длины пакетной выборки обеспечил высокую точность выявления аномалий в случае компрометации протоколов канального уровня в трафике, подчинённом статистическим законам.

Заключение

В настоящей работе проведено исследование, касающееся методов формирования векторных признаков для выявления сетевых аномалий интеллектуальными моделями. В ходе работы были рассмотрены подходы, основанные на использовании временных интервалов и фиксированных байтовых отрезков, отмечены их сильные и слабые стороны. Далее предложен собственный метод формирования векторов, основанный на использовании в качестве расчётного интервала пакетной выборки с фиксированной длиной, протестирована действенность подхода.

Тестирование состояло из двух частей, в ходе которых были получены следующие результаты:

1. На датасете CIC-IDS2017 достигнута средняя точность 0,85 при решении задачи многозначной классификации.
2. При анализе трафика, распределённого по некоторому закону, точность обнаружения аномалий составила 0,98.

Предложенный метод демонстрирует результаты, сопоставимые с результатами аналогичных исследований, и обладает преимуществами, связанными с использованием полного объёма трафика и сохранением постоянного масштаба данных, используемых для обучения моделей. Однако поиск оптимальной длины пакетной выборки требует повторного пересчёта векторов признаков и переобучения моделей на каждой итерации алгоритма, что связано с вычислительными затратами.

Дальнейшее направление исследования может быть связано с оптимизацией алгоритма поиска оптимальной длины пакетной выборки; расширением числа атак, используемых в эксперименте с трафиком, распределённым по математическим законам; переходом от равномерного распределения атакующего трафика к моделированию всплесков, имитирующих спонтанные действия злоумышленника; апробацией моделей, обученных на одних типах атак, в сценариях с атаками, которые не вошли в обучающую выборку.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Экспертно-аналитический центр ГК InfoWatch. Аналитический отчёт. Исследование утечек информации в мире за последние два года [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics/analitika/issledovani ye-utechek-informatsii-v-mire-za-posledniye-dva-goda, свободный (дата обращения: 15.03.2025).
2. Актуальные киберугрозы: III квартал 2024 года [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iii-kvartal-2024-goda/#id18, свободный (дата обращения: 15.03.2025).
3. Экспертно-аналитический центр ГК InfoWatch. Аналитический отчёт. Утечки информации в России: отчет за прошедший год [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-v-rossii-otchet-za-proshedshiy-god, свободный (дата обращения: 15.03.2025).

4. *Ускова М.А., Агафонова В.В.* Преимущества и недостатки систем обнаружения вторжений как средств защиты корпоративной информации // Известия института менеджмента СГЭУ. – 2022. – № 1 (25). – С. 134-136. – DOI: 10.46554/PICS-2022.1-pp.134.
5. *Sharafaldin I., Lashkari A.H., Ghorbani Ali A.* Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization // In Proc. of the 4th International Conference on Information Systems Security and Privacy (ICISSP). – 2018. – P. 108-116.
6. *Гетьман А.И., Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А.* Методика сбора обучающего набора данных для модели обнаружения компьютерных атак // Труды ИСП РАН. – 2021. – Т. 33. – Вып. 5. – С. 83-104. – DOI: 10.15514/ISPRAS – 2021 –33(5) –5.
7. *Веселова В.А., Коломойцев В.С.* Подход к обнаружению аномалий в самоподобном сетевом трафике // Надежность . – 2023. – Т. 23, № 2. – С. 57-63. – DOI: 10.21683/1729-2646- 2023-23-2-57-63. – EDN KLWDU.
8. *Lunardi W.T., Lopez M.A., Giacalone J.P.* ARCADE: Adversarially Regularized Convolutional Autoencoder for Network Anomaly Detection. MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE, 2022.
9. Intrusion Detection Evaluation Dataset (CIC-IDS2017) [Электронный ресурс]. – Режим доступа: https://www.unb.ca/cic/datasets/ids-2017.html, свободный (дата обращения: 15.03.2025).
10. Cisco Images For GNS3 [Электронный ресурс]. – Режим доступа: https://github.com/hegdepavankumar/Cisco-Images-for-GNS3-and-EVE-NG, свободный (дата обращения: 15.03.2025).

УДК 004.056

З.А. Быстрая

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ РАССЛЕДОВАНИИ ИНЦИДЕНТОВ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

Рассматривается подход к созданию системы поддержки принятия решений при расследовании инцидентов в киберфизических системах. Целью исследования является разработка системы, обеспечивающей повышение эффективности выявления, анализа и реагирования на инциденты киберфизических систем за счет процессов обработки данных и формирования рекомендаций. Для достижения поставленной цели исследования, были решены следующие задачи: проведен сравнительный анализ существующих методов и стандартов, а также выявлены их ограничения применительно к киберфизическим системам. Предложена структура графа инцидентов, позволяющая визуализировать взаимосвязи между событиями и упростить анализ атак. В результате исследования была создана система, обеспечивающая комплексный подход к расследованию инцидентов в КФС. Она позволяет автоматизировать процессы обнаружения вредоносного вторжения, минимизировать время реагирования и снижать риски, связанные с многоуровневыми атаками.

Ключевые слова: *киберфизические системы, система поддержки принятия решений, инциденты, атаки, угрозы, уязвимость, безопасность.*

An approach to the creation of a decision support system for the investigation of incidents in cyber-physical systems is considered. The purpose of the study is to develop a system that provides an increase in the efficiency of detection, analysis, and response to incidents of cyber-physical systems through data processing processes and the formation of recommendations. To achieve the goal of the study, the following tasks were solved: a comparative analysis of existing methods and standards was carried out, as well as their limitations in relation to cyber-physical systems were identified. An incident graph structure is proposed to visualize the relationships between events and simplify the analysis of attacks. As a result of the study, a system was created that provides an integrated approach to the investigation of incidents in the CPS. It automates malicious intrusion detection processes, minimizes response time, and reduces the risks associated with multi-layered attacks.

Keywords*: cyber-physical systems, decision support system, Incidents, Attack, Threats, vulnerability, security.*

Введение

Киберфизические системы (КФС) играют ключевую роль в функционировании критической инфраструктуры, такой как энергетика, транспорт и промышленность. Данные системы глубоко интегрируются цифровыми и

физическими процессами, что повышает их эффективность. Однако такое внедрение процессов может сделать уязвимой систему к угрозам безопасности людей и техногенным авариям.

В настоящее время киберугрозы становятся всё более масштабные и разрушительные, поэтому традиционные методы расследования инцидентов при помощи Security Information and Event Management (SIEM) и Supervisory Control and Data Acquisition (SCADA) систем, стандартов Adversarial Tactics, Techniques & Common Knowledge (MITRE ATT&CK) и форматов Structured Threat Information Expression (STIX) ориентированы лишь на анализ киберфизических аспектов безопасности. При этом физические процессы остаются за пределами внимания, что значительно снижают эффективность реагирования на инциденты в КФС.

Для решения данной проблемы была разработана система поддержки принятия решений при расследовании инцидентов в киберфизических системах. Особенностью данной системы является использование графа инцидентов, который позволяет визуализировать взаимосвязи между событиями и прогнозировать возможные атаки. Граф инцидентов представляет собой структурированную модель, которая описывает технические и физические аспекты инцидентов, представляет комплексный подход при расследовании инцидентов.

Обзор вспомогательных решений и стандартов для расследования инцидентов в киберфизических системах

Киберфизическая система – организационно–техническая концепция управления информационными потоками, интегрирующая вычислительные ресурсы в физические процессы производства [1].

Актуальность обеспечения безопасности киберфизических систем вызвана критичностью нарушения их бесперебойного функционирования. В связи с этим, рассматривая задачу обеспечения безопасности КФС, важно учитывать не только безопасность информации, но и корректность протекания технологических процессов.

Для расследования инцидентов в киберфизических системах используют достаточно много современных методов. Среди них – SIEM и SCADA, которые позволяют отслеживать как внутренние изменения системы, так и мониторить физические параметры. Кроме того, существуют широко известные стандарты STIX [2], MITRE ATT&CK [3]. Они помогают моделировать угрозы, координировать усилия по их предотвращению, а также формировать структурированную базу знаний, описывающую тактики и техники злоумышленников.

Применение SIEM-системы при расследовании инцидентов в киберфизических системах

SIEM–системы используются для сбора и анализа событий безопасности в режиме реального времени [4].

Для расследования инцидентов в киберфизических системах используются следующие функции:

- Сбор данных: собирает информацию с всевозможных источников сетевого и канального уровня.
- Анализ логов: просматривает журнал событий на несанкционированный доступ и отклонение трафика.
- Корреляция событий: связывает события разной тематики в единую цепочку, чтоб найти причины и последствия инцидентов.
- Оповещение: при выявлении угрозы или уязвимости приходит уведомление оператору, чтоб предотвратить данный инцидент.

Рассмотрим сценарий расследования инцидента в киберфизической системе с использованием SIEM– системы:

- Обнаружение аномалии: системы регистрируют резкий скачок сетевого трафика, а также получает сигнал от других систем о превышении температуры оборудования.
- Корреляция событий: система связывает вредоносные события, чтоб выявить возможную атаку на киберфизическую систему, например, злоумышленник использовал DDoS–атаку для перегрузки системы и вызвать сбой в работе оборудования.
- Формирование рекомендаций: система выдает рекомендации для оператора, чтоб можно было вовремя среагировать на инцидент.
- Документирование инцидента: вся информация по событиям документируется внутри систему, чтоб можно было детально расследовать инцидент, а также выявить на что он повлиял больше всего, насколько был критичен для киберфизической системы.

Применение SCADA-системы при расследовании инцидентов в киберфизических системах

SCADA – системы являются ключевым компонентом киберфизической системы, которые обеспечивают бесперебойный мониторинг промышленных контроллеров в энергетике, транспорте, на всевозможные отклонения по датчикам температуры, света и управления [5].

Этапы расследования инцидентов в киберфизических системах с использованием SCADA систем:

- Обнаружение инцидента. Данное обнаружение происходит при исследовании автоматических уведомлений о возможных выходах из строя, а также проводится сравнительный анализ с текущими и эталонными показателями.

- Сбор и анализ данных. Журнал событий собирает в себе информацию того, кто и когда вносил изменения, а также сами действия операторов и изменения конфигураций.
- Восстановление событий. Можно определить точку входа злоумышленника, выявить возможные повреждения данных и оборудования, а также выстроить временную шкалу атаки.
- Реагирование и восстановление. При выявлении вредоносных атак можно восстановить конфигурации из резервных копий, а также сгенерировать отчет для внутреннего расследования.

В табл. 1 приведены примеры использования SCADA системы в расследовании инцидентов в киберфизических системах.

Таблица 1

Примеры использования SCADA системы в расследовании инцидентов в КФС

	Инцидент	Роль SCADA
[6]	Атака на Saudi Aramco	SCADA–системы помогли отследить распространение вируса в смежных IT–сетях с помощью логов
[7]	BlackEnergy	Вредоносные макросы в Excel-файлах предоставили доступ злоумышленникам к сетям энергокомпаний. Логи данной системы показали несанкционированные команды на отключение подстанций
[8]	Утечка данных водоканала в Израиле	Хакеры пытались изменить уровень хлора в воде. SCADA система зафиксировала аномальные запросы, что позволило быстро остановить атаку.
[9]	Stuxnet	Вирус модифицировал код Siemens Step7, подменяя команды центрифуг. Аномалии обнаружили через анализ SCADA логов и физические проверки оборудования

Применение STIX при расследовании инцидентов в киберфизических системах

STIX – это открытый стандарт, позволяющий формализовать информацию о киберугрозах, что особенно важно для анализа атак на киберфизическую систему [10].

Этапы расследования инцидентов с использованием STIX:

1. **Сбор и формализация данных об инциденте.** Данный стандарт позволяет представить в структурированном виде наблюдаемые данные, индикаторы компрометации и тактики злоумышленников.

2. **Анализ и корреляция угроз.** STIX поддерживает связи между объектами, что позволяет выявлять связанные атаки, определять уязвимые узлы киберфизической системы, а также прогнозировать следующие этапы злоумышленников.
3. **Обмен информацией между организациями.** Позволяет передавать данные в CERT и регуляторы, интегрироваться с MISP, а также автоматизировать блокировку угроз через TAXII.
4. **Пост-инцидентный анализ и отчётность.** Помогает создавать детальный отчет, строить графы атак, обновлять правила обнаружения.

В табл. 2 приведены примеры использования STIX в расследовании инцидентов в киберфизических системах.

Таблица 2

Примеры использования STIX в расследовании инцидентов в КФС

	Инцидент	Использование STIX
[11]	APT- группа «Triton»	STIX описание TTPs помогло выявить атаки на системы безопасности нефтехимических заводов
[12]	Компания «Industroyer2»	STIX использовался для описания методов атак на энергосети через протокол IEC 104.

Применение MITRE ATT&CK при расследовании инцидентов в киберфизических системах

MITRE ATT&CK – структурированная база знаний о тактиках и техниках киберпреступников, которая стала стандартом для анализа угроз и расследования инцидентов в киберфизических системах [13].

Применение MITRE ATT&CK для расследования инцидентов в КФС:

1. Моделирование атак. Создание сценариев атак
2. Анализ тактик и техник. С помощью данного стандарта можно выявить тактики и техники злоумышленников
3. Оценка уровня защищенности. Помогает оценить, насколько хорошо текущие меры безопасности защищают КФС от угроз
4. Разработка контрмер. При помощи данного стандарта можно разработать план действий реагирования для противодействия угрозам.
5. Документирование инцидентов. Предоставляет структурированный вариант документирования инцидентов, что упрощает их анализ и предотвращение кибератак в дальнейшем.

Таким образом, проведя анализ современных подходов к мониторингу и расследованию инцидентов в киберфизических системах, таких как SIEM, SCADA, формат описания угроз STIX и стандарт для выявления тактик, техник и процедур злоумышленника MITRE ATT&CK, стало очевидным создание инструментов для более глубокого понимания взаимосвязей между различными типами инцидентов. В рамках данного исследования пришла идея построить граф инцидентов КФС, а также создать таблицу, которая структурирует входящие компоненты инцидентов КФС.

Построение графа инцидентов киберфизических систем

Граф инцидентов представляет собой визуализацию взаимосвязей между различными видами атак, аномалий, уязвимостей и угроз. Для построения графа была выбрана программа Obsidian [14], которая обладает удобным инструментарием для визуализации, а также динамически обновлять данные, добавляя новые связи и компоненты.

Для построения данного графа были собраны данные, такие как: кибератаки, физические воздействия, погодные аномалии.

Созданы узлы графа, в которые входят: индикаторы, инциденты, описание данных инцидентов, метки машины состояний, метки модуля анализатора атак, атаки, уязвимости, угрозы, аномалии.

Установлены связи между узлами графа, где инцидент связан с индикатором, описанием инцидента, метки машины состояний и меткой модуля анализатора атак. Модуль анализатора атак связан с угрозой, аномалией, атакой и уязвимостью.

Метки машины состояний выполняют функции отслеживания полета киберфизической системы, определяя точность полета согласно его полетному заданию, позволяя определить соответствие реальных с фактическими данными киберфизической системы [15].

Метки модуля анализатора атак выполняют функции отслеживания изменений в параметрах КФС, позволяет выявлять аномальные отклонения и классифицировать на основе правил корреляций [16].

Визуализация графа была создана при помощи программы Obsidian, где представление выполнено в виде связного дерева, где каждый узел соединен с другими через логические связи (рис. 1).

Для дополнительной структуризации данных была создана таблица, которая содержит информацию об компонентах графа по инцидентам киберфизических систем.

В табл. 3 представлено описание компонентов входящих в граф инцидентов киберфизических систем.

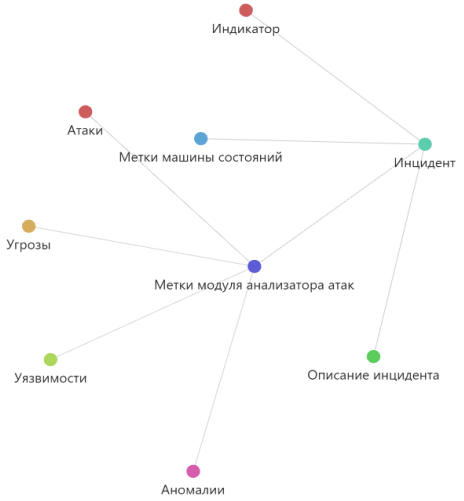


Рис. 1. Граф инцидентов киберфизических систем

Таблица 3

Описание входящих компонентов графа инцидентов киберфизических систем

Индикатор	Инцидент	Описание инцидента	Метка анализатора атак	Угроза	Атака	Уязвимость	Аномалии	Метка машины состояний
IN-1	Изменение траектории движения узла КФС в результате атаки подмены навигационного сигнала	Злоумышленник располагается вблизи КФС и подает сигнал большей мощности на нужной частоте, при этом изменяя валидные данные о координатах полета на собственные	Метка с информацией о подделки навигационного сигнала GPS_SPOOFING	Нарушение целостности данных. В результате подмены данных координат КФС может отклониться от маршрута, что приведет к аварии или потере контроля над системой	GPS-Spoofing	Отсутствие механизмов аутентификации сигнала GPS или навигационных данных	Показания навигационного сигнала не соответствуют данным других датчиков	l_flg int [0,1,2] - Метка доверия к режиму полета l_st int [0,1,2]- Метка доверия состоянию l_crd int [0,1,2] - Метка доверия к координатам 0_crd int [0,1]- Метка доверия к величине изменения координат l_stl int [0,1,2]-Метка доверия количеству спутников l_stl int [0,1]- Метка доверия к величине изменения количества спутников l_alt int [0,1]- Метка доверия к величине изменения высоты
IN-2	Изменение траектории движения узла КФС в результате низкого уровня связи	Модуль оператора с антенной для связи располагается на далеком расстоянии от КФС	Метка с информацией о низком заряде аккумулятора (LOW_BATTERY)	Потеря связи между оператором и КФС. Большое расстояние может вызвать слабый сигнал, тем самым будут задержки или потеря связи	Атаки нет	Ограниченная дальность действия радиоканала связи	Снижение качества связи между оператором и КФС	l_chr int [0,1,2] - Метка доверия к заряду батареи 2_ chr int [0,1] - Метка доверия к направлению изменения заряда батареи l_flg int [0,1,2] -Метка доверия к режиму полета l_st int [0,1,2]- Метка доверия состоянию l_crd int [0,1,2] -Метка доверия к координатам

Окончание табл. 3

IN-3	Изменение траектории движения узла КФС в результате атаки на бортовое ПО	Злоумышленник использует известные уязвимости ПО для захвата контроля над КФС	Метка с информацией об атаки ПО SOFTWARE_ATTACK	Полный или частичный захват управления КФС	Exploit	Отсутствие регулярного обновления. Недостаточная защита от эксплуатации уязвимостей	Необычное поведение КФС. Ошибки в работе ПО или сбои в выполнении задач	l_stl int [0,1,2]-Метка доверия количеству спутников l_flg int [0,1,2] -Метка доверия к режиму полета l_st int [0,1,2]- Метка доверия состоянию l_crd int [0,1,2] -Метка доверия к координатам
IN-4	Получение ложных данных о состоянии окружающей среды в связи с подделкой видеопотока	Злоумышленник подменяет видеопоток, передаваемый с камеры КФС	Метка с информацией о подделки видеопотока VIDEO_STREAM_FORGERY	Оператор получает ложную информацию о состоянии окружающей среды	Video Stream Spoofing	Использование стандартных протоколов передачи данных без дополнительной аутентификации. Недостаточная проверка целостности данных видеопотока	Видеопоток содержит аномальные или несоответствующие реальности данные	l_stl int [0,1,2]-Метка доверия количеству спутников l_flg int [0,1,2] -Метка доверия к режиму полета l_st int [0,1,2]- Метка доверия состоянию l_crd int [0,1,2] -Метка доверия к координатам l_alt int [0,1]- Метка доверия к величине изменении высоты
IN-5	Перебои в передаче команд с модуля оператора в связи с атакой отказ в обслуживании	Злоумышленник отправляет огромное количество запросов для перегрузки системы запросами или трафиком, что приводит КФС к неработоспособности	Метка с информацией об атаки отказ в обслуживании DDoS_ATTACK	Потеря доступности системы	Denial of Service (DoS/DDoS)	Отсутствие механизмов защиты от перегрузки. Использование открытых каналов связи без фильтрации.	Резкое увеличение нагрузки на систему. Прерывиста я или нестабильная связь между компонентами системы.	l_stl int [0,1,2]-Метка доверия количеству спутников l_flg int [0,1,2] -Метка доверия к режиму полета l_st int [0,1,2]- Метка доверия состоянию l_crd int [0,1,2] -Метка доверия к координатам l_alt int [0,1]- Метка доверия к величине изменении высоты

Вывод

В данной работе был проведен анализ существующих методов и стандартов, таких как SIEM, SCADA, STIX, MITRE ATT&CK, с целью их применения для расследования инцидентов в киберфизических системах. На основе анализа была предложена архитектура системы, основанная на графе инцидентов, которая визуализирует взаимосвязи между компонентами: индикатор, инцидент, описание инцидента, метки анализатора атак, угроза, аномалия, уязвимость, атака, метки машины состояний.

В рамках исследования было рассмотрено 30 часто встречающихся инцидентов в КФС, которые были подробно проанализированы и описаны в виде таблицы, из которых 5 инцидентов КФС представлены в данной статье.

В дальнейшем планируется исследовать дополнительные инциденты для расширения базы данных и повышения точности прогнозирования. Предложенная система обеспечивает комплексный подход к расследованию инцидентов и защите КФС.

Благодарности

Исследование выполнено при поддержке НИОКР № Пр01–24 «Платформа принятия решений для повышения киберустойчивости автономного БПЛА»

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Громаков Е.И., Сидорова А.А.* Современные технологии. Киберфизические системы. – 2021.

2. Introduction to STIX: сайт. – [Электронный ресурс]: https://oasis-open.github.io/cti-documentation/stix/intro.html (дата обращения: 26.03.2025).
3. MITRE ATT&CK: сайт. – [Электронный ресурс]: https://attack.mitre.org/ (дата обращения: 27.03.2025).
4. *Зегжда Д.П. и др.* Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. – 2021.
5. *Bailey D., Wright E.* Practical SCADA for industry. – Elsevier, 2003.
6. *Кандаков А.Е.* Современные методы киберзащиты в нефтегазовой промышленности: обзор актуальных технологий и стратегий для защиты автоматизированных систем от кибератак // Вестник науки. – 2024. – Т. 4, №. 5 (74). – С. 1411-1417.
7. *Case D.U.* Analysis of the cyber attack on the Ukrainian power grid // Electricity information sharing and analysis center (E-ISAC). – 2016. – Т. 388, No. 1-29. – P. 3. 8.
8. *Tabansky L.* Cyber security challenges: the Israeli water sector example // Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level. – Cham: Springer International Publishing, 2016. – С. 205-219.
9. *Langner R.* Stuxnet: Dissecting a cyberwarfare weapon //IEEE security & privacy. – 2011. – Vol. 9, No. 3. – P. 49-51. – DOI: 10.1109/MSP.2011.67.
10. Barnum S. Standardizing cyber threat intelligence information with the structured threat information expression (stix) // Mitre Corporation. – 2012. – Vol. 11. – P. 1-22.
11. Стоящая за вредоносом Triton группа снова атакует КИИ по всему миру: сайт. – [Электронный ресурс]: https://www.anti-malware.ru/news/2018-05-24-1447/26349 (дата обращения: 24.03.2025).
12. *Панин Д.Н., Бобков Е.О., Балашова Е.А.* Анализ кибератак на критическую информационную инфраструктуру с IOT технологиями // Автономия личности. – 2020. – № 2 (22). – С. 55-64.
13. Ahmed M. et al. MITRE ATT&CK-driven cyber risk assessment // Proceedings of the 17th International Conference on Availability, Reliability and Security. – 2022. – P. 1-10.
14. Obsidian: сайт. – [Электронный ресурс]: https://publish.obsidian.md/help-ru/Obsidian/Obsidian (дата обращения: 20.03.2025).
15. *Basan E., Lapina M., Lesnikov A., Basyuk A., Mogilny A.* Trust Monitoring in a Cyber-Physical System for Security Analysis Based on Distributed Computing. – Cham: Springer, 2023. – 702 p.
16. *Basan E., Basan A., Nekrasov A., Basyuk A., Lesnikov A.* Trusted Operation of Cyber-Physical Processes Based on Assessment of the System's State and Operating Mode // Sensors. – 2023. – Vol 23, No 4. – P. 1996.
17. *Bystraya Z., Mogilny A., Lesnikov A., Lapin V.* Development of a Framework for Describing Security Incidents //International Workshop on Advanced Information Security Management and Applications. – Cham: Springer Nature Switzerland, 2024. – P. 19-30.

УДК 004.087.2

Д.Е. Вардиков, Е.С. Абрамов

Южный федеральный университет, Россия, г. Таганрог

ВОССТАНОВЛЕНИЕ УДАЛЕННЫХ ДАННЫХ С СИЛЬНО ФРАГМЕНТИРОВАННЫХ НОСИТЕЛЕЙ

Цель и задачи научно-исследовательской работы проанализировать и экспериментально проверить эффективность приложений для восстановления данных с сильно фрагментированных дисков и, как следствие, поиск наилучшего из них.

Ключевые слова: *фрагментация данных, восстановление данных, файловая система, сигнатура.*

The purpose and objectives of the research work are to analyze and experimentally test the effectiveness of data recovery applications from highly fragmented disks and, as a result, to find the best one.

Keywords: *data fragmentation, data recovery, file system, signature.*

Введение

В современном мире стремительно развиваются информационные технологии и данные играют значимую роль в жизни как отдельных людей, так и организаций. Хранение информации на электронных носителях становится неотъемлемой частью повседневной деятельности. Однако с ростом объемов данных и сложности их структуры возрастает вероятность потери информации из-за аппаратных сбоев, программных ошибок или действий пользователей. Одной из наиболее сложных задач в области восстановления данных является работа с сильно фрагментированными дисками, где информация разбросана по множеству несмежных секторов, что значительно усложняет процесс её извлечения.

Актуальность

Фрагментация данных – это естественный процесс, возникающий при длительном использовании дисковых накопителей. Она возникает вследствие многократной записи, удаления и изменения файлов, что приводит к распределению частей одного файла по различным участкам диска. При выходе из строя такого накопителя или повреждении файловой системы процесс восстановления данных становится крайне трудоемким, требующим применения специализированных алгоритмов и методов анализа. Однако традиционные методы восстановления данных часто оказываются не-

эффективными при работе с сильно фрагментированными дисками, что делает необходимым поиск новых подходов и технологий для решения данной проблемы.

Потеря данных на сильно фрагментированных дисках может быть вызвана различными факторами:

- Аппаратные сбои: выход из строя жесткого диска, повреждение магнитных пластин или контроллера.
- Программные ошибки: сбои в работе операционной системы или файловой системы, приводящие к повреждению метаданных.
- Вирусные атаки: удаление или шифрование файлов вредоносным программным обеспечением.
- Человеческий фактор: случайное удаление или форматирование диска.

Особую сложность представляет ситуация, когда фрагментация сочетается с повреждением метаданных файловой системы. В этом случае восстановление данных требует глубокого анализа как логической структуры, так и физического состояния накопителя [1].

Восстановление данных: основные подходы и алгоритмы

Восстановление данных – это процесс восстановления утраченных или поврежденных данных с помощью специализированных методов и инструментов. Основные подходы и алгоритмы включают:

1. Анализ метаданных файловой системы, который используется, когда файловая система частично или полностью сохранилась, поскольку метаданные файловой системы (например, таблицы FAT, MFT в NTFS) содержат информацию о расположении файлов на диске. Преимуществом данного метода является высокая точность восстановления, минимальные временные затраты, однако он неэффективен при полном повреждении метаданных [2].

2. Сигнатурный анализ, который используют для сканирования дисков на наличие характерных заголовков файлов (например, JPEG-файлы начинаются с сигнатуры FF D8 FF). Этот метод работает даже при полном повреждении файловой системы. Но с его помощью невозможно восстановить имена файлов и их структуру, а также возможны ложные срабатывания [3].

3. Анализ свободного пространства обеспечивает поиск данных в тех областях диска, которые помечены как свободные, но еще не перезаписаны. Это позволяет восстановить недавно удаленные файлы, но при этом эффективность снижается при активной записи новых данных [4].

4. Использование "сырого" восстановления (raw recovery) восстанавливает данные без учета файловой системы, основываясь на анализе структуры файлов. Данный метод работает даже при полной потере файловой

системы, хотя требует значительных временных затрат и восстановленные файлы часто лишены имен и структуры [5].

5. Алгоритмы восстановления удаленных данных позволяют анализировать области диска, где ранее хранились удаленные файлы, с целью их восстановления. Благодаря этим алгоритмам обеспечивается поиск заголовков файлов и работоспособность методов реконструкции файлов на основе их структуры [6].

6. Методы восстановления после форматирования используются для восстановления данных после быстрого или полного форматирования диска. Их использование обеспечивает быстрое форматирование оставляет данные нетронутыми, тогда как полное форматирование может перезаписать часть информации [7].

7. Гибридные методы – комбинирование нескольких подходов (например, анализ метаданных и сигнатурный анализ) для повышения эффективности восстановления [8].

Программы для восстановления данных

Ранее мною были рассмотрены теоретические основы некоторых методов, которые используются в программах для восстановления данных с сильно фрагментированных носителей, а также были выявлены их сильные и слабые стороны. Однако объективную оценку эффективности данных методов по имеющейся информации сделать нельзя, поскольку на практике для создания программ по восстановлению данных, обычно, применяют сразу несколько методов.

В основу комбинированного типа входит использование сигнатурного анализа и дальнейшего анализа файловой системы. При обнаружении повреждения файловой системы программа переходит в сигнатурное восстановление. Самыми известными представителями данной подгруппы являются R-Studio, UFS Explorer (рис. 1) и DMDE.

Группа же интеллектуальных реконструкторов восстанавливается информацию с помощью анализа метаданных (MFT). Перед началом восстановления программа анализирует MFT, FAT-таблицы или inode, чтобы в дальнейшем можно было восстановить структуру файла. А также в работе используются эвристические алгоритмы для сборки фрагментированных файлов. На сегодняшний день самыми популярными интеллектуальными реконструкторами являются ReclaiMe Pro и Active@ File Recovery (рис. 2).

Следующая группа отличается от остальных тем, что ей нет необходимости опираться на файловую систему. Программы по RAW-восстановлению и реконструкции сначала сканируют диск в RAW-режиме, а затем применяют алгоритмы сборки файлов по сигнатурам и структуре данных. Одними из таких программ являются Photorec (рис. 3), DiskDigger и Stellar Data Recovery.

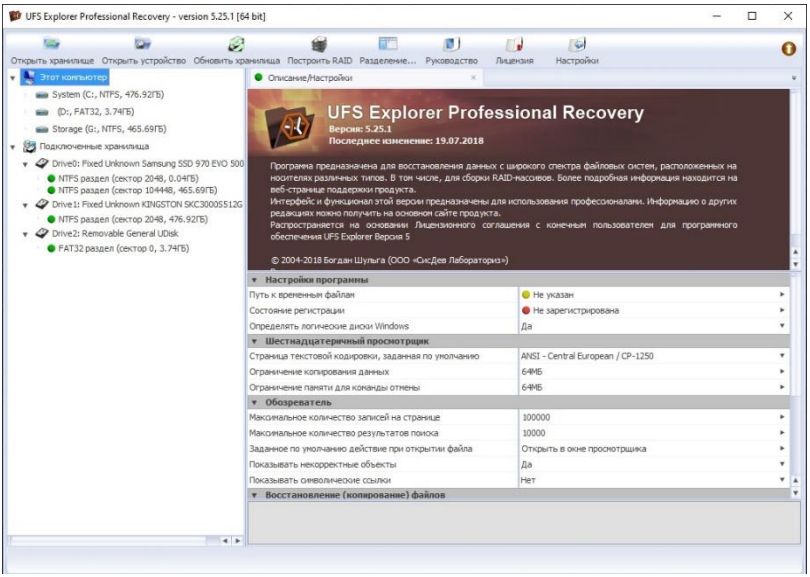


Рис. 1. UFS Explorer Professional Recovery – version 5.25.1

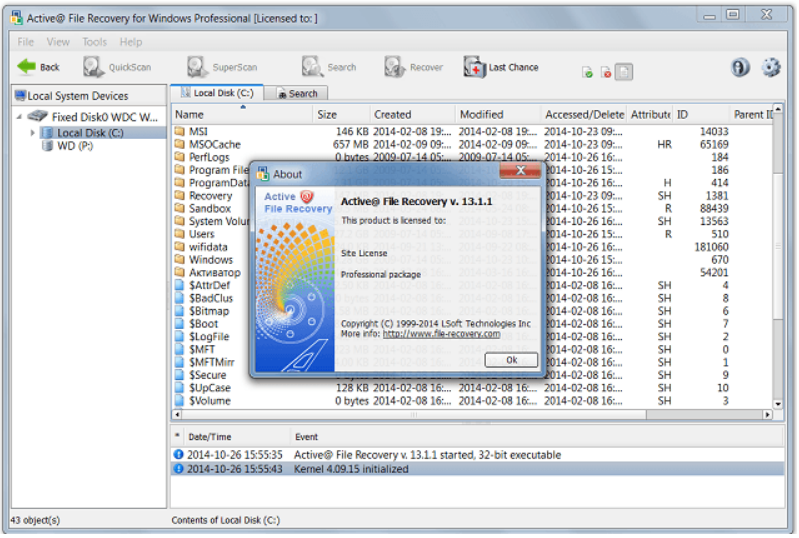


Рис. 2. Active@ File Recovery

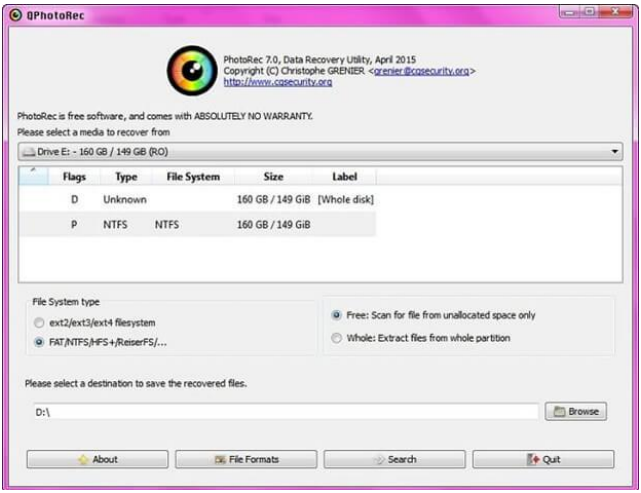


Рис. 3. Photorec

Облачные приложения в процессе своей работы используют локальное сканирование и дальнейшую сверку с облачными базами сигнатур файлов. Особенностью этой группы является то, что её представители подходят для восстановления специфических форматов, таких как базы данных или архивы. Примерами могут служить EaseUS Data Recovery Wizard и Ontrack EasyRecovery (рис. 4).

Рис. 4. Ontrack EasyRecovery

Программы же с аппаратным ускорением используют низкоуровневые методы чтения, а именно через SATA/PCIe напрямую. Подобные программы комбинируют с программными алгоритмами для сборки фрагментов. Например, PC-3000 с аппаратным комплексом и DeepSpar Disk Imager (рис. 5)

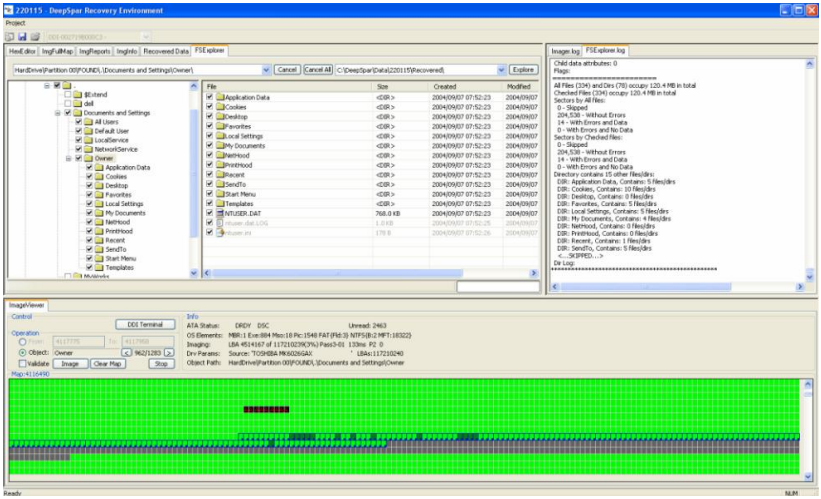


Рис. 5. DeepSpar Disk Imager

Практическая работа

Для проведения дальнейшего эксперимента с целью сравнения эффективности разных программ для восстановления при высокой степени фрагментации мне было необходимо найти несколько подходящих программ и создать фрагментированный диск.

Для более обширного сравнения я решил использовать следующие программы:

1. RS Raid Retrieve (рис. 6) – восстанавливает данные с RAID 0, 1, RAID 4, RAID 5, RAID 6, RAID 0+1, 1+0, 1E, 5EE, 50, 60, JBOD, а также с NAS и DAS устройств в полностью автоматическом режиме, позволяя исправить структуру дисков и вернуть данные, «пропавшие» на проблемном носителей.

2. UFS Explorer Professional Recovery (рис. 1) – набор профессиональных инструментов для восстановления данных, поддерживающих большое число файловых систем, операционных систем и различных типов накопителей: от простейших до сложных составных хранилищ (RAID-массивов различных уровней). Позволяет работать со сложными случаями потери данных на широком спектре файловых систем. Дает возможность изменять исходную информацию на носителе.

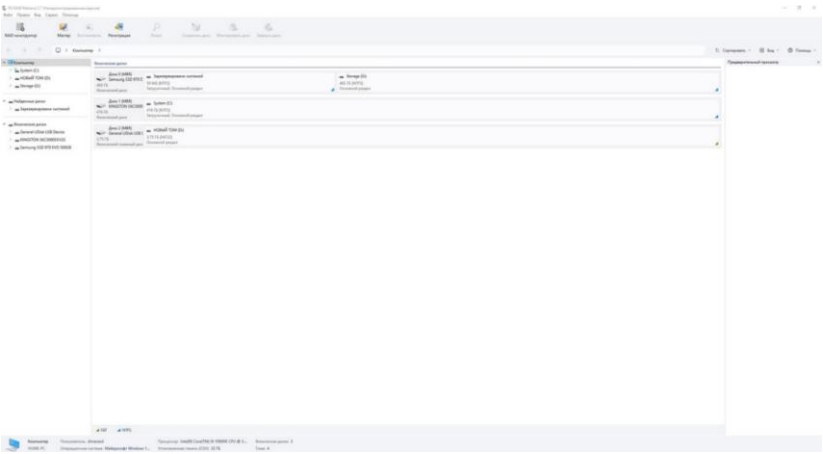


Рис. 6. RS Raid Retrieve

3. R-Studio (рис. 7) – набор утилит для восстановления данных и файлов с жестких дисков, устройств флеш-памяти и других устройств таких, как CD, DVD, дискет, USB дисков, ZIP дисков. Позволяет восстановить файлы удаленные вне Корзины или когда Корзина была очищена, в результате вирусной атакой или сбоя питания компьютера. Работает как на локальных, так и на удаленных компьютерах по сети.

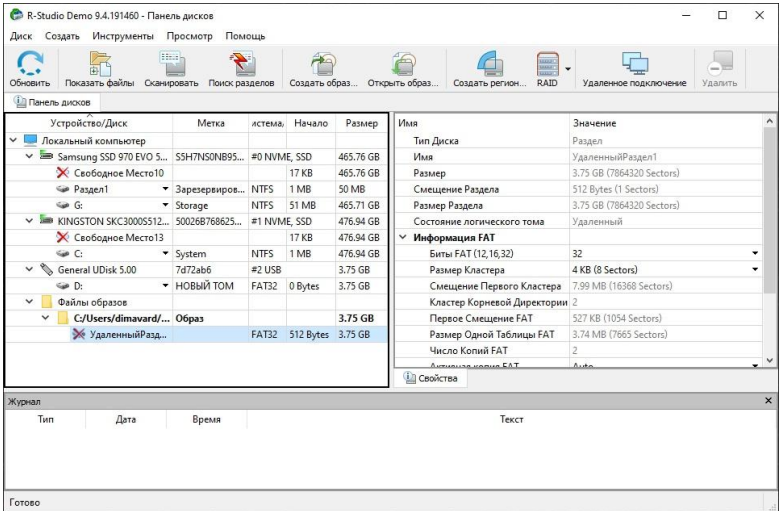


Рис. 7. R-Studio

4. R.saver (рис. 8) – программа для восстановления файлов с различных версий файловых систем NTFS, FAT и ExFAT. Создана на основе полнофункциональных алгоритмов профессиональных версий UFS Explorer.

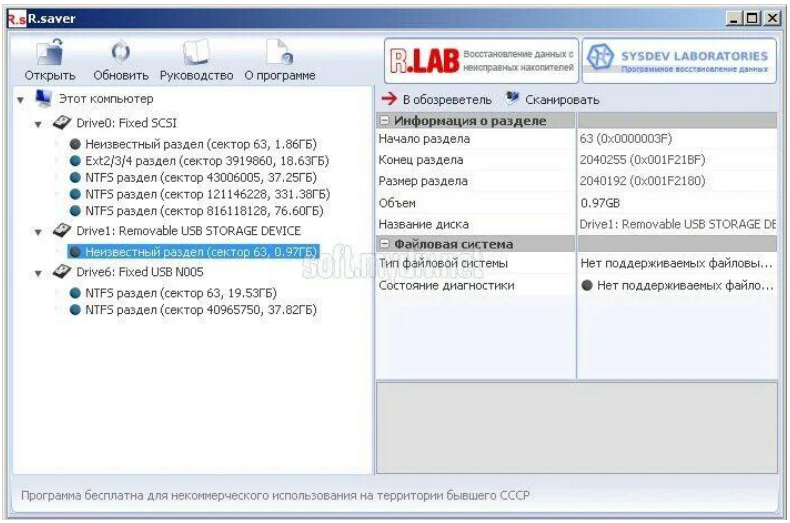


Рис. 8. R.saver

5. DMDE (рис. 9) – программа для редактирования дисков и восстановления данных на жестких и гибких дисках, а также для восстановления логических дисков и разделов физических дисков, для работы с дисками, не доступными для операционной системы.

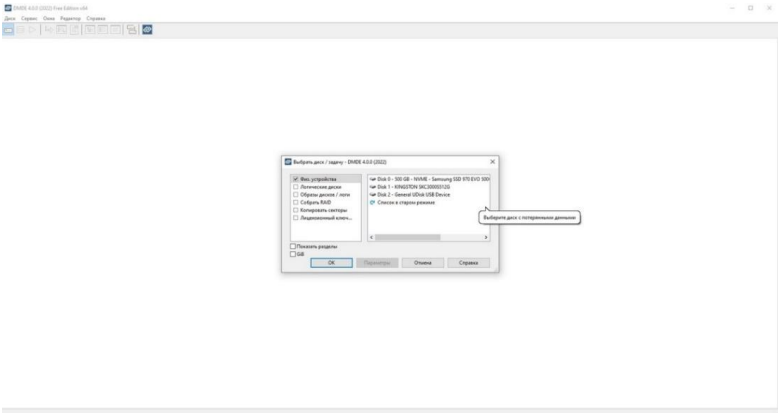


Рис. 9. DMDE

6. Hetman Partition Recovery – программа для восстановления удаленных данных из раздела жесткого диска и других носителей хранения. Утилита поддерживает как функционирующие диски, так и поврежденные логические разделы и восстанавливает данные как с переформатированных дисков, так и с дисков, у которых изменили их файловую систему от FAT на NTFS или наоборот.

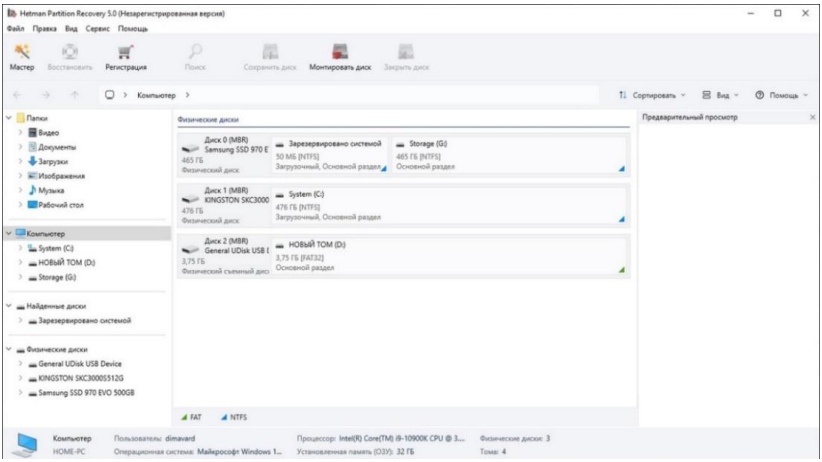


Рис. 10. Hetman Partition Recovery

7. PhotoRec – приложение, с помощью которого пользователи восстанавливают потерянные данные/разделы/загрузочные дисковые области.

Рис. 11. PhotoRec

8. Klennet Carver (рис. 12) – программное обеспечение, выполняющее восстановление конкретных форматов файлов, таких как изображения JPEG, файлы изображений CR2 Canon Raw, Nef Nikon Essential Image Files, MP4 и видеофайлы MOV, видеофайлы AVI, видеофайлы MPEG-2 (также известный как AVCHD или MTS) видеофайлы, также известные как DHAV), созданные Dahua Video-chornders, и конкретные варианты MXF, используемые в SONONAS.

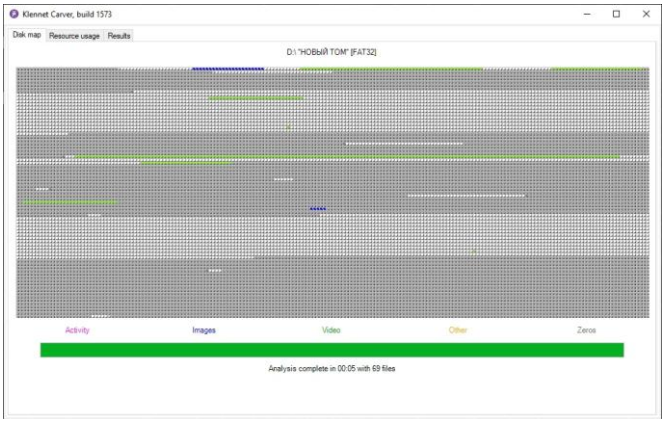


Рис. 12. Klennet Carver

8. Disk Drill (рис. 13) – программа для восстановления удаленных данных для Windows. Без проблем поможет восстановить потерянные документы, видео, музыку или фотографии. Может сканировать и восстановить данные практически с любого носителя информации, будь-то внутренний или внешний жесткий диск, USB флешка, iPod, карта памяти и д.р.

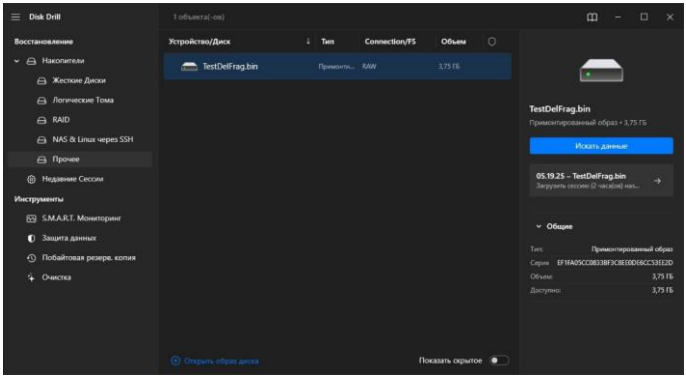


Рис. 13. Disk Drill

Теперь, когда мною были выбраны программы для дальнейшего тестирования, я создал образ фрагментированного носителя (рис. 14).

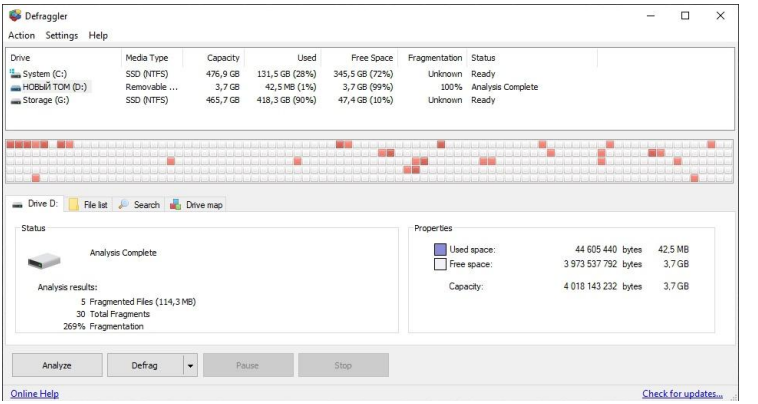


Рис. 14. Фрагментированный носитель

Поскольку вручную создавать подобный носитель довольно долго я использовал специальное программное обеспечение (рис. 15). В состав этого носителя я включил данные различных типов: видео, аудио, текстовые файлы, архив и фото. Это было сделано для дополнительной проверки, поскольку многие программы не поддерживают восстановление всех типов файлов и это было необходимо проверить.

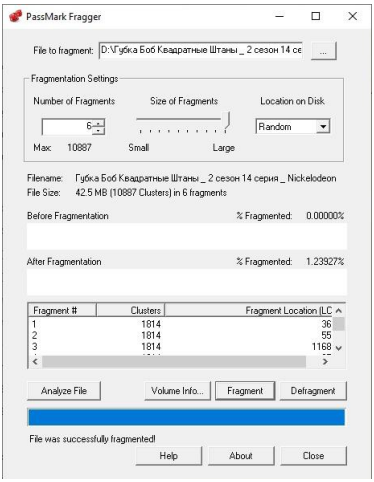


Рис. 15. ПО для фрагментации носителя

Результаты проведенного эксперимента

Проведя восстановление с помощью приведенных выше программ, я могу сделать определенные выводы и представить их в итоговой таблице (рис. 17).

Сокращения, использованные в таблице:

А.Ф. – аудиофайл,

Т.Ф. – текстовый файл,

В.Ф. – видеофайл,

Ф. – фотография,

А. – архив (включает текстовый файл, аудиофайл, видеофайл, фотография)

Программа	Тип данных	Время восстановления	Процент восстановленных данных	Комментарий
RS Raid Retrieve	В.Ф.	3 минуты 32 секунды.	100%	Восстановила видео
	А.Ф.			Первый фрагмент аудио
	Ф., А., Т.Ф.		0%	Ничего не восстановила.
UFS Explorer Professional Recovery	А.Ф., В.Ф., Ф., А., Т.Ф.	-	0%	Ничего не восстановила. Все файлы повреждены после восстановления.
R-Studio	А.Ф., В.Ф., Ф., А., Т.Ф.	-	0%	Бесплатная версия не восстанавливает файлы больше 256КБ. Восстановила текстовый файл повреждённым.
R.saver	Ф., А.Ф., В.Ф.	3 минуты		Фото восстановлен только первый фрагмент. Аудио только первый фрагмент. Видео первый фрагмент.
	А.		75%	В архиве текст полностью цел, видео и фото тоже.
	Т.Ф		0%	Ничего не восстановила.
DMDE	А.	5 сек.	50%	Архив восстановлен, в архиве текстовый и видео восстановлены без повреждений. В архиве повреждены изображение и mp3
	А.Ф., В.Ф., Ф., Т.Ф	-	0%	Остальные файлы повреждены.
Hetman Partition Recovery	В.Ф.	3 сек.	100%	Восстановила видео
	Ф.			Одно фото восстановлено с артефактами
	А.Ф., А., Т.Ф.		0%	Ничего не восстановила.
PhotoRec	А.	4 минуты	75%	В архиве восстановлен текст, фото и видео без артефактов.
	А.Ф., В.Ф.,		100%	Аудио восстановлено. Видео восстановлено.
	Ф., Т.Ф		0%	Ничего не восстановила.
Klennet Carver	А.Ф., В.Ф., Ф., А., Т.Ф.	5 минут	0%	Ничего не восстановила.
Disk Drill	Ф.	13 сек.	30%	Одно фото восстановлено с артефактами
	А.		50%	В архиве восстановлены текст и видео.
	В.Ф., А.Ф.		100%	Восстановлено аудио. Видео восстановлено.
	Т.Ф.		0%	Текстовый повреждён, нечитаем.

Рис. 16. Результаты эксперимента

В итоге результаты получены следующие:

Ни одна из программ не смогла восстановить текстовый файл.

Большая часть программ не справилась со своей прямой задачей и файлы были либо не восстановлены, либо восстановлены с артефактами. Однако следует отметить, что восстановление данных с сильно фрагментированных носителей в принципе очень сложная задача и полученные в итоге результаты не вызывают особого удивления.

Однако среди протестированных программ я бы хотел выделить одну, которая дала наилучший результат. Программа PhotoRec смогла восстановить архив, аудио- и видеофайлы, но не смогла восстановить текстовый файл и, что иронично, фотографию.

Заключение

Поставленные мною задачи и цель были выполнены. Я провел анализ эффективности различных программ по восстановлению данных с сильно фрагментированных дисков.

К сожалению, некоторые программы не удалось протестировать из-за высокой стоимости лицензий. Однако эту проблему можно было бы решить, продолжив работу в данном направлении.

Также, углубившись в изучение темы восстановления данных, я могу сказать, что восстановление данных именно с сильно фрагментированных дисков до сих пор не имеет идеального решения и даже новейшие программы не могут дать стопроцентной гарантии, что любые данные могут быть восстановлены. К такому выводу я пришёл в ходе проведения эксперимента и анализа полученных данных. Среди протестированных мною программ не было ни одной которая восстановила все файлы, некоторые программы восстановили данные с артефактами некоторые – частично, а некоторые не восстановили ни одного. Из этого можно сделать вывод, что тема моей работы действительно актуальна в современных реалиях, когда вопрос сохранения и восстановления данных стоит как никогда остро. Поэтому стоит продолжить работать в данном направлении и результаты, которые мне удалось экспериментально получить, очень пригодятся в будущих исследованиях.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Фрагментация диска и её влияние на целостность данных URL: https://recovery-software.ru/blog/disk-fragmentation-and-its-effects-on-data-integrity.html (дата обращения: 20.03.2025).
2. Файловая система ReFS изнутри. – URL: https://rlab.ru/doc/refs_file_system.html (дата обращения 01.04.2025).

3. *Кошечкин А.А., Андрощенко В.С., Замятин А.В.* Новый метод восстановления пропущенных значений в наборе данных на примере иммуносигнатур // Современные технологии в медицине. – 2019. – Т. 11, № 2. – С. 19-24. – DOI: 10.17691/stm2019.11.2.03.
4. *Шалягов А.М.* Метод восстановления фрагментированных файлов при утрате сведений о фрагментации // Крифференциал. 2012. С. 176. ISSN 0376-8073.
5. *Касперски К., Холмогоров В.А., Кирилова К.С.* Восстановление данных. Практическое руководство. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2021. – 288 с.: ил. – ISBN 978-5-9775-6681-0.
6. *Сенкевич Г.Е.* Искусство восстановления данных. – СПб.: БХВ-Петербург, 2011. – 304 с.: ил. – (Аппаратные средства). – ISBN 978-5-9775-0618-2.
7. Методы восстановления после форматирования. – URL: https://digitalsquare.ru/ctati/vosstanovlenie-dannyh-s-zhestkogo-diska-posle-formatirovaniya-polnoe-rukovodstvo.html (дата обращения 01.04.2025).
8. *Карлов И.А., Конкур В.Д.* Гибридный метод восстановления пропущенных данных с адаптивным управлением на основе нечеткой логики и нейронных сетей // Информационные технологии. – С. 222.

УДК 00.1082

В.В. Вилков, Е.С. Басан

Южный федеральный университет, Россия, г. Таганрог

АНАЛИЗ АТАК НА КОНТЕЙНЕРИЗИРОВАННЫЕ WEB-ПРИЛОЖЕНИЯ: ВЕКТОР УГРОЗ И МЕТОДЫ ЗАЩИТЫ

Контейнеризация получила широкое распространение в веб-разработке благодаря своей гибкости, масштабируемости и простоте развертывания. Особенно это актуально для front-end-приложений, где используется множество библиотек и инструментов сборки. Однако стремительный рост популярности контейнерных технологий привёл к появлению новых векторов атак. В статье рассматриваются принципы работы контейнеров, типичные уязвимости и векторы атак, характерные для контейнеризированных front-end-приложений, а также методы защиты.

Ключевые слова: *контейнеры, front-end, безопасность, supply chain атаки, криптомайнинг, Docker, CI/CD.*

Containerization has become widespread in web development due to its flexibility, scalability, and ease of deployment. This is especially true for frontend applications that rely on various libraries and build tools. However, the rapid adoption of container technologies has introduced new attack vectors. This article explores the principles of containers, typical vulnerabilities and attack surfaces specific to containerized frontend applications, and outlines protection methods.

Keywords: *containers, front-end, security, supply chain attacks, cryptomining, Docker, CI/CD.*

Введение

Современная веб-разработка требует высокой скорости выпуска новых версий программных продуктов, а также стабильности и повторяемости среды исполнения. В этих условиях технологии контейнеризации, такие как Docker, стали стандартом индустрии. С их помощью можно упаковать приложение и все его зависимости в единый образ, легко распространяемый и запускаемый в любом окружении. Особенно это ценно при работе с front-end-приложениями, где важно обеспечить единообразие сборки (build), стабильность окружения Node.js, а также консистентность версий библиотек [1].

Однако вместе с удобством и эффективностью контейнеризация принесла и новые угрозы. Начиная от внедрения вредоносных зависимостей (supply chain атаки), заканчивая эксплойтами, использующими ошибки в конфигурации контейнера, злоумышленники всё чаще находят способы компрометации как отдельных контейнеров, так и всей инфраструктуры в

целом [2]. Кроме того, появление специализированной матрицы MITRE ATT&CK for Containers позволило систематизировать и структурировать эти угрозы [3].

Данная статья посвящена анализу рисков, связанных с контейнеризированными front-end-приложениями, а также методам их минимизации.

Технологии контейнеризации во front-end

Контейнеризация: понятие и цели. Контейнеризация – это технология, позволяющая упаковать приложение со всеми зависимостями в изолированную среду, которую можно запускать на любой машине с установленной контейнерной платформой (чаще всего Docker). Контейнеры используют ядро хостовой операционной системы, но обеспечивают логическую изоляцию, что делает их более лёгкими по сравнению с виртуальными машинами [1].

Во front-end-разработке контейнеризация используется для:

- стандартизации процесса сборки (webpack, Vite, Rollup и пр.),
- обеспечения согласованности версий Node.js, npm, yarn,
- запуска тестов (Jest, Cypress, Playwright) в предсказуемом окружении,
- упрощения CI/CD пайплайнов.

Основные инструменты

- **Docker** – наиболее распространённая контейнерная платформа. Позволяет создавать образы (images), запускать контейнеры и управлять ими [1].
- **Docker Compose** – инструмент для описания мультиконтейнерных приложений, например, frontend, backend и база данных, разбитые по отдельным контейнерам.
- **Kubernetes (k8s)** – платформа оркестрации контейнеров, используемая в масштабируемых production-средах [4].
- **Podman, Buildah** – альтернативы Docker с фокусом на безопасность (не требуют root-доступа).
- **CI/CD платформы** (GitHub Actions, GitLab CI, Jenkins) активно интегрируют сборку и развертывание контейнеризированных front-end приложений [5].

Пример: контейнеризация React-приложения

Этап сборки – использует Node.js-образ для установки зависимостей и запуска сборки (npm run build);

Этап сервера – переносит готовый билд в лёгкий образ, например nginx:alpine, для быстрой отдачи статики.

```
# Этап 1
FROM node:20 AS builder
```

```
WORKDIR /app
COPY . .
RUN npm ci && npm run build
# Этап 2
FROM nginx:alpine
COPY --from=builder /app/dist /usr/share/nginx/html
```

Данный подход позволяет минимизировать итоговый образ, уменьшить поверхность атаки и ускорить деплой.

Сравнение CI/CD платформ: GitHub Actions, GitLab CI и Jenkins

GitHub Actions

- **Описание:** Инструмент автоматизации рабочих процессов, интегрированный с GitHub.
- **Ключевые особенности:**
  - Тесная интеграция с репозиториями GitHub.
  - Маркетплейс предустановленных действий.
  - Поддержка пользовательских действий.
  - Автоматизация pull request.
- **Преимущества:**
  - Простота использования и настройки.
  - Широкий выбор предустановленных действий.
- **Недостатки:**
  - Ограничен репозиториями GitHub.
  - Меньше возможностей для кастомизации по сравнению с Jenkins.

GitLab CI

- **Описание:** Инструмент CI/CD, интегрированный в платформу GitLab.
- **Ключевые особенности:**
  - Интеграция с репозиториями GitLab.
  - Конфигурация на основе YAML.
  - Гибкая система раннеров.
  - Встроенные функции безопасности.
- **Преимущества:**
  - Удобство использования в экосистеме GitLab.
  - Хорошая документация и поддержка.
- **Недостатки:**
  - Ограничен репозиториями GitLab.
  - Некоторые функции требуют платной подписки.

Jenkins

- **Описание:** Открытый сервер автоматизации с обширной экосистемой плагинов.
- **Ключевые особенности:**
  - Поддержка конвейеров и распределенных сборок.
  - Большая библиотека плагинов.
  - Активное сообщество.
- **Преимущества:**
  - Высокая степень кастомизации.
  - Открытый исходный код.
- **Недостатки:**
  - Сложность в настройке и обучении.
  - Возможные проблемы совместимости плагинов.

Заключение

- **GitHub Actions** подходит для пользователей GitHub, ищущих простоту и удобство.
- **GitLab CI** идеален для тех, кто использует GitLab и ценит интеграцию и безопасность.
- **Jenkins** предлагает максимальную гибкость и кастомизацию для сложных проектов.

Типовые угрозы и атаки на контейнеризированные front-end-приложения

Современные атаки на контейнеризированную среду front-end-разработки охватывают как инфраструктурный уровень, так и уровень зависимостей. Особенно уязвимыми оказываются проекты, активно использующие Node.js, Docker и автоматизированные pipeline [6].

Наиболее распространённые угрозы включают:

1. Атаки на цепочку поставок (supply chain attacks)

Атаки на цепочку поставок предполагают внедрение вредоносного кода в зависимости, скрипты сборки или контейнерные образы, используемые в проекте. Наиболее уязвимы front-end-приложения, так как они активно используют npm-пакеты, в том числе от неизвестных или малоизвестных разработчиков. Атаки данного типа трудно обнаружить, потому что они маскируются под легитимные обновления и распространяются автоматически в CI/CD (continuous integration, Continuous Delivery расшифровываются как непрерывная интеграция и доставка) [6, 7].

- злоумышленник находит малообслуживаемый npm (англ. Node Package Manager) пакет или покупает доступ к нему у владельца;

- вносит небольшое «невидимое» изменение в код, например, добавляет postinstall скрипт для скачивания и запуска вредоносного файла;
- публикует обновление в npm под тем же именем и с повышенным минорным номером (например, 1.0.3 → 1.0.4);
- ничего не подозревающие разработчики автоматически получают этот пакет при npm install;
- вредоносный код исполняется на этапе сборки, похищая токены, SSH-ключи или передавая переменные окружения на внешний сервер;
- дальнейшее распространение может происходить через пайплайны CI/CD и заражённые образы.

2. Внедрение криптомайнеров (crypto-mining)

Криптомайнинг в контейнерах – это использование чужих вычислительных ресурсов для майнинга криптовалют. Такая атака остаётся незаметной, особенно если контейнер не отслеживает потребление CPU/GPU, а внутренние процессы не логируются.

- атакующий сканирует интернет на наличие открытых Docker API (порты 2375/2376);
- находит неправильно настроенный хост и отправляет через API команду docker run с образом, содержащим майнер Monero;
- запускается фоновый процесс, который скрытно использует CPU и память хоста;
- в некоторых случаях контейнер маскируется под популярные образы, такие как **nginx** или **alpine**, чтобы избежать подозрений. Это делается для того, чтобы администраторы системы или инструменты мониторинга не распознали вредоносную активность. Маскировка под **nginx** может сделать контейнер менее подозрительным, так как он будет выглядеть как обычный веб-сервер. Администраторы могут не заметить повышенного использования ресурсов, если не проверяют детально, какие процессы запущены внутри контейнера. **Alpine**, как минималистичный образ Linux, часто используется в качестве базового образа для создания других контейнеров, что делает его менее заметным. Таким образом, маскировка помогает скрыть вредоносную активность, делая её менее заметной для стандартных методов мониторинга.
- результаты майнинга отправляются на криптокошелёк злоумышленника, чаще всего через Tor или сокс-прокси.

3. Компрометация CI/CD пайплайнов

При атаке на пайплайн CI/CD злоумышленник встраивает вредоносный код или команды в конфигурацию сборки. Это позволяет запустить произвольный код на машине сборки, часто с правами root [8].

- злоумышленник получает доступ к репозиторию (через утечку токена или прав редактора);
- открывает gitlab-ci.yml или .github/workflows/main.yml и добавляет stage с вредоносной командой (curl, wget, bash);
- при следующем пуше проект автоматически собирается и выполняет заражённую задачу;
- результатом может быть утечка артефактов, токенов, копирование образа, или добавление бэкдора в собранный контейнер;
- если сборка пушит контейнер в registry – вредоносный образ попадает в production.

4. Эксплуатация уязвимостей в контейнерных образах

Устаревшие версии библиотек или операционных компонентов внутри контейнера могут содержать известные уязвимости. Если такие образы попадают в проект, который эксплуатируют пользователи, ими можно воспользоваться для удалённого выполнения кода [7].

- злоумышленник сканирует публичные реестры (например, Docker Hub) на наличие популярных образов без обновлений;
- проверяет версию glibc, OpenSSL или node.js в слое контейнера;
- если есть известный CVE — подготавливает эксплойт под конкретную версию;
- при получении доступа (через запрос, curl, upload) запускает эксплойт прямо внутри приложения;
- в результате может получить shell, права root, или исполнение кода в контейнере.

5. Утечка чувствительных данных из переменных окружения

Секреты и токены, хранящиеся в .env, могут попасть в журнал, debug-страницы, или быть извлечены из контейнера в случае атаки [8].

- злоумышленник сканирует публичные репозитории на наличие .env файлов или .gitignore, в которых они забыты;
- может использовать SSRF или LFI в приложении, чтобы запросить /proc/self/environ;
- если доступен shell внутри контейнера (например, через exec), запускает env и копирует переменные;
- находит секреты: AWS, JWT, токены GitHub, SMTP и т.д.;
- использует эти токены для доступа к инфраструктуре или API сторонних сервисов.

6. Эскалация привилегий внутри контейнеров

Если контейнер запущен с root-доступом или с флагом --privileged, злоумышленник может выйти за пределы контейнера [8].

- злоумышленник находит уязвимое приложение внутри контейнера (например, express с RCE);

- выполняет команду внутри контейнера и видит, что процесс работает от root;
- монтирует системные директории хоста (например, /proc, /var, /etc), если доступны;
- может изменить файлы на хосте, сгенерировать SSH-ключ и вписать его в .ssh/authorized_keys;
- получает полный контроль над хостом и другими контейнерами пример диаграммы представлен на рис. 1.

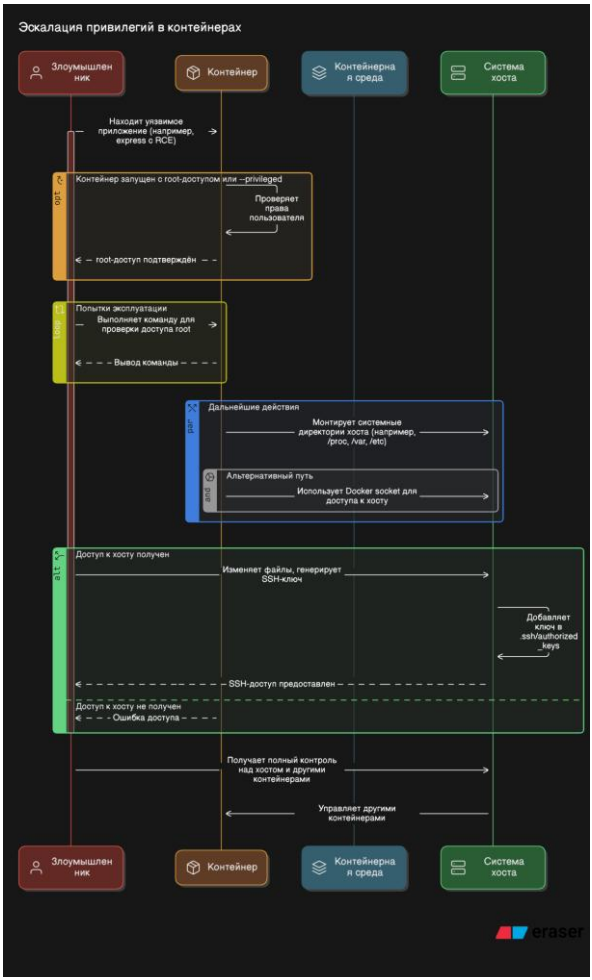


Рис. 1. Диаграмма получения привилегий в контейнере

7. Атаки через публичный Docker API

Некоторые серверы публикуют Docker API на внешний интерфейс без аутентификации, что позволяет удалённо управлять контейнерами.

- злоумышленник сканирует порты 2375 и 2376 на наличие открытых Docker API;
- с помощью curl или Postman отправляет команду POST /containers/create [9, 10];
- разворачивает свой образ из публичного реестра, часто с вредоносным ПО или бэкдором;
- запускает контейнер, подключает volume, или копирует конфигурации других контейнеров;
- может использовать узел как часть ботнета, прокси или шифровальщика.

Краткое описание методов защиты от каждой атаки:

1. Атаки на цепочку поставок:

- **Защита**: Использование подписанных и проверенных образов (Docker Content Trust, Notary v2), регулярное сканирование уязвимостей контейнеров (Trivy, Clair, Anchore, Snyk), контроль использования сторонних зависимостей (npm audit, Snyk, OWASP Dependency-Check).

2. Внедрение криптомайнеров:

- **Защита**: Мониторинг поведения контейнеров в реальном времени (Falco, Sysdig, eBPF-решения), ограничение привилегий контейнеров (отключение запуска от имени root, --cap-drop, SELinux, AppArmor).

3. Компрометация CI/CD пайплайнов:

- **Защита**: Защита CI/CD-пайплайнов и секретов (менеджеры секретов, контроль доступа), использование подписанных и проверенных образов.

4. Эксплуатация уязвимостей в контейнерных образах:

- **Защита**: Регулярное сканирование уязвимостей контейнеров, использование подписанных и проверенных образов.

5. Утечка чувствительных данных из переменных окружения:

- **Защита**: Защита CI/CD-пайплайнов и секретов, мониторинг поведения контейнеров в реальном времени.

6. Эскалация привилегий внутри контейнеров:

- **Защита**: Ограничение привилегий контейнеров, изоляция среды исполнения (seccomp, AppArmor, SELinux).

7. Атаки через публичный Docker API:

- **Защита**: Ограничение привилегий контейнеров, изоляция среды исполнения, мониторинг поведения контейнеров в реальном времени.

Наиболее эффективные методы защиты включают:

1. Использование подписанных и проверенных образов (image signing)

Применение механизмов подписи образов, таких как Docker Content Trust (DCT) или Notary v2, позволяет гарантировать целостность и подлинность контейнера. Это предотвращает подмену образа в реестре, даже если доступ к нему будет скомпрометирован. Использование только доверенных и проверенных образов (например, из официальных репозиториев Docker Hub, GitHub Container Registry) снижает вероятность использования заражённого базового слоя [8, 11].

2. Регулярное сканирование уязвимостей контейнеров (vulnerability scanning)

Сканеры безопасности, такие как Trivy, Clair, Anchore или Snyk, позволяют автоматически анализировать контейнерные образы на наличие известных уязвимостей (CVE). Интеграция таких сканеров в CI/CD пайплайн позволяет блокировать сборку или деплой образов, содержащих критические проблемы. Это особенно актуально для front-end-проектов, зависящих от множества npm-библиотек, среди которых регулярно появляются уязвимые версии.

3. Ограничение привилегий контейнеров (least privilege)

Контейнеры по умолчанию могут запускаться с привилегиями, превышающими необходимый минимум. Отключение запуска от имени root, использование флага --cap-drop, настройка SELinux или AppArmor профилей позволяют снизить потенциальный ущерб в случае успешной атаки. Принцип наименьших привилегий должен применяться и к сервисным аккаунтам в кластере, особенно при использовании Kubernetes.

4. Изоляция среды исполнения (например, через seccomp, AppArmor)

Фреймворки безопасности ядра Linux, такие как seccomp, AppArmor и SELinux, позволяют ограничить системные вызовы, доступные контейнеру, и задать допустимые действия в пространстве пользователя и файловой системе. Это повышает устойчивость среды к атакам, использующим эксплойты нулевого дня или уязвимости ядра [11].

5. Защита CI/CD-пайплайнов и секретов

Следует избегать хранения секретов (токенов, паролей) в виде переменных окружения или в открытом YAML. Необходимо использовать менеджеры секретов (например, HashiCorp Vault, AWS Secrets Manager) и настраивать контроль доступа к этапам пайплайна. Для каждого этапа должны применяться отдельные учётные данные с минимально необходимыми правами [8, 12].

6. Мониторинг поведения контейнеров в реальном времени

Инструменты вроде Falco, Sysdig или eBPF-решений позволяют отслеживать подозрительную активность: создание неизвестных процессов, доступ к конфиденциальным файлам, обращения к сети и системным вызовам. Это помогает выявить отклонения от типичного поведения и оперативно реагировать на инциденты [11].

7. Контроль использования сторонних зависимостей

Для front-end-проектов важно регулярно проводить аудит зависимостей с помощью инструментов вроде npm audit, Snyk или OWASP Dependency-Check. Также стоит ограничивать автоматическое обновление зависимостей и использовать механизмы блокировки версий (package-lock.json, yarn.lock), чтобы избежать внедрения вредоносного кода через случайные обновления [8, 14].

Заключение

Контейнеризация front-end-приложений представляет собой не только мощный инструмент для стандартизации и ускорения процессов разработки, но и новую плоскость угроз, требующую системного подхода к безопасности. Учитывая активное использование сторонних зависимостей, автоматизированных сборок и публичных реестров, даже небольшие ошибки конфигурации или упущения в контроле цепочки поставок могут привести к серьёзным последствиям: компрометации инфраструктуры, утечке данных и финансовым потерям [12].

Атаки на контейнеры становятся всё более изощрёнными, охватывая как уязвимости в образах, так и в пайплайнах CI/CD. Наиболее опасными остаются supply chain-атаки, а также внедрение криптомайнеров и использование привилегий контейнера для выхода за его пределы. При этом реальная угроза нередко остаётся незамеченной из-за отсутствия мониторинга и слабых политик безопасности [8, 11].

Для эффективной защиты необходимо внедрение комплексных мер: подписывание и контроль целостности образов, постоянное сканирование уязвимостей, ограничение прав контейнеров, мониторинг в реальном времени, а также защита конфигурации CI/CD. Не менее важно – формирование культуры безопасной разработки, где безопасность рассматривается как неотъемлемая часть всего жизненного цикла приложения.

Применение описанных в статье практик позволяет значительно повысить устойчивость front-end-инфраструктуры к современным типам атак и обеспечить надёжную защиту не только кода, но и доверия пользователей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Документация Docker [Электронный ресурс] // docs.docker.com: [сайт]. – URL: https://docs.docker.com/ (дата обращения: 11.04.2025).
2. Фишки VS Угрозы технологии контейнеризации [Электронный ресурс] // habr.com: [сайт]. – URL: https://habr.com/ru/companies/trendmicro/articles/439986/ (дата обращения: 11.04.2025).
3. Документация AttackMitre [Электронный ресурс] // attack.mitre.org: [сайт]. – URL: https://attack.mitre.org/ (дата обращения: 11.04.2025).
4. Документация Kubernetes [Электронный ресурс] // kubernetes.io: [сайт]. – URL: https://kubernetes.io/docs/home/ (дата обращения: 11.04.2025).
5. Документация GitLab CI/CD: Использование Docker [Электронный ресурс] // docs.gitlab.com: [сайт]. – URL: https://docs.gitlab.com/ci/docker/using_docker_build/ (дата обращения: 11.04.2025).
6. Kaspersky. Защита сред контейнеризации от А до Я [Электронный ресурс] // kaspersky.ru: [сайт]. – URL: https://www.kaspersky.ru/blog/container-security/36087/ (дата обращения: 11.04.2025).
7. OWASP. OWASP Top 10 - 2017 [Электронный ресурс] // owasp.org: [сайт]. – URL: https://owasp.org/www-project-top-ten/ (дата обращения: 11.04.2025).
8. Обеспечение безопасности Frontend приложений [Электронный ресурс] // habr.com: [сайт]. – URL: https://habr.com/ru/articles/736866/ (дата обращения: 11.04.2025).
9. Curl / [Электронный ресурс] // curl.se: [сайт]. – URL: https://curl.se/ (дата обращения: 11.04.2025).
10. Postman [Электронный ресурс] // postman.com: [сайт]. – URL: https://www.postman.com/ (дата обращения: 11.04.2025).
11. Безопасность контейнеризированных приложений в рамках DevSecOps [Электронный ресурс] // habr.com: [сайт]. – URL: https://habr.com/ru/companies/ swordfish_security/articles/731746/ (дата обращения: 11.04.2025).
12. Обзор способов предотвращения атак при разработке и эксплуатации контейнеризированных приложений [Электронный ресурс] // na-journal.ru: [сайт]. – URL: https://na-journal.ru/6-2024-informacionnye-tekhnologii/13732-obzor-sposobov-predotvrashcheniya-atak-pri-razrabotke-i-ekspluatacii-konteinerizirovannyh-prilojenii (дата обращения: 11.04.2025).
13. Docker Security: Пособие для самостоятельного изучения [Электронный ресурс] // hackmd.io: [сайт]. – URL: https://hackmd.io/@noble5836/SyohEHI-o (дата обращения: 11.04.2025).
14. OWASP Dependency-Check [Электронный ресурс] // owasp.org: [сайт]. – URL: https://owasp.org/www-project-dependency-check/ (дата обращения: 11.04.2025).

УДК 004.056.5

В.И. Вышегородцева

Южный федеральный университет, Россия, г. Таганрог

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ КИБЕРРАЗВЕДКИ В РАССЛЕДОВАНИИ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ: ИННОВАЦИОННЫЕ ПОДХОДЫ И ПЕРСПЕКТИВЫ

В статье рассмотрены современные технологии киберразведки (Cyber Threat Intelligence, CTI) и их прикладное использование при расследовании инцидентов информационной безопасности. Приведен обзор актуальных методов и инструментов киберразведки, включая жизненный цикл threat intelligence и популярные базы знаний (например, MITRE ATT&CK). Показано, как разведданные об актуальных киберугрозах интегрируются в процесс реагирования на инциденты: от обнаружения и анализа вредоносной активности до атрибуции атак и выработки мер противодействия. Особое внимание уделено инновационным подходам – применению методов искусственного интеллекта и машинного обучения для автоматизации сбора и анализа разведданных, а также оркестрации расследований. Рассматриваются международный и отечественный опыт внедрения платформ киберразведки и обмена индикаторами компрометации. Обсуждаются перспективы развития отрасли: усиление роли автоматизации и ИИ, расширение сотрудничества и обмена данными между организациями, а также решение текущих проблем (качество данных, стандартизация, этические аспекты).

Ключевые слова: *киберразведка; расследование инцидентов; информационная безопасность; threat intelligence; машинное обучение; автоматизация; MITRE ATT&CK; индикаторы компрометации.*

The article examines modern cyber threat intelligence (CTI) technologies and their practical use in computer security incident investigations. It provides an overview of current threat intelligence methods and tools, including the intelligence lifecycle and popular knowledge bases (e.g., MITRE ATT&CK). The paper demonstrates how threat intelligence data on current cyber threats is integrated into the incident response process – from detecting and analyzing malicious activity to attributing attacks and devising countermeasures. Special attention is given to innovative approaches such as the application of artificial intelligence and machine learning to automate the collection and analysis of threat data, as well as orchestration of investigations. The article reviews international and domestic experiences in implementing threat intelligence platforms and sharing indicators of compromise. Future perspectives of the field are discussed, including the growing role of automation and AI, expanded collaboration and data exchange between organizations, and addressing current challenges (data quality, standardization, ethical aspects). The paper is focused on applied aspects and is supported by references to recent research and cases, meeting the requirements of the "Perspective – 2025" conference.

Keywords: *Cyber threat intelligence; incident investigation; information security; threat intelligence; machine learning; automation; MITRE ATT&CK; indicators of compromise.*

Введение

Рост количества и сложности кибератак в последние годы повышает требования к расследованию инцидентов информационной безопасности. Традиционные методы защиты уже недостаточны – требуется проактивный подход, одним из ключевых элементов которого стала киберразведка. Под киберразведкой понимается сбор и анализ информации о актуальных киберугрозах, злоумышленниках, их тактиках, техниках и процедурах (Tactics, Techniques and Procedures, TTP), а также об индикаторах компрометации (Indicators of Compromise, IOC) [1]. Эти разведданные позволяют лучше понимать природу атак и заблаговременно принимать меры для снижения их влияния. Согласно исследованиям, киберразведка набирает популярность в организациях по всему миру – почти половина крупных предприятий уже сформировали специальные CTI-команды, а еще ~14% имеют хотя бы одного выделенного специалиста по киберразведке.

Одновременно с этим растёт и объем информации об инцидентах: компании и центры мониторинга фиксируют всё больше атак, новых уязвимостей и вредоносных кампаний. Без автоматизации обмена данными специалисты SOC быстро перегружаются, что снижает эффективность расследований [2]. В этих условиях интеграция технологий киберразведки в процесс реагирования на инциденты стала насущной необходимостью.

Цель данной работы – проанализировать современные технологии threat intelligence и продемонстрировать их применение при расследовании компьютерных инцидентов, а также обсудить инновационные методы и перспективы развития данного направления. В разделе 2 представлен обзор концепций и инструментов киберразведки, включая жизненный цикл обработки разведданных и распространенные базы знаний об атаках. В разделе 3 рассматривается практическое использование киберразведки на этапах расследования инцидентов информационной безопасности. Раздел 4 посвящен передовым подходам – внедрению машинного обучения и автоматизации для повышения эффективности расследований. В разделе 5 обобщается международный и отечественный опыт применения CTI, и в разделе 6 обсуждаются перспективы и дальнейшее развитие технологий киберразведки.

Современные технологии киберразведки

Понятие и жизненный цикл CTI. Термин “Threat Intelligence” (киберразведка) получил распространение около 15 лет назад и сейчас прочно вошел в лексикон специалистов по безопасности. Киберразведка включает процесс сбора, обработки, анализа и распространения информации о киберугрозах. Этот процесс часто представляют в виде цикла разведки угроз (Threat Intelligence Lifecycle), состоящего из последовательных этапов: планирование и определение требований; сбор данных из различных источни-

ков; обработка и фильтрация полученной информации; аналитический анализ и производство разведданных; распространение полученной информации заинтересованным сторонам; и получение обратной связи (корректировка требований) [3].

На этапе сбора данных используются разнообразные источники. Они делятся на открытые (OSINT – Open Source INTelligence: например, данные из публичных отчетов, новостных сайтов, социальных сетей, форумов даркнета), коммерческие или закрытые (подписки на TI-фиды от специализированных компаний, данные от отраслевых центров обмена информацией – ISAC), а также внутренние источники самой организации (логи системы, результаты собственных расследований). Обработка включает фильтрацию шума, приведение данных к стандартному формату и обогащение – например, привязку IP-адресов к доменам, хешей файлов к известным семействам malware и т.п. Анализ – ключевой этап, на котором аналитики (или автоматизированные системы) исследуют полученные сведения, выявляют связи между событиями, построением хронологии атаки, атрибутируют угрозу конкретным группам или кампаниям. Результатом анализа является разведывательный отчет или сигнатуры/правила для защитных систем – то есть продукт разведки, предназначенный для практического применения. Далее следует распространение разведданных – передача их тем, кто отвечает за принятие мер защиты (SOC, группа реагирования на инциденты, руководство). Важным элементом является обратная связь: насколько полученная разведка оказалась полезной, какие новые требования появляются к информации – это позволяет скорректировать последующие сбор и анализ.

Инструменты и базы знаний. Для поддержки процесса кибербразведки разработан ряд технологий и платформ. Важную роль играют стандарты обмена информацией. Наиболее широко применяется формат STIX (Structured Threat Information eXpression) для структурированного представления сведений о киберугрозах и формат TAXII (Trusted Automated Exchange of Indicator Information) для транспортировки этих данных между системами [4]. С их помощью организации обмениваются индикаторами компрометации и данными об атаках в автоматизированном режиме. Также существуют платформы обмена разведданными – например, открытая платформа MISP (Malware Information Sharing Platform), позволяющая сообществам (союзы CERT/CSIRT, отраслевые ISAC и пр.) совместно наполнять базу IOC и тактик атак и получать обновления в реальном времени. Для хранения и систематизации знаний о тактике и техниках противника создана база MITRE ATT&CK, впервые представленная в 2013 году как эксперимент по классификации действий злоумышленников [5].

Сейчас MITRE ATT&CK стала де-факто стандартом: она представляет матрицу из тактик и конкретных техник, используемых группами APT и киберпреступниками, и широко используется для сопоставления обнару-

женных активностей с известными шаблонами атаки. Другой пример – модель Diamond Model, описывающая каждое кибер-воздействие четырьмя основными гранями: злоумышленник (adversary), возможности (capability, например используемый эксплойт или malware), инфраструктура (infrastructure – средства связи и доставки атаки) и жертва (victim) . Такая модель помогает аналитикам выстроить взаимосвязи между элементами инцидента и понять картину в целом.

Современный рынок предлагает и коммерческие платформы киберразведки (Threat Intelligence Platform, TIP) – программные системы, интегрирующие сбор данных из множества источников, их обработку (в том числе обогащение за счет кросс-проверки по разным базам), хранение и поиск по базе знаний, а также автоматическое распространение важных обновлений в связанные системы безопасности (SIEM, системы корреляции событий, средства предотвращения атак). Использование таких платформ позволяет значительно ускорить получение релевантных предупреждений о новых угрозах и снизить нагрузку на аналитиков. Как отмечают исследователи, без применения автоматизированных TI-платформ растущий поток сырых данных о инцидентах просто “захлестывает” специалистов, требуя все больше ручной работы [2]. Поэтому организации все чаще внедряют централизованные системы управления данными киберразведки.

Применение киберразведки в расследовании инцидентов

Роль CTI на этапах расследования. Киберразведка существенно обогащает каждый этап цикла реагирования на инцидент (Detect – Respond – Recover). На стадии обнаружения (детектирования) угроз разведданные позволяют настроить более точные индикаторы и корреляционные правила. Например, получив обновления о новых IOC (вредоносные IP-адреса, домены управления, хеш-суммы вирусов), SOC может оперативно добавить их в системы мониторинга и блокировки. Тем самым многие атаки выявляются на раннем этапе благодаря знаниям, полученным извне. По данным аналитиков, проактивное использование внешних индикаторов сокращает “время до обнаружения” (Mean Time to Detect) и снижает вероятность пропустить известную угрозух.

На этапе анализа и сдерживания инцидента информация из CTI помогает расследовать происшествие более глубоко. Имея сведения о типе атаки и типичных техниках злоумышленника, аналитики могут быстрее понять, каким путем проник враг, какие уязвимости были использованы и какова конечная цель. Например, зная, что определенная APT-группа применяет набор техник из матрицы ATT&CK (скажем, сочетание фишинга для первоначального доступа, затем использование легитимных средств администрирования в системе и разворачивание вымогательского ПО), команда реагирования сопоставляет эти шаблоны с событиями, зафиксированными в ин-

фраструктуре. Это помогает выстроить хронологию атаки и определить границы компрометации. Кроме того, CTI дает контекст – кто может стоять за атакой (киберпреступники, нацеленные на выкуп, или государственная APT-группа и т.д.), каковы их мотивации и ресурсы. Такая атрибуция по косвенным признакам основывается на базах данных о известных группах угроз и их “почерке” атак.

В результате расследование выходит за рамки чисто технического анализа локальных артефактов и приобретает черты разведывательного расследования, отвечая на вопросы “кто организовал атаку и зачем”.

Атрибуция и выработка мер противодействия. Когда инцидент предварительно изучен, перед ответственной командой стоит задача купировать ущерб и предотвратить повторение подобного сценария. Здесь данные кибербразведки также незаменимы. Во-первых, они позволяют атрибутировать инцидент – сопоставить его характеристики с известными кампаниями. Например, если в ходе анализа найдены индикаторы, ранее связывавшиеся с группировкой X, то есть высокая вероятность, что атакующая сторона – именно она. Это подтверждается и тактическими приемами (TTP), уникальными для данной группировки.

Во-вторых, CTI предоставляет рекомендации по реагированию, основанные на опыте прежних инцидентов. В отчётах threat intelligence часто содержатся советы: какие хеши заблокировать, какие домены добавить в черный список, какие уязвимости немедленно закрыть патчами, какие резервные меры предпринять. Опираясь на эту информацию, специалисты быстрее разрабатывают план нейтрализации и восстановления. Кроме того, по завершении инцидента данные разведки могут лечь в основу усовершенствования защитных мер: обновления правил IDS/IPS, настроек фаерволов, обучения персонала примерам новых атак и т.д.

Повышение эффективности расследований. Практика показывает, что интеграция кибербразведки в работу центров мониторинга и реагирования (SOC/CSIRT) повышает их эффективность. Например, в работе А.М. Вульфина описано внедрение платформы управления данными кибербразведки в корпоративном SOC, что привело к росту эффективности на ~41,7% и повышению уровня зрелости процесса реагирования с «начального» до «базового» уровня.

Это достигается за счет автоматизации рутинных этапов (агрегирование индикаторов, оповещение о новых угрозах), снижения количества ложных срабатываний и ускорения доступа аналитиков к релевантной информации. Таким образом, CTI действует как катализатор процесса расследования: многие шаги выполняются быстрее, а результаты становятся качественнее благодаря широте обзора угроз. При грамотной организации, кибербразведка превращает реагирование на инциденты из сугубо реактивной меры (после атаки) в проактивный процесс, где выявление и пресечение угроз возможно еще до того, как они нанесли серьезный ущерб.

Инновационные методы и автоматизация расследований

Применение искусственного интеллекта. С ростом объемов данных о киберугрозах аналитики все чаще обращаются к методам искусственного интеллекта (ИИ) и машинного обучения (МО), чтобы автоматизировать обработку разведданных и помочь в расследованиях. Традиционные методы CTI уже не успевают “переваривать” лавину информации – ежедневно появляются сотни отчетов об угрозах, тысячи новых IOC и уязвимостей. ИИ предлагает решения для ускорения и масштабирования этого процесса. В новейших исследованиях представлен концепт pipeline кибербразведки на базе ИИ, где на разных стадиях используются обучаемые модели.

Например, на этапе сбора и фильтрации применяются алгоритмы обработки естественного языка (NLP) для извлечения из текстовых потоков сущностей, связанных с атаками (имен группировок, упоминаний CVE, IOC) – такие модели могут автоматически выделять индикаторы из потоков OSINT с точностью ~89% .

Далее, для анализа и корреляции данных могут использоваться методы машинного обучения без учителя (кластеризация) – они группируют схожие инциденты, выявляют аномальные связки событий, помогая обнаруживать скрытые паттерны. Наконец, на этапе рекомендаций ИИ способен генерировать подсказки для реагирования: например, какие действия предпринять, исходя из характера атаки, сравнивая с исторической базой знаний.

Интересный пример – применение больших языковых моделей (LLM) для задач кибербразведки. Появились работы, где модели вроде GPT-3/4 используются для анализа крупных текстовых отчётов об угрозах и даже для диалогового взаимодействия, когда аналитик может “спросить” у модели совета по инциденту.

Первые результаты многообещающие: сообщается о высоких показателях точности при классификации техник по MITRE ATT&CK (до 97% в экспериментальных условиях). Однако, как показывают исследования, существуют и серьезные ограничения. Модели ИИ склонны генерировать недостоверные данные (hallucinations) и пока не гарантируют устойчивой работы на реальных больших отчётах. Например, при подаче полномасштабного отчета (несколько тысяч слов) качество извлечения снижается по сравнению с отрывками текста, на которых модели обучались.

Кроме того, ИИ требует наличия больших размеченных датасетов для обучения, что затруднено в сфере CTI (данные могут быть конфиденциальными и редко публикуются с разметкой). Таким образом, интеграция ИИ в кибербразведку – перспективное направление, но требующее решения проблем надёжности и прозрачности. Тем не менее, уже сейчас автоматизированные модели помогают сократить “шум” в разведданных и выделить главное: например, классифицировать входящие оповещения по степени критичности, связывать новые индикаторы с известными кампаниями и пр.

Автоматизация и оркестрация (SOAR). Помимо анализа данных, технологии автоматизации внедряются и непосредственно в процесс реагирования на инциденты – концепция SOAR (Security Orchestration, Automation and Response). Идея состоит в том, чтобы типовые цепочки действий при расследовании исполнялись автоматически по заданным плейбукам, с минимальным участием человека. Кибербразведка играет здесь важную роль: она обеспечивает обогащение инцидента дополнительной информацией и триггеры для автоматических реакций. К примеру, поступивший сигнал от системы мониторинга о сетевой аномалии автоматически обогащается платформой CTI – дополняется сведениями, известна ли замеченная IP-адрес или хэш-файл как вредоносный (проверка по TI-базе). Если да – система может сразу повысить критичность инцидента и запустить скрипт изоляции соответствующего узла сети, не дожидаясь ручного подтверждения. Далее, оркестрация может по готовому сценарию собрать с подозрительного хоста артефакты (файлы, логи) и передать их на анализ в песочницу или ИИ-модель malware-анализа. Таким образом, часть рутины, ранее выполнявшейся аналитиком, автоматизируется и ускоряется на порядки. Исследователи отмечают, что особенно эффективно автоматизировать реагирование на типовые массовые инциденты (например, блокировка фишинговых писем, отработка сигнатур IPS) – это высвобождает время экспертов для расследования действительно сложных, целевых атак.

В итоге сочетание CTI-платформ и SOAR приводит к созданию самоуправляемого конвейера: поступающая информация о новых угрозах сразу настраивает защитные механизмы, а выявленные инциденты автоматически проверяются на известные шаблоны атак и частично локализуются без участия человека.

Применение объяснимого ИИ и аналитики графов. Ещё одно новшество – использование графовых баз данных и методов для представления разведданных. Угрозовая информация по природе своей графовая: группы хакеров связаны с кампаниями, те – с конкретными IOC, эксплойты – с уязвимостями, и т.д. Построив граф знаний о угрозах, можно применять алгоритмы поиска путей, центральных узлов (центров влияния) и др. для выявления ключевых элементов атаки. Например, обнаружив новый малваре-хеш, система на графе сразу покажет, к каким семействам malware он может принадлежать, с какими атаками связан и через какие инфраструктурные узлы (серверы управления) проходит – это облегчает расследование. Кроме того, все больший интерес вызывает объяснимый ИИ (XAI) в кибербразведке.

Речь о том, чтобы модели не только выдавали предсказание (скажем, “данный URL подозрителен”), но и объясняли, какие признаки к этому привели (например, “URL был замечен ранее в связке с доменом из ботнет-сети”). В 2022 году опубликованы работы, где объединяются методы XAI и OSINT для улучшения обмена разведданными.

Это позволяет повысить доверие аналитиков к автоматическим рекомендациям и упростить валидацию – критически важную для успеха CTI. Ведь ценность представляет только достоверная и проверенная разведывательная информация; ложные срабатывания или устаревшие сведения могут дезориентировать команду. Поэтому в инновационных подходах делается упор на поддержание качества данных: вводятся метрики надежности источников, автоматические системы оценивают “свежесть” индикаторов и отметку о том, подтверждались ли они реальными инцидентами.

Международные и отечественные практики применения

Международный опыт. В мировой практике кибербразведка уже стала неотъемлемой частью киберзащиты на уровне государства и крупных корпораций. В США после серии крупных атак (например, эпизод с SolarWinds в 2020 г.) был сделан акцент на усилении обмена threat intelligence между частным и гос. секторами. Действуют программы обмена индикаторами (AIS – Automated Indicator Sharing) под эгидой DHS, где данные о обнаруженных угрозах оперативно рассылаются участникам через стандарты STIX/TAXII. Кроме того, существуют отраслевые центры обмена – ISAC (Information Sharing and Analysis Center) для разных секторов (финансы – FS-ISAC, энергетика – E-ISAC и т.д.), которые собирают сведения об атаках, специфичных для отрасли, и распространяют рекомендации. На уровне компаний многие завели собственные разведывательные подразделения или как минимум подписываются на коммерческие TI-фиды. Например, крупные технологические компании имеют команды Threat Intelligence, которые не только реагируют на угрозы, но и проводят активные исследования деятельности хакерских групп, публикуя результаты в открытых отчетах. Базы знаний вроде MITRE ATT&CK используются повсеместно: они позволяют всем участникам говорить на одном языке при описании атак, что упрощает корреляцию данных между разными организациями. Популярны регулярные отчеты о ландшафте угроз (Threat Landscape) – ежегодные обзоры (например, от ENISA в Европе, от компаний вроде Cisco Talos, Palo Alto Unit42), где анализируются ключевые тенденции и статистика инцидентов. Эти отчеты служат ориентиром для ИБ-специалистов, показывая, какие типы атак выросли, какие техники сейчас на пике, какие уязвимости эксплуатируются наиболее часто и т.д. Научное сообщество также активно исследует CTI: появляются конференции и рабочие группы, посвященные обмену разведданными, разрабатываются новые методы (как упомянуто в предыдущем разделе – ИИ, графы, NLP для CTI). Таким образом, на международной арене сформировалась экосистема, где правительства, бизнес и исследователи совместно движут прогресс в области кибербразведки.

Отечественные подходы и кейсы. В Российской Федерации интерес к киберразведке также возрос на фоне участившихся кибератак на бизнес и государственные ресурсы. Банк России с 2016 года развивает центр ФинЦЕРТ (Financial CERT), предназначенный для обмена данными о киберугрозах в финансовом секторе. Участники (банки, финорганизации) через ФинЦЕРТ получают информационные рассылки о выявленных схемах мошенничества, новых видах вредоносного ПО, индикаторах, характерных для атак на банки. Кроме того, с 2018 года функционирует государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), координируемая ФСТЭК – в ее рамках накоплены сведения о инцидентах на критически важных объектах и налажен обмен информацией между госструктурами и операторами связи. Отдельного упоминания заслуживает вклад российских компаний в threat intelligence: лидеры индустрии кибербезопасности (Лаборатория Касперского, Group-IB, Positive Technologies, BI.ZONE и др.) имеют собственные подразделения киберразведки, которые отслеживают действия киберпреступности (в том числе в даркнете), выпускают отчеты о крупных атаках и предлагают коммерческие сервисы по предоставлению TI-данных. Например, Group-IB известна расследованиями деятельности российских и международных хакерских группировок, раскрытием сетей ботнетов; Positive Technologies публикует исследование уязвимостей и методы их эксплуатации, что тоже является частью CTI (информация о том, какие брешь наиболее опасны и активно используются). Такие компании зачастую сотрудничают с правоохранительными органами, передавая разведданные, которые помогают раскрывать киберпреступления.

В академической среде в России тема киберразведки также развивается. Проводятся исследования по внедрению платформ киберразведки в SOC отечественных организаций, анализируется эффективность обмена индикаторами компрометации между компаниями. Появляются учебные программы, готовящие специалистов по киберразведке и анализу угроз. Например, в ряде вузов введены дисциплины, где студентов учат применять методы ИИ в ИБ, разбирать реальные кейсы кибератак, используя бриллиантовую модель и MITRE ATT&CK для их анализа. Это способствует формированию сообщества экспертов, владеющих современными подходами к threat intelligence.

Можно отметить и некоторые кейсы применения киберразведки в расследованиях инцидентов в России. Так, в 2020-2021 годах крупные банки сообщали, что благодаря данным от ФинЦЕРТ им удалось предотвратить несколько целевых атак на системы ДБО (дистанционного банковского обслуживания) – индикаторы, полученные из центра, позволили быстро выявить подготовительные действия злоумышленников и заблокировать их. Другой пример – расследование атаки вымогателей на одну из нефтегазо-

вых компаний: анализ показал, что использовались инструменты группы X, о чем ранее предупреждали в отчете Лаборатории Касперского; зная это, специалисты смогли предсказать дальнейшие шаги вымогателей и подготовиться к восстановлению системы из резервных копий, минимизировав простой. Эти случаи иллюстрируют практическую пользу CTI: знания, почерпнутые из внешних источников, напрямую конвертируются в уменьшение ущерба и повышение устойчивости к атакам.

Перспективы и дальнейшее развитие

Развитие сотрудничества и обмена данными. В будущем ожидается еще более тесная интеграция кибербразведки в коллективную безопасность. Ни одна, даже самая большая, организация не в состоянии самостоятельно отследить весь спектр киберугроз. Поэтому тренд – в расширении партнерских сетей обмена CTI. Появляются новые ISAC и аналогичные обменные площадки даже для нетрадиционных секторов (например, для отрасли здравоохранения, для университетов). Международные организации (ООН, Интерпол) призывают страны делиться информацией о кибератаках для глобального противодействия. В техническом плане стандарты обмена (STIX/TAXII) будут развиваться, чтобы поддерживать еще более сложные типы данных (например, обмен источниками телеметрии для обучения ИИ). Важной задачей остается стандартизация терминологии и классификаций – помимо MITRE ATT&CK, могут появляться новые таксономии для описания определенных классов угроз (скажем, для IoT-устройств, для АСУ ТП). Их согласование и принятие сообществом позволит эффективнее сопоставлять данные из разных источников.

Интеграция с управлением рисками. Еще одна перспективная линия – связь между кибербразведкой и управлением киберрисками организации. Уже сейчас некоторые продвинутые программы CTI стремятся не просто собрать данные об угрозах, но и оценить их релевантность конкретной организации. Идея “Threat Intelligence to Risk Intelligence” заключается в том, чтобы на основе разведданных формировать метрики риска: например, учитывая отрасль компании, технологии, которые она использует, автоматически вычислять, какие угрозы из глобального ландшафта наиболее вероятны и критичны именно для нее. Для этого CTI-системы будут интегрироваться с инвентаризацией ИТ-активов, сканерами уязвимостей, бизнес-контекстом. Перспектива такова, что отчеты кибербразведки станут не просто техническими сводками, а частью стратегического принятия решений на уровне бизнеса – например, вложиться ли в усиление защиты определенной системы, исходя из роста атак на аналогичные системы в отрасли (подсказанного CTI).

Усиление роли искусственного интеллекта. К 2025–2030 гг. можно ожидать значительного прогресса в применении ИИ для автоматизации кибербразведки. Вероятно появление специализированных крупных моделей,

обученных на массивах данных инфобезопасности, оптимизированных под извлечение IOC, классификацию атак и даже предсказание шагов злоумышленников. Такие модели будут интегрированы в инструментарий аналитиков в виде интеллектуальных помощников. Однако параллельно встанет вопрос об их надежности: потребуется решать проблему адверсариальных атак на сами системы ИИ (когда злоумышленники могут “кормить” модель искаженными данными, чтобы сбить аналитику с толку).

Будут разрабатываться методы защиты моделей и проверки их выводов человеком (human-in-the-loop останется важной частью процесса). Также внимание уделят вопросам этики и конфиденциальности: при сборе разведданных важно соблюдать законность (например, OSINT не должен нарушать персональные данные), а при обмене – не раскрывать лишнего. По мере усложнения аналитических систем могут возникнуть и правовые требования – вплоть до лицензирования деятельности по киберразведке в отдельных юрисдикциях.

Расширение охвата новых доменов. Традиционно CTI фокусировалась на ИТ-системах, но с развитием Интернета вещей, промышленных сетей, автотранспорта и др. появляется необходимость в разведданных и для этих областей. Например, прогнозируется рост угроз для автомобилей с подключением к сети (Car Hacking) – производители уже обмениваются данными о обнаруженных уязвимостях в программном обеспечении автомобилей. Похожая ситуация с медтехникой: нужны специализированные разведывательные сведения о взломе медицинских приборов, госпитальных систем. Это приведет к появлению нишевых платформ threat intelligence, ориентированных на конкретные сектора или типы устройств. Также возрастает интерес к разведке в социальной сфере – отслеживание информационных операций, фейков, которые могут сопровождать кибератаки (например, вбросы в СМИ как отвлекающий маневр). Такие гибридные угрозы потребуют совмещения киберразведки с традиционной информационной разведкой.

В целом, перспектива развития киберразведки – это движение к более опережающему, предиктивному характеру защиты. Если сегодня CTI во многом реагирует на уже произошедшие события (пусть и быстро), то в идеале она должна предугадывать векторы атак. За счет накопления огромного массива данных и применения аналитики big data, возможно, удастся строить модели прогнозирования: какие уязвимости с наибольшей вероятностью будут эксплуатироваться в ближайшие месяцы, какие типы атак возрастут в связи с политической обстановкой, и т.п. Такие прогнозы помогут заранее укреплять самые уязвимые места. Путь к этому лежит через дальнейшую профессионализацию сообщества CTI, развитие технологий и – главное – через доверие и обмен между всеми участниками. Киберразведка эффективно работает там, где есть кооперация, поэтому будущее за открытыми экосистемами обмена знаниями об угрозах.

Заключение

Кибербразведка из вспомогательного направления ИБ превратилась в один из краеугольных компонентов защиты от сложных киберугроз. В ходе расследования инцидентов технологии CTI предоставляют необходимый контекст и знания, позволяющие быстрее обнаруживать атаки, глубже их анализировать и эффективнее реагировать. Интеграция threat intelligence в процессы SOC и DFIR (Digital Forensics and Incident Response) доказала свою эффективность на практике – сокращаются сроки выявления и ликвидации угроз, снижается ущерб от инцидентов, повышается осведомленность команд о актуальных тактиках злоумышленников.

Современные тенденции показывают стремление сделать кибербразведку более автоматизированной и проактивной. Инновационные подходы, такие как использование машинного обучения для обработки больших объемов разведданных и внедрение SOAR-оркестрации, закладывают основу для “самообороны” инфраструктур, где многие рутинные действия выполняются без участия человека. В то же время, роль экспертов-аналитиков не снижается: напротив, автоматизация освобождает время для творчества – расследования наиболее нетривиальных, новых атак, требующих аналитического мышления и интуиции.

Отдельно стоит подчеркнуть значение сотрудничества. Ни одна организация не может обладать полной картиной всех угроз, поэтому обмен информацией и общий ситуационный контроль – необходимое условие успешного противодействия. Создание сообществ, общих баз индикаторов (таких как MISP), международных центров обмена и доверительных отношений между частными и государственными структурами – все это показало свою эффективность и должно развиваться.

Таким образом, применение технологий кибербразведки в расследовании инцидентов будет только расширяться. Новые инструменты позволят предсказывать ходы противника, а совместные усилия помогут сдерживать даже самые изощренные атаки. Индустрия кибербезопасности стоит на пороге качественного рывка, где intelligence-подходы станут основой опережающей защиты. Для российских специалистов участие в этом глобальном тренде открывает возможности использовать лучшие мировые наработки и одновременно вносить свой вклад в развитие методов кибербразведки.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. GOEL N., MANSI, SETHI N. Cyber Threat Intelligence: A Survey on Progressive Techniques and Challenges // International Journal of Advances in Science, Engineering and Technology (IJASEAT). – 2022. – Vol. 10, No. 3. – P. 65-70.
2. *Вульфин А.М.* Система управления данными кибербразведки // Моделирование, оптимизация и информационные технологии. – 2021. – Vol. 9, No. 1. – DOI: 10.26102/2310-6018/2021.32.1.020. – Режим доступа: https://moitvivt.ru/ru/journal/pdf?id=925.

3. *Masilela L., Nel D.* Cyber threat intelligence practices in the national sphere of government in South Africa // *International Journal of Research in Business and Social Science*. – 2023. – Vol. 12. – P. 402-414. – DOI: 10.20525/ijrbs.v12i8.2914.
4. Mezzi E., Massacci F., Tuma K. Large Language Models are unreliable for Cyber Threat Intelligence // arXiv preprint arXiv:2503.23175v1 [cs.CR]. – 2025, 29 Mar. – Режим доступа: https://arxiv.org/html/2503.23175v1#:~:text=by%2095,6.
5. *Серёдкин С.П.* Кибербразведка как эффективная стратегия защиты от киберугроз // Информационные технологии и математическое моделирование в управлении сложными системами: электрон. науч. журнал. – 2024. – № 4. – С. 14-22. – Режим доступа: http://ismmirgups.ru/toma/424-2024 (свободный). – Загл. с экрана. – Яз. рус., англ. (дата обращения: 09.12.2024).

УДК 004.4

В.Н. Гудимов, С.Г. Самохвалова

Амурский государственный университет, Россия, г. Благовещенск

ПРОГРАММНАЯ ВИЗУАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ПЕРЕСТАНОВКИ

Чем глубже цифровые технологии проникают в нашу жизнь, тем острее встает проблема кибербезопасности. Защититься от угроз виртуального мира поможет криптография. Для повышении интереса к криптографии и ее историческим аспектам, в статье рассматривается программная визуализацию криптографических методов перестановки. Для визуализации криптографических методов перестановки разработан программный продукт.

Ключевые слова: *криптография, программа, визуализация, магический квадрат, шифр «скитала», методы перестановки.*

The deeper digital technologies penetrate our lives, the more acute the problem of cybersecurity becomes. Cryptography will help protect against threats of the virtual world. In order to increase interest in cryptography and its historical aspects, the article considers software visualization of cryptographic methods of permutation. A software product has been developed for visualization of cryptographic methods of permutation.

Keywords: *cryptography, program, visualization, magic square, Skitale cipher, permutation methods.*

Введение

Криптография на протяжении всей истории занимает важное место в обеспечении безопасности информации и коммуникаций. Современные устройства, такие как смартфоны и компьютеры, часто используют шифрование, о котором пользователи могут не догадываться. Методы криптографии, помогают расширить кругозор студентов, развивают нестандартное мышление, создают условия для повышения познавательного интереса.

Цель создания данной программы заключается в том, чтобы сделать криптографию более доступной и увлекательной для широкой аудитории. Она имеет обучающий характер, предоставляя пользователям возможность не только наблюдать за процессом шифрования в реальном времени, но и самим осваивать основные принципы работы с различными методами защиты информации.

Описание разрабатываемого программного продукта

Программа предназначена для функционирования на большинстве современных компьютеров и обладает интуитивно понятным игровым процессом, что способствует легкой ориентации пользователей в обучении. В процессе разработки акцент был сделан на избегание перегруженности функционала, исключая ненужные элементы, которые могут отвлекать или запутывать пользователей. Визуальная составляющая программы была разработана с учетом привлекательности и приятности восприятия, при этом не отвлекая от основной цели – обучения.

Для того чтобы программная визуализация соответствовала предъявленным требованиям были решены следующие задачи:

- изучена предметная область (история происхождения и алгоритмы работы);
- выбрано программное обеспечение для реализации программной визуализации;
- спроектированы и созданы модели для игровых локаций;
- разработан пользовательский интерфейс и визуализация криптографических методов.

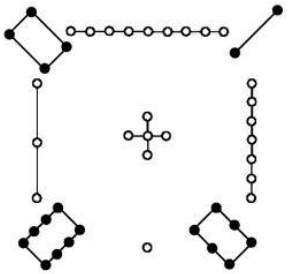
Описание предметной области

Для того чтобы ввести пользователей в мир криптографии были выбраны криптографические методы перестановки. Они известны с древнейших времён, тем самым демонстрируют историческую значимость криптографии и имеют простоту алгоритмов, что делает их идеальным выбором для введения в криптографию.

В качестве основных методов, которые были представлены в программе, были выбраны шифр перестановки «скитала» и магический квадрат.

Магический квадрат представляет собой квадратную матрицу, в которой сумма чисел в каждой строке, столбце и диагонали равна одной и той же «магической» константе.

Происхождение магического квадрата уходит корнями в древнюю культуру Китая. Одной из наиболее известных легенд о магическом квадрате является предание о Ло Шу. Согласно нему, когда люди наблюдали за наводнением на реке Ло, они увидел на берегу черепаху. На её панцире были изображены числа, которые, как оказалось, образовывали магический квадрат 3x3, с магической константой равной 15, рис. 1.



4	9	2
3	5	7
8	1	6

Рис. 1. Магический квадрат Ло Шу

Этот квадрат стал символом гармонии и баланса, а также предметом изучения как в математике, так и в оккультных практиках.

Процесс шифрования с использованием магического квадрата включает создание матрицы, заполненной числами от 1 до n^2, где n – размер квадрата. Числа располагаются таким образом, чтобы сумма всех строк, столбцов и диагоналей была одинаковой. При шифровании сообщения каждая буква заменяется соответствующим числом из магического квадрата.

Дешифрование осуществляется путем восстановления изначального магического квадрата и замены чисел на буквы по аналогичному принципу. Однако данный метод имеет свои недостатки, так как по своей сути дешифрование происходит методом перебора.

Основным плюсом шифрования данным методом является простота в использовании и наглядность, что делает его доступным для понимания. Тем не менее, уязвимость к частотному анализу может стать серьезной проблемой, особенно если зашифровано большое количество текста. Кроме того, ограниченность по размеру и сложности шифра зависит от размеров квадрата.

Шифр «скитала», известный в Древней Греции, использовался спартанцами для передачи секретных сообщений. Информация записывалась на ленте, которая затем обматывалась вокруг цилиндра которую называют «скитала», рис. 2. Только тот, кто имел идентичный цилиндр, мог прочитать сообщение, диаметр цилиндра является ключом.

Процесс шифрования с использованием шифра «скитала» начинается с подготовки цилиндра определенного диаметра. Лента обматывается вокруг «скиталы» без зазоров, и сообщение записывается вдоль ленты. После снятия ленты текст становится неразборчивым, что обеспечивает определенный уровень безопасности при передаче сообщения.

Рис. 2. Скитала

Дешифрование осуществляется путем обматывания ленты вокруг конусообразного объекта пока текст не станет разборчивым или составляется шифрующая таблица с помощью, которой подбирается число N – количество букв на окружности «скиталы», после чего по формуле (2) можно рассчитать её диаметр.

$$\mathrm{N} = \pi D, \tag{1}$$

$$\mathrm{D} = \frac{N}{\pi}, \tag{2}$$

Преимущества шифра «скитала» заключаются в простоте реализации с использованием доступных материалов и безопасности, поскольку перехваченные сообщения без соответствующего цилиндра остаются неразборчивыми.

К недостаткам можно отнести: необходимость физического доступа к цилиндру для дешифрования и то, что длина сообщения зависит от размера «скиталы», что может стать препятствием при передаче более объемной информации.

Разработка моделей

Первостепенной задачей стало проектирование, создание локации и отдельных моделей. Локации и модели создавались с учётом исторических корней методов шифрования. Для магического квадрата – Китай, а для шифра «скитала» – древняя Спарта.

Для реализации было выбрано приложение Blender, рис. 3. Этот инструмент оказался идеальным выбором благодаря своей доступности, многофункциональности и простоте освоения.

Рис. 3. Blender3D

Для того чтобы создать локацию первостепенно необходимо создать её макет, который станет основой для дальнейшей разработки. На этом этапе необходимо четко определить, какие модели должны находиться на локации и какой у неё должен быть рельеф. С помощью простых геометрических фигур был создан макет, на который в будущем можно ссылаться, рис. 4

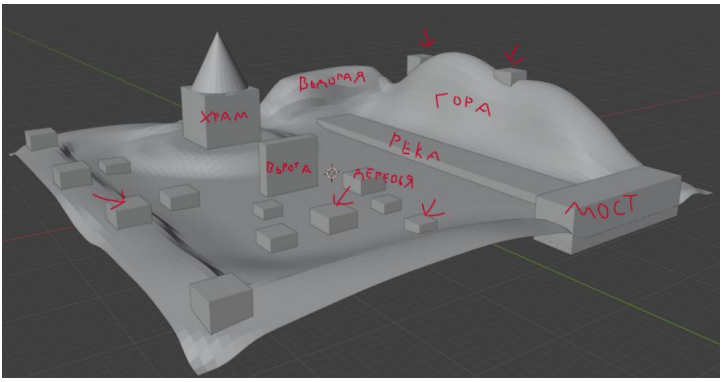


Рис. 4. Макет локации

Следующим важным аспектом стал выбор визуального стиля. Поскольку игровой процесс не привязан к точной симуляции реальной жизни и локация требуется в основном как фон для игрового процесса, было решено использовать метод LowPoly (низко полигональный).

После определения визуального стиля и создания макета, необходимо собрать вспомогательные изображения, на основе которых будут создаваться модели. Изучая различные изображения были выбраны несколько архитектурных особенностей культурного контекста которые необходимо реализовать в виде моделей.

Для локации магического квадрата были созданы следующие модели. Модель моста в традиционном китайском стиле, рис. 5.

Рис. 5. Модель моста в китайском стиле

Пагода, как важный элемент восточной архитектуры, тоже была воссоздана в виде модели, рис. 6.

Рис. 6. Модель Пагоды

В локации нашлось место воротам Тории. Несмотря на простоту конструкции, существует множество типов торий. Мёдзин-тории, более распространённые, поэтому было принято решение изобразить их, рис. 7.

Рис. 7. Модель Мёдзин-тории

Для локации шифра «скитала» было создано несколько моделей основываясь на вспомогательных изображениях, создана модель статуи Леонида I, рис. 8.

Рис. 8. Модель Леонида I

Одной из главных моделей на локации служит храм Афины, рис. 9.

Рис. 9. Модель храма Афины

Ещё одной важной моделью стал спартанский театр, рис. 10.

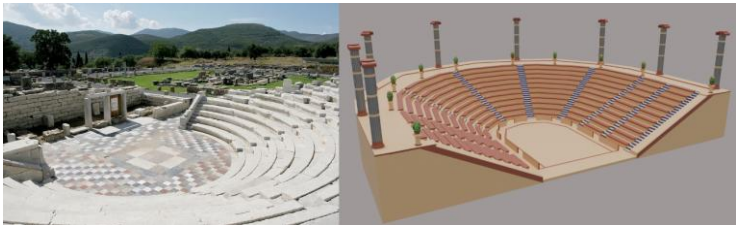


Рис. 10. Модель спартанского театра

После создания моделей ориентируясь на макет, создаём похожий рельеф, добавляем деревья, траву, камни, расставим созданные ранее модели. В результате получим две готовые локации для магического квадрата (рис. 11), для шифра «скитала» (рис. 12).

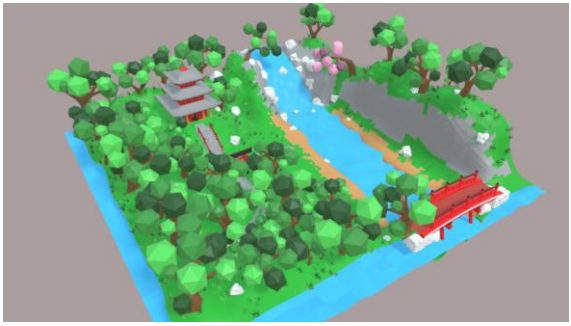


Рис. 11. Итоговый вариант локации для Магического квадрата

Рис. 12. Итоговый вариант локации для шифра «скитала»

Разработка программы

В качестве среды разработки и движка для программы был выбран Unity. Unity зарекомендовал себя как одна из наиболее популярных платформ для создания игр и интерактивных программ, что делает его отличным выбором для небольших проектов, подобных этому.

В результате проведенной работы была разработана программа визуализации, которая представляет собой лекцию, дополненную иллюстрациями, рис. 13, 14.

Рис. 13. Демонстрация игрового процесса

Рис. 14. Демонстрация игрового процесса

В рамках программы визуализации предоставлены не только теоретические знания, но и внедрены практические элементы для закрепления материала, например присутствуют задания на дешифровку сообщений, рис. 15.

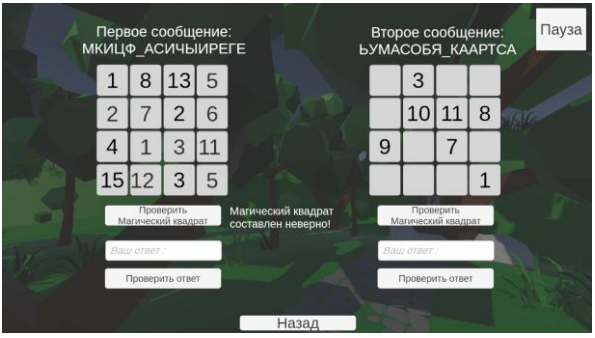


Рис. 15. Задание с дешифрованием

У пользователей есть возможность попрактиковаться в шифровании сообщений, рис. 16.

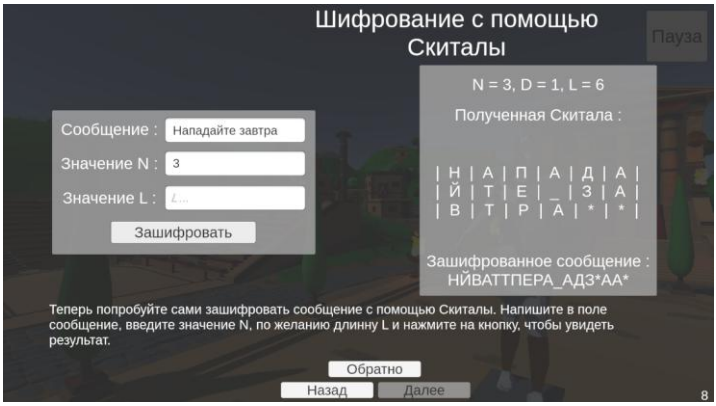


Рис. 16. Задание с шифрованием

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Бонд Д.Г.* Unity и C#. Геймдев от идеи до реализации. – 2-е изд. – Питер, 2023. – 928. – ISNB 978-5-4461-0715-5.
2. *Денисов Д.* Разработка игры на Unity. С нуля до публикации. – SelfPub, 2021. – 177. – ISNB978-5-0437-2633-9.
3. *Жадаев А.* Нумерология на компьютере. Расчет судьбы по методике Пифагора. – ЛитРес, 2022. – 66. – ISNB 978-5-0403-4924-1.
4. *Крючкова Е., Крючкова О.* Китайская магия (Книга сакральных традиций Китая). – Велигор, 2021. – 240. – ISNB978-5-0405-4130-0.
5. *Романенко Е.* Blender. Дизайн интерьеров и архитектуры. – Питер, 2024. – 176. – ISNB978-5-4461-2136-6.
6. *Саллинс С.* Low Poly 3D Modeling in Blender. –Packt Publishing, 2024. – 318. – ISNB 978-1-8032-4123-4.
7. *Фомичёв В.* Криптография – наука о тайнописи. – ЛитРес, 2021. – 168. – ISNB978-5-0430-6670-1.

УДК 004.089

А.А. Даньшина

Волгоградский государственный университет, Россия, г. Волгоград

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПРЕДСКАЗАНИЯ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ

Целью данной статьи является повышение эффективности предсказания мошеннических транзакций в антифрод-системах. Для этого разработан программный комплекс и описаны этапы его работы. В ходе исследования проанализирована статистика количества операций без добровольного согласия клиентов в банковской сфере за 2023 и 2024 года, рассмотрены правила и фильтры, применяемые в системах противодействия мошенничеству, проанализированы современные методы машинного обучения, описан процесс предобработки входных данных и определены критерии для сравнительного анализа моделей. Результатом исследования является определённая с помощью программного комплекса наилучшая обучающая модель с подобранными гиперпараметрами.

Ключевые слова: *антифрод-система; мошеннические транзакции; модели машинного обучения; программный комплекс; предобработка данных.*

The purpose of this article is to increase the effectiveness of predicting fraudulent transactions in anti-fraud systems. For this purpose, a software package was developed and the stages of its operation are described. The study also analyzed statistics on the number of transactions without the voluntary consent of customers in the banking sector for 2023 and 2024, reviewed the rules and filters used in anti-fraud systems, analyzed modern machine learning methods, described the process of input data preprocessing and defined criteria for comparative analysis of models. The result of the research is the best training model with selected hyperparameters determined using the software package.

Keywords: *anti-fraud system; fraudulent transactions; machine learning models; software package; data preprocessing.*

Введение

Современная тенденция развития электронных технологий послужила толчком к модернизации и усовершенствованию различных сфер жизни человека. Сети передачи информации позволили перейти на новый уровень коммуникации, обмена данными и организации рабочих процессов. Сферой, на которую наибольшим образом повлияла цифровизация, является экономика. Активно развивается рынок платёжных инструментов, о чём свиде-

тельствует рост использования цифровой валюты, составляющей подавляющую часть денежного оборота страны. Формирование такой прогрессивной информационной среды позволяет сократить издержки бизнеса и перевести традиционные рынки на новый уровень.

Банки, как основные регуляторы финансового рынка, также претерпели видоизменения в своей деятельности. Статистика за декабрь 2024 года показывает, что постепенный переход из оффлайн режима оказания услуг в онлайн послужил приросту числа использования онлайн-банкинга на 60% по сравнению с прошлым годом [1]. Всё большее количество клиентов банка отдаёт предпочтение использованию безналичного расчёта и хранению денежных средств в цифровом виде.

Однако с ростом эксплуатации электронных финансов, увеличилось число атак злоумышленников с целью незаконного хищения денежных средств. Наиболее распространённой тактикой получения прибыли является применение различных мошеннических схем. Центральный Банк России приводит статистику за 2024 год, согласно которой, объём операций без добровольного согласи клиентов увеличился на 74,36% по сравнению с 2023 годом [2].

Рис. 1. Динамика общего объёма и количества операций без добровольного согласия клиентов

Как показала статистика, основную долю из общего объёма хищений составляют денежные средства, похищенные у физических лиц.

Объём похищенных средств у физических лиц в 40 раз превышает объём у юридических лиц. Это свидетельствует о том, что в большинстве случаев, целью злоумышленников являются обычные граждане.

Рис. 2. Операции без добровольного согласия клиентов в 2024 году: физические и юридические лица

Предлагаемый метод решения

Для возможности противодействия кибератакам на банковские учреждения, а также для обеспечения необходимого и достаточного уровня защиты информации, разработано множество антифрод-систем, использующих адаптированные подходы специально под специфику финансового сектора.

Для выявления аномалий в портрете клиента банка, создаются типовые и уникальные правила, задающие следующие из возможных ограничений:

- количество покупок по одной банковской карте за определённый период времени;
- максимальная сумма разовой покупки по одной карте в определённый период;
- учёт истории покупок по банковским картам;
- частота совершаемых однотипных транзакций.

Также для выявления мошеннических транзакций применяются возможные фильтры:

- валидаторы – проверка реквизитов банковской карты на корректность;
- география – проверка IP-адреса клиента, совершающего транзакцию;
- соответствия параметров – соответствие страны IP-адреса клиента и эмитента банка;
- стоп-лист – проверка карты клиента на наличие её в «черных списках».

Системы противодействия банковскому мошенничеству нового поколения созданы с использованием машинного обучения и применения искусственного интеллекта, что позволяет значительно увеличить скорость и точность анализа событий. Применение технологии Big Data способствует формированию набора данных для автоматической интеллектуальной оценки потребительского поведения. Это позволяет быстро агрегировать метаданные о транзакциях и сопоставлять их с историей предыдущих платежей.

Для достижения таких результатов, применяются различные методы машинного обучения:

- обучение на исторических данных, что способствует прогнозированию вероятностей мошеннических транзакций;
- обучение без учителя, благодаря которому модели способны к анализу данных без предварительных разметок. Модели, обученные на таком подходе, могут извлекать необходимую информацию из больших объёмов данных, автоматически обнаруживая в них внутреннюю структуру;
- применение методов анализа текстовых данных позволяет разделять информацию на категории для выявления паттернов, что способствует выявлению аномалий в поведении клиента;
- использование свёрточных и рекуррентных нейронных сетей значительно увеличивает число обнаруженных мошеннических транзакций по сравнению с показателями простых моделей.

Стоит учитывать, что входные наборы данных для моделей машинного обучения чаще всего содержат артефакты, такие как шум, пропуски, дубликаты, или некорректно введённые значений, что может быть обусловлено как человеческим фактором, так и программными ошибками при сборе информации. Именно поэтому, важным этапом является процесс предобработки датасета для получения наиболее релевантных результатов обучения.

Центр Статистических Технологий Analytera систематизирует этапы предобработка данных следующим образом [3]:

1) изучение данных. Обеспечение ясности данных, что осуществляется путём оценки полноты данных, их формального описания, визуализации анализа в виде различных графиков.

2) очистка данных. Обеспечивается полнота, истинность, корректность и непротиворечивость данных. На этом этапе заполняются пропуски, если модель чувствительна к ним или неспособна самостоятельно их восстановить, обрабатываются невозможные значения, дубликаты записей, исправляются форматы ввода и осуществляется сглаживание возможных выбросов.

3) преобразование данных. Обеспечивается структурированность, однородность, согласованность и безызбыточность данных. Этап включает в себя кодирование номинативных переменных, приведение данных к нужному диапазону и стандартному нормальному распределению, дополнение данных новыми параметрами для повышения интерпретируемости модели, а также новыми данными, оптимизацию пространства признаков.

4) отбор переменных. Определяется совокупность переменных, на которых будет получен наилучший результат предсказания.

Если антифрод-система обучалась на качественно предобработанных данных, то эффективность обнаружения мошеннических транзакций будет значительно выше.

Для оценки обучающих моделей наиболее значимыми вводятся такие метрики как:

1) эффективность – насколько правильно подход способен выявить мошеннические транзакции среди общего объёма данных. Данный критерий подразделяется на метрики:

а) accuracy – доля верно предсказанных транзакций от общего числа транзакций. Рассчитывается по формуле (1):

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \quad (1)$$

где TP (true positives) – верно классифицированные мошеннические транзакции;

TN (true negatives) – верно классифицированные нормальные транзакции;

FP (false positives) – неверно классифицированные нормальные транзакции как мошеннические;

FN (false negatives) – неверно классифицированные мошеннические транзакции как нормальные.

б) precision – оценивает, сколько из всех транзакций, которые система классифицировала как мошеннические, действительно являются мошенническими. Рассчитывается по формуле (2):

$$precision = \frac{TP}{TP + FP} \quad (2)$$

в) recall – доля всех мошеннических транзакций, которую система смогла правильно классифицировать как мошеннические. Рассчитывается по формуле (3):

$$recall = \frac{TP}{TP + FN} \quad (3)$$

г) AUC-ROC – оценивает способность модели различать мошеннические транзакции от нормальных. Рассчитывается по формуле (4):

$$AUC = \int TRP(x)\, dx, \quad (4)$$

где AUC – это площадь под ROC-кривой, которая показывает соотношение между чувствительностью на оси Y и специфичностью на оси X. Чем выше AUC, тем лучше модель различает мошеннические транзакции

д) F1-score – гармоническое среднее между точностью и полнотой. Рассчитывается по формуле (5):

$$F1score = 2 \times \frac{precision \times recall}{precision + recall} \quad (5)$$

2) скорость обработки – время классификации мошеннической транзакции.

По этим критериям в данной статье будут сравниваться такие модели как: Логическая регрессия [4], XGBoost, LightGBM [5], SVC, Random Forest [6].

Для выполнения этой задачи и достижения поставленной цели был разработан программный комплекс способный предобработать входные данные, сформировать из них обучающий и тестовый наборы, провести сравнительный анализ моделей, а также определить наиболее эффективную из представленного перечня и сформировать для неё наилучшие гиперпараметры, позволяющие повысить эффективность предсказания.

Работа программного комплекса разделена на три этапа:

1) анализ входных данных посредством формирования диаграмм и таблиц, отображающих информацию о транзакциях, содержащуюся в транзакционном наборе; предобработка данных, где категориальные переменные, при их наличии, преобразуются в числовые, исключаются блоки, не имеющие большой значимости для обучающей выборки; разделение данных на обучающую и тестовую выборки в определённом соотношении с целью последующего машинного обучения.

2) определение базовых гиперпараметров для исследуемых моделей; машинного обучения с помощью моделей на базовых гиперпараметрах; получение результатов в виде сравнительной таблицы и выявление наиболее эффективной обучающей модели на её основе.

3) определения наилучших гиперпараметров для наиболее эффективной обучающей модели и машинное обучение на её основе.

Для проведения экспериментального исследования был сгенерирован размеченный набор данных, имитирующий реальные банковский транзакции. Целью машинного обучения будет решение задачи бинарной классификации для обнаружения незаконных транзакций. Размер датасета составляет 1000 строк и содержит переменные, описанные в табл. 1.

Таблица 1

Описание переменных, составляющих входной набор данных

Название переменной	**Описание**
1	**2**
step	Идентификационный номер, который присваивается каждой транзакции.
type	Описывает тип транзакционной операции.
amount	Сумма денежных средств, прошедших через транзакцию.
nameOrg	Имя отправителя денежных средств.
nameDest	Имя получателя денежных средств.

Окончание табл. 1

Название переменной	Описание
1	**2**
oldbalanceOrg	Обозначает старый баланс отправителя до совершения транзакции.
oldbalanceDest	Обозначает старый баланс получателя до совершения транзакции.
newbalanceOrg	Обозначает новый баланс отправителя после совершения транзакции.
newbalanceDest	Обозначает новый баланс получателя после совершения транзакции.
isFraud	Указывает, является ли транзакция мошеннической или законной.

Ключевыми переменными, указывающими на возможность мошеннической транзакции, являются amount, nameOrg и nameDest. Если же они имеют значения, сильно разнящиеся с ранее принимаемыми, то переменная isFraud выставляется в 1, что сигнализирует о возможной незаконной транзакции.

Переменные step, amount, oldbalanceOrg, oldbalanceDest, newbalanceOrg, newbalanceDest являются числовыми, а type, nameOrg, nameDest – категориальными. Наличие последних требует предобработки данных, приводящей все переменные к одному типу – числовому. Это необходимо для возможности последующего обучения моделей.

В реальных датасетах количество мошеннических транзакций меньше, чем законных. В исследуемом наборе данных это также учитывается. Именно поэтому для корректности результатов применяется балансировка данных методом SMOTE.

	step	amount	oldbalanceOrg	newbalanceOrg	oldbalanceDest	newbalanceDest	isFraud
count	1000.000000	1000.00000	1000.000000	1000.000000	1000.000000	1.000000e+03	1000.000000
mean	399.546000	494920.78400	494423.863484	-496.920516	510842.053949	1.005763e+06	0.044000
std	230.245223	289737.74752	288732.344270	404375.576148	289766.908806	4.056426e+05	0.205198
min	0.000000	2022.00000	1160.273380	-948834.550684	1021.760534	4.229278e+04	0.000000
25%	197.000000	243533.00000	252630.832454	-286267.838528	253018.339209	7.141371e+05	0.000000
50%	392.000000	485370.00000	493172.936431	-4581.486293	519061.858626	1.020104e+06	0.000000
75%	603.250000	741583.50000	742787.394577	307026.826959	755818.851933	1.300998e+06	0.000000
max	800.000000	997665.00000	998773.744988	912721.898049	999978.436963	1.986259e+06	1.000000

Рис. 3. Статистическая сводка транзакционного набора данных

На рис. 3 представлена таблица, описывающая общее количество транзакций в наборе; среднее значение переменных, являющееся мерой центральной тенденции; стандартное отклонение, показывающее, насколько значения в наборе данных отклоняются от среднего значения; процентную сводку значений параметров; минимальное и максимальное значение переменных.

Для анализа транзакционных записей формируются гистограммы количества операций и суммы операций различного типа, позволяющие сделать вывод, какой тип транзакций наиболее часто встречается в исследуемом наборе данных. Определено, что наиболее частой операцией является поступление денежных средств с общей суммой 196.440.004 рубля. Также для определения наиболее значимых переменных датасета формируется корреляционная матрица, отражающая информацию о зависимости переменных друг от друга. Обобщая её результаты, составляется табл. 2.

Таблица 2

Наиболее зависимые переменные корреляционной матрицы

Название переменной	**Значения зависимостей**		
1	**2**		
newbalanceDest	0.69		0.68
newbalanceOrg		0.69	
	amount	oldbalanceOrg	oldbalanceDest

Предобработка данных осуществляется в несколько этапов:

1. Кодирование переменной «type» – переменная типа совершаемой операции принимает значение 1, остальные принимают значение 0.
2. По ранее сформированной корреляционной матрице определяются нерелевантные столбцы и удаляются из набора данных. Оставшиеся данные разделяются на признаки и целевую переменную, в нашем случае – isFraud.
3. Категориальные переменные преобразуются в числовые.
4. Для балансирования числа мошеннических транзакций и законных, применяется метод SMOTE, синтезирующий данные до необходимого количества.

Для обучения моделей набор данный разделяется на обучающую и тестовую выборки в процентном соотношении 80% к 20% соответственно.

Разработанный программный комплекс производит машинное обучение с помощью моделей Логической регрессии, XBoost, LightGBM, SVC, Случайный лес на их базовых гиперпараметрах и производит сравнение. Результатом сравнительного анализа является таблица оценки параметров каждой модели, представленная на рис. 4.

```
Сравнение моделей по всем параметрам:
                  Model  Training Accuracy  Validation Accuracy  F1-score
0      LogisticRegression           0.769784             0.751958  0.754522
1           XGBClassifier           1.000000             0.924282  0.925831
2          LGBMClassifier           1.000000             0.916449  0.918367
3                     SVC           0.661216             0.597911  0.605128
4  RandomForestClassifier           0.992152             0.887728  0.890585

    AUC-ROC  Training Time
0  0.865952       0.000002
1  0.967545       0.000001
2  0.970436       0.000001
3  0.659535       0.000002
4  0.946449       0.000002

Наилучшие модели по каждому параметру:
Training Accuracy: XGBClassifier, LGBMClassifier с результатом 1.0
Validation Accuracy: XGBClassifier с результатом 0.9242819843342036
F1-score: XGBClassifier с результатом 0.9258312020460358
AUC-ROC: LGBMClassifier с результатом 0.9704358261059292
Training Time: LGBMClassifier с результатом 1.265e-06
```

Рис. 4. Сравнение моделей по всем параметрам и вывод наилучшей модели по каждому из них

По результатам сравнительного анализа наиболее эффективными моделями являются: XBoost и LightGBM. Однако для дальнейшего исследования и формирования обучающей модели на наилучших гиперпараметрах будет применяться модель LightGBM, так как она отличается скоростью обучения, а также способностью обрабатывать большой набор транзакционных данных с наивысшей точностью, что является значимым показателем при работе с реальным набором данных в банковской системе.

Программный комплекс позволяет определить наилучшие гиперпараметры для выбранной модели: boosting_type, learning_rate, max_depth, n_estimators, num_leaves. Далее происходит процесс переобучения. Для наглядной визуализации повышения эффективности результатов переобучения, формируется диаграмма показателей (рис. 5).

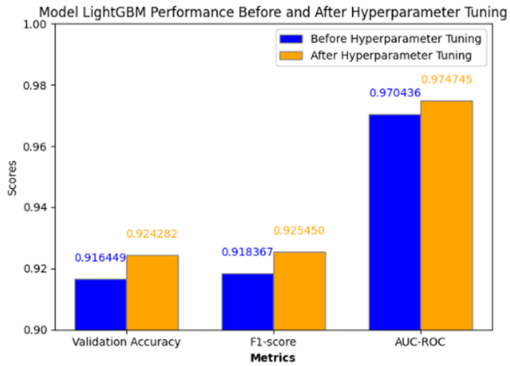


Рис. 5. Сравнение результатов обучения модели LightGBM на базовых и наилучших гиперпараметрах

Результаты эксперимента доказывают возможность повышения эффективности предсказания мошеннических операций и доказывают достижение поставленной цели.

Заключение

Статистический анализ банковских операций без добровольного согласия клиентов наглядно продемонстрировал важность продвижения исследований в сфере противодействия мошенничеству. Выявлено, что одним из значительных этапов в машинном обучении является качественная предобработка входного набора данных. Работа программного комплекса показала положительный результат машинного обучения с применением модели LightGBM, где с помощью наилучших гиперпараметров повысилась эффективность предсказания мошеннических операций. Дальнейшие исследования будут направлены на внедрение программного комплекса в систему противодействия банковскому мошенничеству.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Исследование: число гаджетов с подключенным онлайн-банкингом выросло на 15% [Электронный ресурс]. – URL: https://ria.ru/20241225/gadzhety-1991200249.html (дата обращения: 03.03.2025).
2. Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций [Электронный ресурс]. – URL: https://cbr.ru/analytics/ib/operations_survey/2024/ (дата обращения: 03.03.2025).
3. Обзор методов предобработки данных [Электронный ресурс]. – URL: https://golnk.ru/J5yM0 (дата обращения: 03.03.2025).
4. *Константин Буров.* Обнаружение знаний в хранилищах данных // Открытые системы.СУБД. – 1999. – № 5–6. – С. 67-77. – URL https://www.osp.ru/os/1999/05-06/179852 (дата обращения: 03.03.2025).
5. *Игорь Кураленок, Александр Щекалев.* GPU в задачах машинного обучения // Открытые системы.СУБД. – 2013. – № 8. – С. 44-46. – URL: https://www.osp.ru/os/2013/08/13037858/ (дата обращения: 03.03.2025).
6. Виктор Китов. Практические аспекты машинного обучения // Открытые системы.СУБД. – 2016. – № 1. – С. 14-17. – URL: https://www.osp.ru/os/2016/01/13048648 (дата обращения: 03.03.2025).

УДК 004.056

Ю.А. Дмитриев, В.Д. Михайлова

Южный федеральный университет, Россия, г. Таганрог

МОДУЛЬ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ ДЛЯ УМНОГО ПРОИЗВОДСТВА

Статья посвящена разработке концепта модуля тестирования безопасности для умного производства, ориентированного на киберфизические системы (КФС). Актуальность исследования обусловлена растущими угрозами для промышленных экосистем, включая атаки на SCADA-системы и уязвимости в промышленных протоколах передачи данных. Цель работы – предложить гибридный подход, сочетающий автоматизацию тестирования, использование цифровых двойников и интеграцию открытых инструментов для обеспечения сквозной оценки защищённости КФС без остановки производственных процессов. В основе концепта лежит трёхкомпонентная архитектура: Компонента сетевого анализа на базе nmap и Nessus API, обеспечивающий обнаружение устройств, сканирование портов и выявление уязвимостей в промышленных протоколах; Компонента эксплуатации уязвимостей с интеграцией Metasploit API для автоматизации атак на Modbus-регистры PLC и генерации кастомных пакетов через Scapy; Компонента генерации отчётов, формирующий результаты тестирования в форматах PDF (для операторов) и JSON (для интеграции с системами моделирования угроз). Ключевой инновацией является применение цифровых двойников – виртуальных копий физических устройств, позволяющих имитировать атаки в контролируемой среде. Интеграция API инструментов (nmap, Metasploit, Nessus) реализована через Python, что демонстрируется в статье на примерах кода для сканирования сети и запуска эксплойтов. Ограничения концепта связаны с поддержкой заданного набора протоколов (Modbus) и необходимостью ручной адаптации под специфику оборудования. Перспективы развития включают расширение функционала для MQTT и OPC UA, внедрение машинного обучения для прогнозирования уязвимостей, а также автоматизацию валидации цифровых двойников. Практическая значимость исследования заключается в создании адаптивной платформы, способной повысить устойчивость промышленных систем к эволюционирующим киберугрозам. Предложенный подход может быть применён в энергетике, нефтегазовой отрасли и других секторах умного производства.

Ключевые слова: *киберфизические системы, безопасность умного производства, цифровые двойники, автоматизация тестирования, промышленные протоколы, Modbus.*

The article is devoted to the development of the concept of a security testing module for smart manufacturing focused on cyber-physical systems (CPS). The relevance of the research is due to the growing threats to industrial ecosystems, including attacks on SCADA systems and vulnerabilities in industrial data communication protocols. The goal

of the work is to propose a hybrid approach combining test automation, the use of digital twins, and the integration of open source tools to provide end-to-end security assessment of KFSs without stopping production processes. The concept is based on a three-component architecture: a network analysis component based on nmap and Nessus API, providing device discovery, port scanning and vulnerability detection in industrial protocols; a vulnerability exploitation component with Metasploit API integration to automate attacks on PLC Modbus registers and generation of custom packets via Scapy; and a report generation component that generates test results in PDF (for operators) and JSON (for integration with threat modeling systems). The key innovation is the use of digital twins – virtual copies of physical devices that allow to simulate attacks in a controlled environment. Integration of API tools (nmap, Metasploit, Nessus) is implemented via Python, which is demonstrated in the article with code examples for scanning the network and launching exploits. The limitations of the concept are related to the support of a limited set of protocols (Modbus) and the need for manual adaptation to the specifics of the equipment. Development prospects include extending functionality for MQTT and OPC UA, introducing machine learning for vulnerability prediction, and automating validation of digital twins. The practical significance of the research lies in the creation of an adaptive platform that can improve the resilience of industrial systems to evolving cyber threats. The proposed approach can be applied in the energy, oil and gas, and other smart manufacturing sectors.

***Keywords**: cyber-physical systems, smart manufacturing security, digital twins, test automation, industrial protocols, Modbus.*

Введение

Промышленные системы всё чаще становятся мишенями кибератак, что подчёркивает критическую важность их защиты. В настоящее время с развитием технологий подобные решения включают в себя совокупность “Интернета вещей”, “Интернета людей” и “Интернет сервисов”. Такое объединение принято называть киберфизической системой (КФС).

Интеграция КФС в нашу жизнь сталкивается с растущими угрозами. Ключевыми проблемами являются [1]:

- гетерогенность компонентов используемых систем;
- сложность взаимодействия между вычислительным и физическими слоями;
- устаревшие протоколы передачи данных, не рассчитанные на современные угрозы безопасности;

Современные технологические процессы, реализуемые на производственных цепочках, предполагают постоянное взаимодействие физических активов и оборудования обеспечения производства с программными компонентами и ИТ-процессами. Цифровизация позволяет значительно повысить эффективность технологических и бизнес-процессов, но также она делает системы более уязвимыми перед киберпреступниками. Поскольку даже простые исполнительные механизмы и сенсоры становятся частью системы промышленного интернета вещей (IIoT) при подключении, значительно

возрастают случаи кибератак. Помимо оконечных устройств (сенсоры, актуаторы), злоумышленники часто выбирают в качестве целей различные промышленные контроллеры (PLC). Аппаратные уязвимости и уязвимости прошивки могут привести к перехвату контроля над оборудованием, подмене данных на стороне системы диспетчерского управления и сбора данных (SCADA-системы) или его отказу в обслуживании (DoS) – это критически опасно для отрасли промышленности, так как может повлечь за собой остановку производства на промышленных объектах [3].

Примером низкого уровня защищенности киберфизических систем можно считать недавний инцидент, связанный с компанией «Львовтеплоэнерго». Специалисты компании Dragos провели анализ вредоносного программного обеспечения FrostyGoop. По данным исследователей, это ПО использовалось в январе 2024 года для атаки на систему отопления более чем в 600 многоквартирных домах во Львове (Украина). Исследование подчеркивает, что это первый случай, когда напрямую эксплуатируется уязвимость протокола Modbus, который стандартно применяется во многих промышленных секторах [4].

Подобные случаи кибератак становятся актуальной проблемой, требуя обратить особое внимание на внедрение инструментов тестирования безопасности, адаптированных к специфике промышленных экосистем и комбинирующих в себе уже готовые открытые инструменты автоматизации проверки систем на защищенность. Такие решения помогут предотвратить утечки информации, обнаруживая слабые места до их эксплуатации.

Основная проблематика существующих решений, таких как Burp Suite, Nessus и Metasploit, заключается в их ограниченной ориентированности на универсальные IT-системы [5]. Они не учитывают особенности промышленных протоколов, низкую частоту обновлений ПО в производственных системах и высокие риски атак на физические компоненты. Кроме того, фрагментированность методов тестирования (статический анализ, динамическое сканирование, тестирование на проникновение) и использование производствами средств накладной безопасности (межсетевые экраны, антивирусы) затрудняет комплексную оценку защищенности КФС [6].

Целью данной работы является повышение защищённости умного производства за счёт автоматизации тестирования киберфизических систем (КФС) и моделирования многоэтапных атак, направленных на выявление уязвимостей в промышленных протоколах. В рамках статьи предложен прототип модуля тестирования безопасности для умного производства, объединяющего три ключевых компонента:

1. Инструменты сетевого анализа для определения устройств в системе.
2. Интеграционный слой эксплуатации уязвимостей (эксплойты) и нагрузочного тестирования (Metasploit API, Nesus API, hping3).
3. Механизм обратной связи, автоматизирующий генерацию отчетов и рекомендаций на основе результатов тестов.

Новизна предложенного подхода заключается в комбинации методов сканирования сети с сохранением найденных устройств, нагрузочного тестирования и использования модуля поиска готового ПО для реализации уязвимостей, что позволяет имитировать многоэтапные атаки на киберфизические системы.

Теоретические основы безопасности киберфизических систем

Для обеспечения безопасности КФС должна удовлетворять следующим требованиям [7]:

- конфиденциальность;
- отказоустойчивость;
- способность противостоять атакам;
- возможность обнаружения вторжений.

При проведении тестов на проникновение обычно пользуются методиками, которые регламентируют этапы тестирования, порядок испытаний тестируемых объектов, порядок взаимодействия аудитора с заказчиком и т.д. К широко распространенным зарубежным стандартам и методикам относятся [8]:

1) OWASP – Open Web Application Security Project [9];
2) PTF – Penetration Testing Framework [10];
3) ISSAF – Information System Security Assessment Frame-work [11];
4) PTES – Penetration Testing Execution Standard [12];
5) OSSTMM – The Open Source Security Testing Methodology Manual [13];
6) NIST SP 800–115 – Technical Guide to Information Security Testing and Assessment [14].

Для концепта будет использована методика PTF с некоторыми изменениями. Ключевым элементом является интеграция всех перечисленных требований в единую архитектуру безопасности, при которой компрометация одного уровня не приводит к полной утрате работоспособности КФС, а каждая подсистема перекрестно проверяет целостность и актуальность информации друг друга.

Кроме того, жёсткие временные ограничения и ограниченные вычислительные ресурсы встроенных контроллеров требуют применения лёгких криптографических механизмов и оперативных алгоритмов мониторинга, способных функционировать без значительного влияния на производственные процессы.

Таким образом, теоретические основы безопасности КФС формируют каркас для разработки прототипа модуля тестирования безопасности, обеспечивая комплексный подход к оценке и повышению уровня защищённости умного производства.

Архитектура прототипа платформы

Прототип программного обеспечения для тестирования безопасности умного производства спроектирован как модульная система, ориентированная на интеграцию современных инструментов анализа, эксплуатации уязвимостей и генерации отчетов. Архитектура включает три ключевых модуля, взаимодействующих через единый веб-интерфейс и базу данных (БД), что обеспечивает гибкость и масштабируемость для работы с киберфизическими системами (КФС).

Компонент сканирования основан на комбинации инструментов nmap и Nessus API, что позволяет выполнять многоуровневый анализ сети и устройств.

Функции:

1. Автоматическое обнаружение активных хостов, открытых портов и сервисов с использованием nmap с сохранением в БД с привязкой к ID КФС, включая IP, MAC-адреса и ОС устройств.

2. Интеграция с Nessus API для проверки обнаруженных сервисов на наличие известных уязвимостей.

3. Сканирование сети на наличие использования протокола ModBus с дальнейшим чтением регистров PLC и анализа их конфигурации. Выявление аномалий, таких как открытые регистры записи или некорректные настройки доступа.

Компонент интеграции эксплойтов и нагрузочного тестирования объединит готовые эксплойты из Metasploit Framework, Nessus и пользовательские реализации для атак на промышленные протоколы.

Функции:

1. Интеграция Metasploit API для автоматизации эксплуатации уязвимостей.

2. Подключение Nessus для запуска целевых тестов на основе данных сканирования.

3. Использование клиента для протокола ModBus для эмуляции действий устройств удаленного ввода-вывода (Remote I/O), включая чтение/запись регистров, подмену данных датчиков и инициирование аномальных команд.

4. Использование библиотеки для языка программирования Python Scapy для генерации кастомных пакетов, имитирующих легитимный трафик, что позволяет тестировать устойчивость систем к подделке взаимодействия.

5. Применение утилиты hping3 для нагрузки на сетевые узлы и оценки устойчивости инфраструктуры к перегрузкам.

Компонент генерации отчетов обеспечивает автоматизированную обработку данных из базы данных (БД) и формирование файлов по результатам тестирования.

Функции:

1. Группировка результатов по категориям: уязвимости, успешные/неудачные атаки, критичность рисков.

2. Автоматическая генерация файла отчета о проведенных тестированиях.

Диаграмма взаимодействия изображена на рис. 1

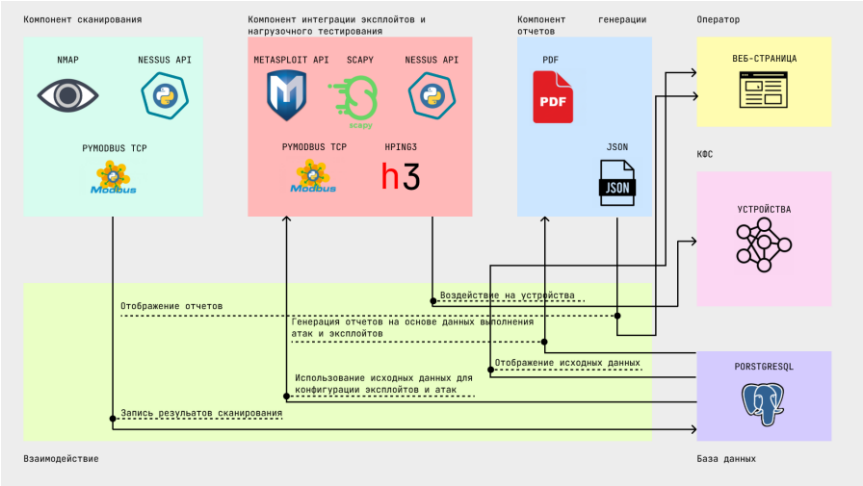


Рис. 1. Диаграмма взаимодействия компонентов модуля

Методология тестирования

В рамках предложенного концепта подразумевается использование открытого программного обеспечения (ПО) для тестирования объектов на безопасность. Используя инструменты в комплексе, получаемые результаты становятся более объективными и в дальнейшем помогают обеспечить сквозную оценку защищённости умного производства.

Для взаимодействия с компонентами КФС используются API инструментов Metasploit, Nessus и nmap, что обеспечивает автоматизацию процессов.

Интеграция nmap позволяет обнаруживать устройства в промышленной сети, включая PLC-контроллеры с открытым портом Modbus-TCP (502). Пример кода для Python [15]:

```
import nmap

scanner = nmap.PortScanner()
scan_result = scanner.scan('192.168.1.0/24',
       arguments='-p 502 --open')
```

```
for host in scanner.all_hosts():
    if scanner[host].has_tcp(502):
        print(f"Обнаружен PLC: {host}, порт 502
        открыт")
```

Эти результаты сохраняются в базу данных и используются как исходные при реализации различных сценариев атак.

Для запуска готового ПО для эксплуатации уязвимостей имеется возможность воспользоваться API Metasploit. Пример запроса к модулю auxiliary/scanner/scada/modbus_banner_grabbing [16]:

```
import requests

# Подключение к Metasploit RPC API
url = "http://localhost:55553/api/"
headers = {"Content-Type": "application/json"}

# Запуск сканирования Modbus
payload = {
    "method": "module.execute",
    "params": ["auxiliary", "scan-
       ner/scada/modbus_banner_grabbing",
       {"RHOSTS": "192.168.1.10"}]
}

response = requests.post(url, json=payload,
       headers=headers)
print("Результат сканирования:", response.json())
```

Интеграция с Nessus выполняется через REST API, что позволяет воспользоваться всеми его возможностями прямо из программного кода на языке программирования (ЯП) Python.

Отчеты необходимо генерировать в двух форматах:

- PDF – для визуализации результатов, предоставляемых оператору;
- JSON – для интеграции с внешними системами моделирования угроз.

Методология тестирования безопасности киберфизических систем (КФС) в рамках предложенного концепта должна базироваться на использовании цифровых двойников – виртуальных копий физических устройств, позволяющих имитировать атаки без остановки реальных производственных процессов. Это особенно актуально для критических инфраструктур, где простои недопустимы. По данным исследования Kaspersky ICS CERT, применение цифровых двойников позволяет проводить тренинги персонала и киберучения, для анализа возможных последствий вы-

явленной атаки и оценки возможного ущерба, в том числе, и прямо в ходе расследования на реальном объекте, пользуясь информацией об обнаруженных деталях атаки [17].

Практическая проверка инструментов: применение и результаты

Рассмотрим инструмент hping3. Он позволяет проводить атаки «отказ в обслуживании» с различными конфигурациями.

PUSH-ACK flood

Команда: sudo hping3 -i u150 -a 192.168.100.201 -PA 192.168.100.202

Сценарий атаки: злоумышленник совершает TCP-flood атаку с установленными флагами PUSH и ACK. Он спуффит IP-адрес SCADA и использует его в качестве источника трафика и отправляет пакеты на PLC контроллер. Злоумышленник атакует 502 порт (ModBus).

Количественный результат повышения входящих пакетов изображен на рис. 2:

Рис. 2. Количество TCP пакетов под воздействием атаки PUSH-ACK flood

ACK flood

Команда: sudo hping3 -q -i u150 -a 192.168.100.201 -A -p 502 192.168.100.202

Сценарий атаки: злоумышленник совершает TCP-flood атаку с установленными флагом ACK. Он спуффит IP-адрес SCADA и использует его в качестве источника трафика и отправляет пакеты на PLC контроллер. Злоумышленник атакует 502 порт (ModBus).

Количественный результат повышения входящих пакетов изображен на рис. 3:

Рис. 3. Количество TCP пакетов под воздействием атаки ACK flood

Рассмотрим атаку, написанную с использованием библиотеки Scapy и языка программирования Python.

Алгоритм генерации и отправки Modbus TCP-пакетов

1. Инициализация параметров:
- source_ip (IP отправителя);
- destination_ip (IP получателя);
- port (502 – порт Modbus);
- num_packets (количество пакетов).

2. Генерация Modbus TCP-пакета
- transaction_id (случайное число);
- protocol_id = 0;
- length = 6;
- unit_id = 1;
- function_code = 6 (запись в регистр);
- register_address = 100;
- register_value (случайное число).

3. Упаковка данных в бинарный формат (PDU + ADU).

4. Формирование и отправка пакетов
- генерация случайного исходного порта;
- сборка TCP-пакета с флагами PA и данными Modbus;
- добавление финального пакета с флагом в заголовке протокола TCP «F»;
- отправка всех пакетов функцией send();

Сценарий атаки: Злоумышленник запускает код на своём компьютере для проведения атаки на сервер Modbus на порту 502. Цель атаки – создать высокую нагрузку на сервер, отправляя большое количество запросов на запись в Modbus-регистр, что может привести к перегрузке сервера и отказу в обслуживании.

Количественный результат повышения входящих пакетов изображен на рис. 4:

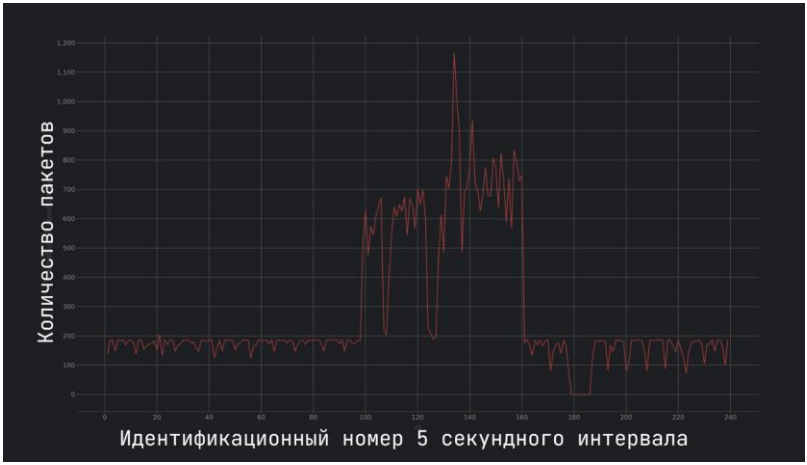


Рис. 4. Количество TCP пакетов под воздействием атаки на протокол ModBus

Вывод

Разработанный концепт модуля тестирования безопасности для умного производства демонстрирует эффективность интеграции открытых инструментов и цифровых двойников в обеспечении безопасности киберфизических систем (КФС). Основной акцент сделан на автоматизации процессов сканирования, эксплуатации уязвимостей и генерации отчетов, что позволяет минимизировать риски остановки реальных производственных процессов.

Практическая значимость концепта подтверждается ГОСТ Р 71576–2024 и стандартом IEC 62443, где указаны требования к безопасности тестируемых систем, что делает его применимым в различных промышленных экосистемах. Однако предложенное решение имеет ограничения, связанные с поддержкой узкого набора протоколов и необходимостью ручной адаптации под специфику оборудования.

Перспективы развития включают:

- расширение поддержки протоколов MQTT и OPC UA;

- внедрение машинного обучения для прогнозирования уязвимостей на основе исторических данных;
- автоматизацию валидации цифровых двойников через интеграцию с системами IoT.

Предложенный подход открывает новые возможности для создания адаптивных систем безопасности, способных противостоять эволюционирующим киберугрозам в условиях цифровой трансформации промышленности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Humayed A., Lin J., Li F., Luo B.* Cyber-Physical Systems Security—A Survey // IEEE Internet of Things Journal. – 2017. – Vol. 4, No 6. – P. 1802-1831. – DOI: 10.1109/jiot.2017.2703172.
2. *Рылов С.* Кибербезопасность промышленной автоматизации [Электронный ресурс]. – [б.г.]. – URL: https://finestart.school/media/cyber_security?ysclid=m9tzzexcfe852411852.
3. *Снегирева Е.* Киберугрозы для промышленности: Industrial IoT [Электронный ресурс]. – 2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberugrozy-dlya-promyshlennosti-industrial-iot/#id1.
4. *Graham M., Ahlers C., O'Meara K.* DRAGOS, INC. Impact of FrostyGoop ICS Malware on Connected OT Systems [Электронный ресурс]. – 2024. – URL: https://regmedia.co.uk/2024/07/23/dragos_frostygoop-report.pdf.
5. Top 15 Best Ethical Hacking Tools – 2025 [Электронный ресурс] // CybersecurityNews. – 2023. – URL: https://cybersecuritynews.com/ethical-hacking-tools/.
6. *Новиков И.* Безопасность киберфизических систем должна стать драйвером развития ИБ [Электронный ресурс]. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Physical-Systems-Security.
7. ГОСТ Р 71576–2024. Системы киберфизические. Общие положения [Текст]. – Введ. 2025-01-01. – М.: Стандартинформ, 2024. – 8 с.
8. *Макаренко С.И., Смирнов Г.Е.* Анализ стандартов и методик тестирования на проникновение // Системы управления, связи и безопасности. – 2020. – № 4. – С. 44-71. – DOI: 10.24411/2410-9916-2020-10402.
9. OSWAP Testing Guide. Version 4. – 2014. – URL: https://www.owasp.org/index.php/OWASP_Testing_Project.
10. *Оррей К.* Penetration Test Framework. Vulnerability Assessment [Электронный ресурс]. – 2014. – URL: http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html.
11. ISSAF - Information System Security Assessment Framework [Электронный ресурс]. – 2006. – URL: http://www.oissg.org/issaf02/issaf0.1-5.pdf.
12. PTES – The Penetration Testing Execution Standard [Электронный ресурс]. – 2012. – URL: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines.
13. *Херцог П.* OSSTMM – The Open Source Security Testing Methodology Manual [Электронный ресурс]. – Нью-Йорк, 2006. – 129 с. – URL: https://www.isecom.org/OSSTMM.3.pdf.

14. NIST Special Publications 800-115. Technical Guide to Information Security Testing and Assessment [Электронный ресурс]. – США, Гейтерсбург, 2008. – 80 с. – URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.
15. Nmap Python Documentation [Электронный ресурс]. – URL: https://xael.org/pages/python-nmap-en.html.
16. Metasploit RPC API Guide [Электронный ресурс]. – URL: https://docs.rapid7.com/metasploit/rpc-api.
17. Kaspersky ICS CERT. Цифровые двойники в промышленной безопасности [Электронный ресурс]. – 2023. – URL: https://ics-cert.kaspersky.ru/media/Kaspersky-ICS-CERT-Digital-twins-and-ensuring-the-cybersecurity-of-enterprises-Oil-and-gas-industry-Ru.pdf.

УДК 004.77

К.С. Дунюшкина, И.В. Машкина

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ЗАЩИЩЕННОСТИ СРЕДИ ГИПЕРВИЗОРНОЙ ВИРТУАЛИЗАЦИИ

В статье рассматривается актуальная проблема обеспечения информационной безопасности в условиях виртуализации корпоративных инфраструктур. Представлена комплексная модель защиты виртуальной инфраструктуры, основанная на принципах многоуровневой безопасности и учитывающая специфику современных угроз. Описаны ключевые компоненты модели, включающие системы идентификации и управления доступом, механизмы сегментации сети, средства шифрования данных, антивирусной защиты и резервного копирования. Особое внимание уделено вопросам мониторинга безопасности и регулярного аудита защищенности виртуальной инфраструктуры. Практическая значимость работы заключается в возможности применения предложенной модели для защиты виртуальных сред с учетом требований регуляторов в области информационной безопасности. Представлены рекомендации по внедрению защитных мер. Результаты исследования могут быть использованы администраторами безопасности, специалистами по информационной безопасности и IT-специалистами при проектировании и внедрении систем защиты виртуальной инфраструктуры в организациях различного масштаба.

Ключевые слова: *виртуальная инфраструктура, информационная безопасность, модель защиты, гипервизор, виртуальные машины, система защиты виртуальной инфраструктуры, мониторинг безопасности, аудит безопасности.*

The article considers the urgent problem of ensuring information security in the context of virtualization of corporate infrastructures. A comprehensive model of virtual infrastructure protection based on the principles of multi-level security and taking into account the specifics of modern threats is presented. The key components of the model are described, including identification and access control systems, network segmentation mechanisms, data encryption tools, anti-virus protection and backup. Particular attention is paid to the issues of security monitoring and regular audit of the security of the virtual infrastructure. The practical significance of the work lies in the possibility of using the proposed model to protect virtual environments taking into account the requirements of regulators in the field of information security. Recommendations for the implementation of protective measures are presented. The results of the study can be used by security administrators, information security specialists and IT specialists in the design and implementation of virtual infrastructure protection systems in organizations of various sizes.

Keywords: *virtual infrastructure, information security, protection model, hypervisor, virtual machines, virtual infrastructure protection system, security monitoring, security audit.*

Введение

В эпоху стремительного развития информационных технологий виртуализация заняла центральное место в IT-инфраструктуре современных организаций. Создавая эффективные решения для использования средств виртуализации и повышения масштабируемости систем, она одновременно выдвигает серьезные требования к обеспечению информационной безопасности.

С ростом популярности виртуальных платформ увеличивается и количество целенаправленных атак на их компоненты. Киберпреступники активно ищут уязвимости в гипервизорах, виртуальных машинах и системах управления, стремясь получить несанкционированный доступ или украсть конфиденциальные данные. Особенности виртуализации, такие как динамическая миграция виртуальных машин (ВМ) и совместное использование ресурсов, создают новые векторы атак, требующие особого внимания при разработке защитных мер.

Спектр угроз для виртуальной инфраструктуры включает различные аспекты: от компрометации гипервизоров до утечек данных между виртуальными машинами. Последствия успешной реализации таких атак могут быть разрушительными для бизнеса, включая значительные финансовые потери и репутационный ущерб.

В контексте цифровой трансформации бизнеса безопасность виртуализированных систем приобретает решающее значение. Предлагаемая модель защиты призвана стать надежным инструментом для минимизации рисков и обеспечения устойчивости IT-инфраструктуры перед лицом постоянно эволюционирующих угроз [1].

Основная часть

Виртуальная инфраструктура, объединяя программные и аппаратные компоненты для создания и управления виртуальными средами, стала краеугольным камнем современных IT-систем, обеспечивая организациям гибкость управления ресурсами и оптимизацию затрат.

Виртуальная инфраструктура включает несколько ключевых компонентов:

- гипервизор – это ключевой компонент виртуальной инфраструктуры, который обеспечивает создание, управление и изоляцию ВМ. Гипервизоры делятся на два типа: первого типа (bare-metal) работают непосредственно на аппаратном обеспечении (VMware ESXi, Microsoft Hyper-V, Xen), второго типа (hosted): работают поверх операционной системы (Oracle VirtualBox, VMware Workstation);

- виртуальные машины (ВМ) – изолированные среды, которые эмулируют работу физических серверов, каждая ВМ может иметь свою операционную систему и приложения;
- виртуальные хранилища включающее в себя ресурсы для хранения данных, которые могут быть динамически распределены между виртуальными машинами;
- системы управления – платформы для централизованного управления виртуальной инфраструктурой (например, VMware vCenter, Microsoft System Center) [2].

Виртуализация предоставляет ряд уникальных возможностей, которые отличают ее от традиционных физических инфраструктур:

- динамическая миграция ВМ – возможность перемещения виртуальных машин между физическими серверами без остановки их работы (например, vMotion в VMware);
- высокая плотность размещения, когда на одном физическом сервере может быть запущено множество виртуальных машин, что позволяет эффективно использовать ресурсы.
- Возможность быстрого развертывания, когда для создания новых ВМ требуется значительно меньше времени по сравнению с установкой физических серверов.

К преимуществам использования гипервизорной виртуализации (ГВ) можно отнести экономию ресурсов, поскольку виртуализация позволяет сократить количество физических серверов, что снижает затраты на оборудование и энергопотребление, гибкость и масштабируемость, поскольку ресурсы могут быть быстро перераспределены в зависимости от текущих потребностей. Также к преимуществам относится упрощение управления, благодаря возможности централизованного управления, позволяющего администраторам контролировать всю инфраструктуру из одной точки и повышение отказоустойчивости при использовании технологии, такие как live migration и репликация ВМ, что обеспечивает высокую доступность сервисов.

Поскольку виртуальная инфраструктура стала неотъемлемой частью современных IT-ландшафтов, предоставляя организациям значительные преимущества. Однако ее использование требует тщательного подхода к обеспечению безопасности, так как специфика виртуализации создает уникальные риски, которые необходимо учитывать при построении системы защиты.

Возможные риски использования ГВ:

- компрометация гипервизора в результате эксплуатации уязвимостей, что может привести к нарушению работы всех виртуальных машин, которые он обслуживает;

- утечки данных через общие ресурсы (например, память или процессор);
- некорректная конфигурация из-за ошибок, допущенных при настройке или при разработке правил политики разграничения доступа [3].

Таким образом, виртуальная инфраструктура, несмотря на свои преимущества, подвержена ряду специфических угроз и рисков, которые могут привести к серьезным последствиям, включая утечку данных, нарушение работы сервисов и финансовые потери. Рассмотрим основные угрозы и риски, связанные с виртуальными средами.

Поскольку гипервизор контролирует все виртуальные машины, работающие на физическом сервере, его компрометация может привести к катастрофическим последствиям для всей виртуальной среды. Атаки на гипервизоры представляют собой одну из наиболее серьезных угроз для виртуальной инфраструктуры. В табл. 1 представлены основные типы атак на гипервизоры, их механизмы и последствия [4].

Таблица 1

Основные типы атак на гипервизоры, их механизмы и последствия

Тип Атаки	Механизмы	Пример уязвимость	Последствия
Атаки через управляющую систему	1. Ошибка в коде. 2. Неправильная конфигурация. 3. Недостатки в архитектуре.	1. CVE-2021-21972 – уязвимость в VMware vCenter Server, позволяющая удаленно выполнить код. 2. CVE-2018-3646 – уязвимость в гипервизорах, связанная с аппаратными особенностями процессоров (Spectre и Meltdown).	1. Получение контроля над гипервизором. 2. Доступ ко всем виртуальным машинам, управляемым гипервизором. 3. Возможность создания, удаления или изменения виртуальных машин.
Атаки типа «виртуальный побег» (VM Escape)	1. Злоумышленник эксплуатирует уязвимости в изоляции виртуальных машин. 2. Используются ошибки в коде гипервизора или аппаратные уязвимости (например, Spectre и Meltdown). 3. Атака может быть выполнена через вредоносное ПО, установленное на виртуальной машине.	1. Venom (CVE-2015-3456) – уязвимость в виртуальном Floppy Disk Controller, позволяющая выполнить VM Escape. 2. CloudBurst – эксплойт для VMware ESX/ESXi, позволяющий получить доступ к гипервизору.	1. Полный контроль над гипервизором и всеми виртуальными машинами. 2. Возможность кражи данных, установки вредоносного ПО или нарушения работы инфраструктуры.

Окончание табл. 1

Тип Атаки	Механизмы	Пример уязвимость	Последствия
Атаки через аппаратные уязвимости	1. Злоумышленник использует аппаратные уязвимости для обхода изоляции виртуальных машин. 2. Атака может быть выполнена из виртуальной машины для получения доступа к данным других ВМ или гипервизора.	1. Spectre и Meltdown – уязвимости, связанные с спекулятивным выполнением команд в процессорах. 2. Foreshadow (L1TF) – уязвимость, позволяющая получить доступ к данным в кэше процессора.	1. Утечка данных между виртуальными машинами. 2. Получение контроля над гипервизором.
Атаки через виртуальные устройства	1. Злоумышленник эксплуатирует уязвимости в виртуальных устройствах для получения доступа к гипервизору. 2. Пример: атака через виртуальный сетевой интерфейс для перехвата трафика или выполнения кода на уровне гипервизора.	1. VENOM (CVE-2015-3456) – уязвимость в виртуальном Floppy Disk Controller. 2. Атаки на виртуальные сетевые устройства: использование уязвимостей в виртуальных коммутаторах или маршрутизаторах	1. Получение контроля над гипервизором. 2. Утечка данных или нарушение работы виртуальной инфраструктуры.

Для обеспечения безопасности гипервизорной виртуализации необходимо внедрить комплексную модель защиты, которая включает несколько ключевых компонентов. Эти компоненты охватывают аспекты безопасности, начиная от защиты самого гипервизора и заканчивая мониторингом и управлением доступом. Рассмотрим каждый из них подробнее [5].

Таблица 2

Механизмы обеспечения безопасности виртуальной инфраструктуры [6]

Компонент ВИ	Меры защиты	Реализация мер	Идентификатор ФСТЭК
Гипервизор	1. Изоляция гипервизора	• Запуск на выделенном сервере без дополнительных сервисов. • Минимизация установленного ПО (только необходимые компоненты).	ЗВС.1 ЗВС.2 ЗВС.7
	2. Контроль доступа	• Использование многофакторной аутентификации (MFA) для администраторов. • Ролевое управление доступом (RBAC) с минимальными привилегиями.	ЗВС.1 ЗВС.2 ЗВС.4 ЗВС.6 ЗВС.7

	3. Защита от атак	• Аппаратные технологии безопасности (Intel VT-d, AMD-Vi для изоляции DMA). • Защита от • Spectre/Meltdown (обновление микрокода CPU).	ЗВС.3 ЗВС.5 ЗВС.9
	4. Мониторинг и аудит	• Логирование всех действий администраторов. • Использование SIEM-систем для анализа событий безопасности.	ЗВС.3 ЗВС.1 ЗВС.2
	5. Обновления и исправления	• Регулярное обновление гипервизора (ESXi, Hyper-V, KVM). • Отключение ненужных функций (например, USB-портов).	ЗВС.8 ЗВС.9
Виртуальная машина	1. Изоляция ВМ	• Запрет взаимодействия между ВМ, если это не требуется (vLAN, микросегментация). • Использование Trusted Platform Module (vTPM) для защиты загрузки.	ЗВС.7
	2. Контроль целостности	• Шифрование дисков ВМ (BitLocker, LUKS, VMware VM Encryption). • Проверка цифровых подписей образов перед запуском.	ЗВС.1 ЗВС.2 ЗВС.4 ЗВС.6 ЗВС.7
	3. Защита от НСД	• Отключение ненужных сервисов (CD-ROM, USB). • Ограничение доступа к консоли ВМ.	ЗВС.3 ЗВС.5 ЗВС.9
	4. Резервное копирование и восстановление	• Регулярные снепшоты и резервные копии (Veeam, Zerto). • Защита снепшотов от модификации (WORM-хранилища).	ЗВС.8
Виртуальные сетевые устройства	1. Сегментация сети	• Использование микросегментации (VMware NSX, Cisco ACI). • Изоляция окружений (Dev/Test/Prod) через VLAN/VXLAN.	ЗВС.1 ЗВС.2 ЗВС.10
	2. Шифрование трафика	• VPN между ВМ (IPsec, WireGuard). • TLS для служебного трафика (API, управление).	ЗВС.4 ЗВС.6 ЗВС.9

	3. Защита от сетевых атак	• Виртуальные фаерволы (VMware Distributed Firewall, Palo Alto VM-Series). • IDS/IPS на уровне гипервизора (Suricata, Snort).	ЗВС.4 ЗВС.5 ЗВС.6 ЗВС.7
	4. Контроль доступа	• NAC (Network Access Control) для виртуальных портов. • Запрет promiscuous mode на виртуальных NIC.	ЗВС.1 ЗВС.2 ЗВС.4 ЗВС.6 ЗВС.7
Система управления гипервизорами (vCenter, SCVMM, OpenStack)	1. Аутентификация и авторизация	• Интеграция с LDAP/Active Directory + MFA. • Минимальные привилегии для ролей (например, «только просмотр»).	ЗВС.1 ЗВС.2
	2. Шифрование данных	• TLS 1.2/1.3 для всех API и веб-интерфейсов. • Шифрование баз данных (SQL TDE, PostgreSQL pgcrypto).	ЗВС.4 ЗВС.6 ЗВС.9
	3. Резервирование и мониторинг	• Кластерная настройка (vCenter HA). • Аудит изменений (кто, когда и что изменил).	ЗВС.3 ЗВС.4 ЗВС.5 ЗВС.6 ЗВС.7
	4. Физическая защита	• Размещение системы управления в защищенном сегменте сети (DMZ).	ЗВС.9
Устройства хранения (SAN, NAS, vSAN, Ceph)	1. Шифрование данных	• Шифрование «на лету» (VMware vSAN Encryption, BitLocker). • Шифрование «в покое» (Self-Encrypting Drives – SED).	ЗВС.4 ЗВС.6 ЗВС.9
	2. Контроль доступа	• iSCSI CHAP-аутентификация. • Zoning в Fibre Channel (изоляция LUN).	ЗВС.1 ЗВС.2 ЗВС.4 ЗВС.6 ЗВС.7
	3. Резервное копирование	• 3-2-1 правило (3 копии, 2 типа носителей, 1 оффлайн). • Защита от ransomware (иммутабельные бэкапы).	ЗВС.8
	4. Мониторинг целостности	• Проверка контрольных сумм (ZFS, RAID с контролем ошибок). • Защита от удаления (retention policies, WORM).	ЗВС.1 ЗВС.2 ЗВС.3 ЗВС.7 ЗВС.10

Подводя итоги, можно сказать, что гипервизоры подвержены множеству угроз, которые могут привести к серьезным последствиям, включая утечку данных, нарушение работы сервисов и финансовые потери. Для защиты гипервизоров необходимо внедрять комплексные меры, включая регулярное обновление, мониторинг безопасности и обучение персонала [7].

Модель защиты виртуальной инфраструктуры для уязвимости CVE-2021-21985 (VMware vCenter Server).

Описание уязвимости:

Уязвимость CVE-2021-21985 в VMware vCenter Server связана с удаленным выполнением кода (RCE) через плагин виртуальной SAN (vSAN). Злоумышленник может использовать эту уязвимость для выполнения произвольного кода на сервере vCenter, что может привести к полной компрометации виртуальной инфраструктуры.

Модель защиты

Первый этап включает в себя идентификацию уязвимых систем, для этого необходимо провести Проверку всех экземпляров VMware vCenter Server на наличие уязвимой версии (6.5, 6.7, 7.0), а так же использовать инструменты сканирования уязвимостей (например, Nessus, OpenVAS) для подтверждения наличия уязвимости.

После этого необходимо провести оценку рисков, то есть определить критичность уязвимости для бизнеса (например, возможность полной компрометации инфраструктуры), а так же провести приоритизация обновления или применения временных мер защиты.

Второй этап включает в себя временные меры защиты, а именно: отключение плагина vSAN, если плагин vSAN не используется, его можно отключить для устранения уязвимости. Ограничение доступа к vCenter Server – настройка firewall для ограничения доступа к vCenter Server только с доверенных IP-адресов.

На рис. 1 представлен пример правил для iptables:

```bash
iptables -A INPUT -p tcp --dport 443 -s <trusted_ip> -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j DROP
```

Рис. 1. Пример правил для iptables

Мониторинг подозрительной активности – настройка SIEM-системы (например, Splunk, IBM QRadar) для отслеживания попыток эксплуатации уязвимости. Пример правил для обнаружения: попытки доступа к /ui/vsanui/rest/proxy/service/. * с подозрительных IP-адресов.

Третий этап – это установка последних обновлений для VMware vCenter Server, устраняющих уязвимость, а также проверка успешности обновления: повторное сканирование уязвимостей для подтверждения устранения CVE-2021-21985.

Четвертый этап - усиление защиты, а именно применение многофакторной аутентификации (MFA), настройка MFA для доступа к vCenter Server через интеграцию с решениями, такими как RSA SecurID или Duo Security. Применение шифрование трафика - настройка TLS для всех соединений с vCenter Server. В этом же этапе можно произвести сегментацию сети, то есть разделить виртуальные сети на изолированные сегменты (например, для управления, хранения данных и пользовательских ВМ).

Пятый этап это настройка SIEM-системы: интеграция vCenter Server с SIEM для сбора и анализа логов. Пример правил для обнаружения аномалий:

1. Попытки доступа к отключенному плагину vSAN.

2. Подозрительные действия администраторов (например, создание новых пользователей).

План реагирования на инциденты: разработка сценариев реагирования на попытки эксплуатации уязвимости. Пример сценария:

1. Блокировка IP-адреса злоумышленника через firewall.

2. Проверка логов на предмет компрометации других систем.

3. Уведомление ответственных лиц и проведение расследования.

Шестой этап это обучение персонала, он включает: обучение администраторов, то есть проведение тренингов по безопасной настройке и эксплуатации vCenter Server, повышение осведомленности пользователей, то есть обучение пользователей виртуальных машин по вопросам безопасности (например, использование стойких паролей, предотвращение фишинга).

Результаты внедрения модели – устранение уязвимости CVE-2021-21985:

- установка обновлений и отключение плагина vSAN устраняет возможность эксплуатации уязвимости;
- повышение уровня безопасности: внедрение MFA, шифрование трафика и сегментация сети снижают риски компрометации;
- оперативное реагирование на инциденты: настройка SIEM и разработка плана реагирования позволяют быстро выявлять и устранять угрозы.

Предложенная модель защиты виртуальной инфраструктуры для уязвимости CVE-2021-21985 включает временные меры, устранение уязвимости, усиление защиты и обучение персонала. Такой подход позволяет не только устранить конкретную уязвимость, но и повысить общий уровень безопасности виртуальной инфраструктуры. Регулярный аудит и обновление мер защиты обеспечивают устойчивость к новым угрозам [8].

Заключение

В результате проведенного исследования разработана комплексная модель защиты виртуальной инфраструктуры, учитывающая современные вызовы информационной безопасности. Модель базируется на принципах многоуровневой защиты, включающей как технологические, так и организационные меры безопасности.

Дальнейшее развитие модели предполагает интеграцию передовых технологий защиты, таких как искусственный интеллект для анализа угроз и автоматизированного реагирования на инциденты безопасности. Также планируется расширение функционала для поддержки новых сценариев использования виртуальной инфраструктуры.

Таким образом, предложенная модель представляет собой эффективный инструмент для обеспечения безопасности виртуальной инфраструктуры в современных условиях, сочетающий проверенные практики и инновационные подходы к защите информации [9].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Гринь В.С.* Анализ угроз информационной безопасности и каналов утечки информации // Научно-образовательный журнал для студентов и преподавателей «StudNet». – 2021. – № 7. – с. 1616-1620.
2. *Афонин Д.Н.* Виртуализация, классификация и области применения в ФТС России. Возможности виртуализации. Системы и среды виртуализации // Санкт-Петербургский имени В.Б. Бобкова филиал Российской таможенной академии – Москва, Общество с ограниченной ответственностью «Русайнс». – 2024. – С. 104.
3. *Пепп М.А.* Анализ угроз информационной безопасности при использовании технологии виртуализации // «Научный аспект № 5 – 2024» – Информ. Технологии // Научно-издательский центр Аспект. – 2024. – С. 86.
4. *Окунев Б.В., Лазарев А.И., Харламов П.С.* Виртуализация контейнера тестирования уязвимостей информационных объектов на основе технологии DEX и нейронных сетей глубокого обучения // Филиал Федерального государственного бюджетного образовательного учреждения высшего образования «Национальный исследовательский университет «МЭИ»» в г. Смоленске, Смоленск, Россия. – 2021. – Т. 16, № 4 (94). – С. 96-109.
5. *Mining E.* Kali Linux Hacking: A complete step by step guide to learn the fundamentals of cyber security, hacking, and penetration testing. Includes valuable basic networking concepts. Independently published, 2019. – 175 p.
6. *Sviridova E.A., sviridov A.N., demkin V.I.* Algorithm of interaction data center cooling systems and virtualization platforms for implementing preventive temperature management / National Research University of Electronic Technology // SCIENCE PROSPECTS. – 2023. – No. 11 (170). – C 54-58.
7. *Штеренберг С.И., Москальчук А.И., Красов А.В*. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения // Информационные технологии и телекоммуникации/Т. – 2021. – Т. 9. – С. 1-2.

8. *Николаев А.А., Горященко И.С., Ивановский А.А., Истомина И.А.* Современные технологии на службе УИС: преимущества контейнерной виртуализации на примере Docker // Информационные технологии в УИС. – 2021. – № 3. – С. 31-47.
9. *Щеголькова А.А., Лещенко К.Д.* виртуализация контейнеров: революция в развертывании и управлении программным обеспечением // Кубанский государственный аграрный университет им. И.Т. Трубилина, г. Краснодар, Российская Федерация: THEORY AND PRACTICE OF MODERN SCIENCE: THE VIEW OF YOUTH Proceedings of the III all-Russian scientific and practical conference in English. In 2 parts. Санкт-Петербург, 2024. – С. 257-261.

УДК 004.94

С.А. Елизарова

Волгоградский государственный университет, Россия, г. Волгоград

МОДЕЛЬ АНАЛИЗА ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Целью работы является выявление аномального поведения пользователей в информационных системах. Для достижения цели рассматриваются современные подходы к обеспечению информационной безопасности, уделяя особое внимание угрозам, связанным с человеческим фактором. Проанализированы методы выявления аномального поведения пользователей в информационных системах, а также источники данных, используемые для этого. Приведены классификации алгоритмов анализа поведения, их сравнительный анализ и выбор наиболее эффективного метода. Разработаны функциональная модель, архитектура и пользовательский интерфейс модели. Приведены результаты экспериментальных исследований с разработанной моделью.

Ключевые слова: *информационная безопасность, анализ поведения пользователей, аномалии в поведении пользователей, машинное обучение, алгоритмы анализа, человеческий фактор.*

The aim of this work is to identify anomalous user behavior in information systems. To achieve this goal, modern approaches to ensuring information security are examined, with a particular focus on threats related to the human factor. Methods for detecting anomalous user behavior in information systems, as well as the data sources used for this purpose, are analyzed. Classifications of behavior analysis algorithms are provided, along with a comparative analysis and the selection of the most effective method. A functional model, architecture, and user interface for the model are developed. The results of experimental studies using the developed model are presented.

Keywords: *information security, user behavior analysis, anomalous user behavior, machine learning, analysis algorithms, human factor.*

В современных условиях подходы к обеспечению информационной безопасности постоянно эволюционируют. Несмотря на активное внедрение технических средств защиты, многие организации недостаточно уделяют внимания утечкам информации, вызванным человеческим фактором. Такие утечки могут быть как непреднамеренными (ошибки пользователей, приводящие к изменению или потере данных), так и преднамеренными (действия, направленные на хищение информации).

Для эффективного противодействия угрозам, связанным с человеческим фактором, необходимо комбинировать организационные и технические меры защиты. Одним из актуальных подходов является анализ поведения пользователей, который позволяет выявлять аномалии в их действиях и своевременно предотвращать утечки информации, вызванные внутренними нарушителями.

Согласно статистике утечек конфиденциальных данных за третий квартал 2024 года, представленной компанией Positive Technologies, наиболее часто компрометируются данные коммерческой тайны (24%), персональные данные (23%), учетные данные (23%), данные платежных карт (7%), переписки (6%) и медицинская информация (3%). Эти данные подчеркивают важность разработки и внедрения методов, направленных на минимизацию рисков, связанных с человеческим фактором [1].

Анализ поведения пользователей в информационной системе – это комплекс действий по сбору данных о конкретных действиях пользователей при использовании компьютерной инфраструктуры, включая последующую их обработку для выявления закономерностей взаимодействий с различными приложениями, интернет-порталами, и сервисными ресурсами. Данный подход предусматривает следующие этапы работы:

1. Сбор и обработка данных о действиях пользователя.
2. Выявление паттернов и трендов в поведении.
3. Оценку эффективности интерфейса и функционирования системы.
4. Идентификацию проблем и слабых мест в пользовательских действиях.

Для анализа поведения пользователей чаще всего используются наборы данных, которые делятся на две категории: внутренние и внешние.

Внутренние данные включают:

1. Логи. В них содержится информация о действиях пользователей, такие как включение и выключение системы, успешные и неудачные попытки входа, установка, удаление и обновление программного обеспечения или драйверов, ошибки в работе приложений, проблемы с носителями информации, а также их подключение и отключение.

2. Сетевые данные (трафик). Сбор информации о передаче данных между пользователями и сервером через мониторинг сетевого трафика (например, с помощью Wireshark или NetFlow). Это позволяет анализировать поведение пользователей в режиме реального времени.

3. Базы данных. Данные о действиях пользователей при взаимодействии с базой данных, включая количество запросов, время их выполнения, ошибки и внесенные изменения.

4. Файлы cookie и данные сессий. Эти данные помогают отслеживать пользователей между посещениями, анализировать их предпочтения и поведение на различных страницах системы.

Внешние данные включают:

1. Системы аналитики: Такие инструменты, как Google Analytics и Yandex.Metrica, собирают данные о посещениях веб-страниц, действиях пользователей (клики, скроллинг, время на странице) и их демографических характеристиках (география, устройства, браузеры). Эти данные полезны для анализа поведения и предпочтений пользователей.

2. Инструменты отслеживания действий (heatmaps, session replay): Сервисы вроде Hotjar, Crazy Egg и Mouseflow фиксируют движения мыши, клики, скроллинг и записывают сессии пользователей, что позволяет детально анализировать их взаимодействие с интерфейсом.

3. Социальные сети и отзывы: Информация из социальных сетей, форумов или чатов, где пользователи оставляют отзывы или обсуждают продукт, также может быть использована для анализа поведения.

4. Ручной ввод и формы: Данные, введенные пользователями в формы, анкеты или другие интерфейсы (например, данные о покупках, поисковых запросах или регистрациях), представляют ценность для анализа.

5. Обратная связь от пользователей: Данные, полученные через опросы, анкеты, системы отзывов и оценок, помогают понять намерения и предпочтения пользователей.

Также стоит определить источники данных в информационных системах, которые способствуют выявить аномалии в поведении пользователей, такими источниками чаще всего являются журналы событий (табл. 1).

Таблица 1

Источники данных в ИС

Название источника	**Информация в источнике**	**Что позволяет выявить**
1	2	3
Журнал приложений	Информация о событиях, связанных с приложениями, установленными в системе	Позволяет выявить действия пользователя, которые привели к ошибке в работе приложений
Журнал безопасности	Информация о безопасности системы	Позволяет выявить такие действия пользователя, как вход в систему, неудачные попытки входа в систему, изменения прав доступа

Окончание табл. 1

Журнал системных событий	Информация о событиях, связанных с работой операционной системы	Позволяет выявить действия пользователей о запуске и выключении компьютера, отключении служб и т.д.
Журнал установки	Информация о процессах установки, удаления и обновлении программного обеспечения	Позволяет выявить действия пользователя связанные с установкой, удалением и обновлением программного обеспечения и драйверов
Журнал событий оборудования	Информация о событиях, связанных с аппаратным обеспечением компьютера	Позволяет выявить действия пользователя, связанные с подключением и отключением носителей информации, об ошибках в работе носителей информации и в отказах работы устройств

Стоит отметить, что данные журналы можно отнести к группе внутренних наборов данных для анализа поведения пользователей, а точнее к лог-файлам, данный набор зачастую используется для выявления аномалий в поведении пользователя, исходя из этого в разрабатываемом программном комплексе для выявления аномалий в поведении пользователей будут использоваться лог-файлы (журналы событий).

Существуют также признаки аномального поведения пользователя в информационной системе, которые могут свидетельствовать о попытке злоупотребления правами доступа, нарушении безопасности данных или намерении совершить противоправные действия, такими признаками могут быть:

1. Необычные или неожиданные действия. Пользователь начинает выполнять операции, которые выходят за рамки его обычной деятельности, например, доступ к данным, к которым он не должен иметь доступ. Частое или неожиданное изменение настроек системы, паролей, прав доступа или конфиденциальных данных.

2. Попытки обхода системы безопасности. Использование устаревших паролей или попытки использовать слабые или угаданные пароли. Попытки отключения систем защиты, таких как антивирус, файрволы или системы мониторинга.

3. Необычные логин-активности. Частые неудачные попытки входа в систему с различных устройств или IP-адресов.

4. Невозможность или отказ от выполнения нормальных процедур. Игнорирование предписанных процедур безопасности или отказ от их выполнения.

5. Подозрительные сообщения или запросы. Пользователь может задавать странные или подозрительные вопросы относительно системы или информации, которая может быть использована для взлома.

6. Повторяющиеся ошибки или сбои. Постоянные ошибки в работе с системой, особенно если они связаны с обходом проверок безопасности или попытками получить несанкционированный доступ.

7. Чрезмерное использование системных ресурсов. Необычное повышение нагрузки на серверы или сети, что может указывать на запуск вредоносных программ или попытки провести атаку.

8. Скачивание и загрузка подозрительных файлов. Загрузка или запуск неизвестных или подозрительных программ, файлов или скриптов, которые могут быть связаны с вредоносной активностью.

9. Перемещение данных без видимой причины. Перемещение больших объемов данных или их копирование в места, которые не соответствуют нормальной бизнес-практике (например, на внешние носители или в облачные сервисы).

10. Использование несанкционированных устройств. Подключение сторонних устройств (например, USB-накопителей, мобильных телефонов) к рабочим компьютерам, что может быть способом скрытого сбора данных.

Опираясь на типы обрабатываемых данных для выявления аномалий в поведении пользователя, можно составить их взаимосвязь с признаками аномального поведения пользователя в информационной системе, которая представлена в табл. 2.

Таблица 2

Взаимосвязь признаков и анализируемых данных

Признак	**Анализируемые данные**
1	2
Необычные или неожиданные действия	Для выявления указанных действий, анализируются данные с журнала безопасности
Необычные логин-активности	Для выявления необычной активности, анализируются данные с журнала безопасности и журнала системных событий
Повторяющиеся ошибки или сбои	Для выявления ошибок, связанных с работой системы, анализируются данные с журнала приложений
Скачивание и загрузка подозрительных файлов	Для выявления скачивания и установки подозрительных файлов, анализируются данные с журнала установки
Использование несанкционированных устройств	Для выявления несанкционированных устройств, анализируются данные с журнала событий оборудования

Таким образом, исходя из связи, представленной в табл. 2, между признаками и анализируемыми данными для выявления аномалий в поведении пользователей, определены признаки, которые будет учитывать разрабатываемый программный комплекс.

Далее рассмотрим методы анализа поведения пользователя в информационной системе и определим наиболее лучший.

Существуют несколько основных методов, которые используются для выявления аномалий в поведении пользователя.

Анализ аномалий используется для выявления отклонений от нормального поведения пользователей и включает следующие основные методы:

1. Анализ аномалий.
2. Анализ последовательности событий.
3. Методы классификации.
4. Анализ сетевых взаимодействий.
5. Методы анализа текста и действий.
6. Методы анализа с использованием нейросетей.

Наиболее эффективные методы часто комбинируют несколько подходов, чтобы создать комплексную систему защиты, способную обнаруживать как простые аномалии, так и более сложные, скрытые угрозы.

Чтобы определить наиболее лучший метод анализа поведения пользователя, необходимо определить критерии для их сравнения. Данные критерии представлены в табл. 3.

Таблица 3

Критерии для сравнения методов анализа поведения пользователей в ИС

Обозначение критерия	**Название**	**Описание**	**Возможное значение**
2	3	4	5
К1	Точность результатов	Оценка способности алгоритма выявлять аномалии или правильно классифицировать поведение пользователя	Высокая, Низкая
К2	Сложность реализации	Легкость внедрения алгоритма в существующую инфраструктуру	Высокая, Низкая
К3	Адаптивность	Способность алгоритма адаптироваться к изменению поведения пользователей со временем	Высокая, Средняя, Низкая
К4	Время обучения	Время, необходимое для первоначального обучения модели, особенно для методов, использующих машинное обучение	Высокая, Низкая
К5	Полнота анализа	Способность алгоритма учитывать различные аспекты поведения пользователей и их взаимодействия с системой	Высокая, Низкая

В таблице, показатели возможных значений равны: высокая – 0, средняя – 0.5, низкая – 1.

Для сравнительного анализа используется метод евклидова расстояния. Для расчета создадим таблицу соответствия алгоритмов анализа поведения пользователя заданным критериям и для каждого из них вычислим значения по формуле 1.

$$E = \sqrt{(1 - К1)^2 + (1 - К2)^2 + (1 - К3)^2 + (1 - К4)^2 + (1 - К5)^2} \quad (1)$$

Таблица 4

Значение и оценки методов анализа поведения пользователей

№ метода анализа	Метод анализа	Критерии					Результат
1	2	3					4
		К1	К2	К3	К4	К5	
1	Анализ аномалий	1	1	1	0	0	1,41
2	Анализ последовательности событий	1	1	1	1	1	0
3	Методы классификации	0	0	0	0	0	2,24
4	Анализ сетевых взаимодействий	0	0	0,5	0	0	2,06
5	Методы анализа текста и действий	0	0	0,5	0	0	2,06
6	Методы анализа с использованием нейросетей	1	0	1	0	0	1,73

После вычисления расстояний для всех методов нужно сравнить их значения. Здесь меньшее значение расстояния указывает на более эффективную работу методов анализа поведения пользователей.

Исходя из полученных результатов, мы можем сделать вывод о том, что анализ последовательности событий является самым эффективным методом анализа поведения пользователей в ИС из рассматриваемых вариантов.

Контекстная IDEF0-диаграмма процесса выявления аномалий в поведении пользователя представляет функциональный блок, на который воздействуют:

1. Входные данные – журнал событий, установленное ПО, подключенные устройства.
2. Управляющая информация – нормативно-правовые акты.

3. Механизмы, необходимые для произведения данного процесса – программный комплекс и пользователь.
4. Выходной результат – выявленные аномалии в поведении пользователя.

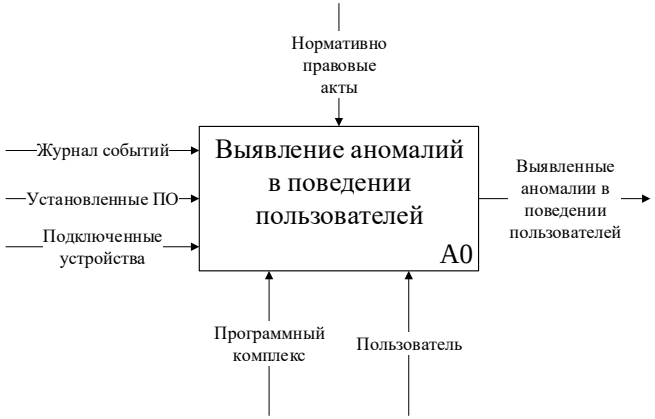


Рис. 2. Функциональная модель программного комплекса выявления аномалий в поведении пользователей

Декомпозиция функционального блока представлена на рис. 3.

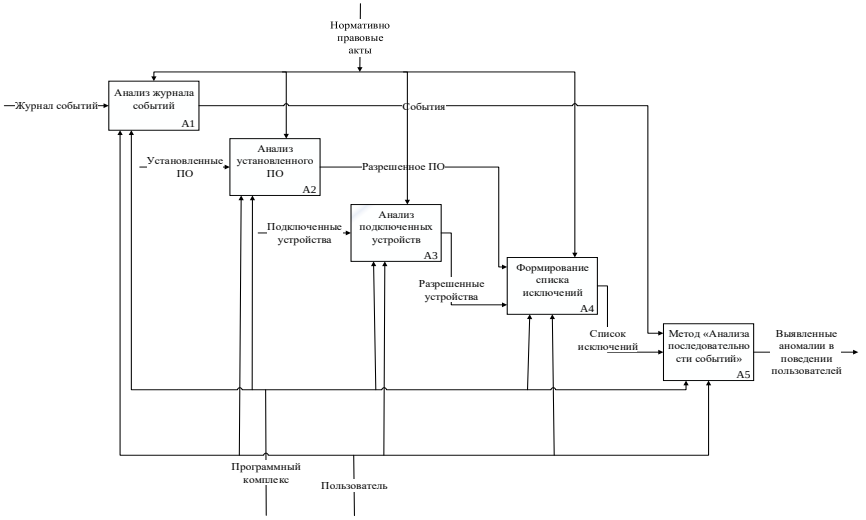


Рис. 3. Функциональная модель программного комплекса выявления аномалий в поведении пользователей

Функциональная модель позволила разработать программный комплекс выявления аномалий в поведении пользователя, который имеет клиент-серверную архитектуру.

На основании функциональной модели разработан интерфейс программного комплекса, интерфейс представлен на рис. 4 и 5.

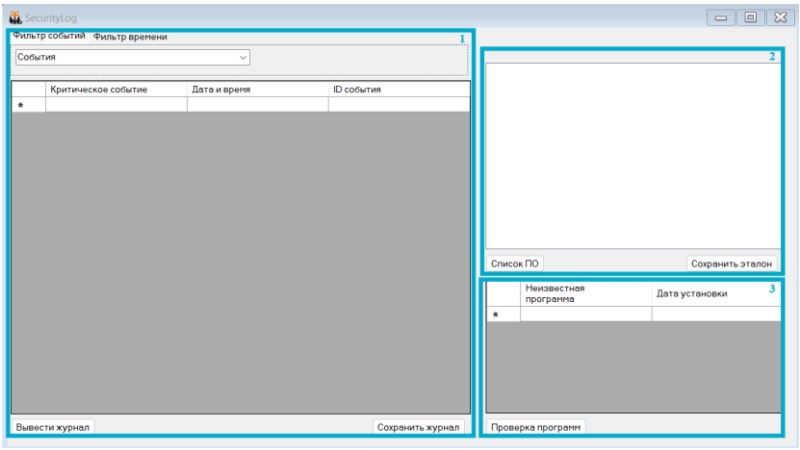


Рис. 4. Пользовательский интерфейс SecurityLog программного комплекса (экранная копия)

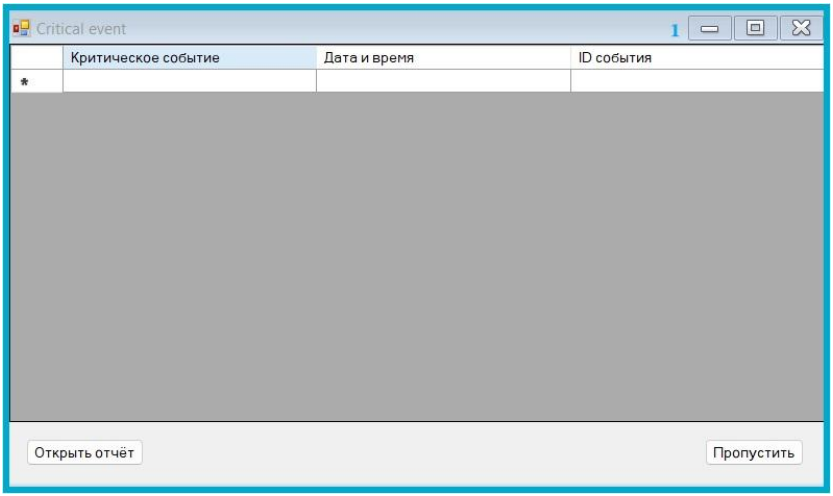


Рис. 5. Пользовательский интерфейс «Critical event» программного комплекса (экранная копия)

Пользовательский интерфейс состоит из следующих элементов:

1) область просмотра событий;
2) область просмотра списка установленного программного обеспечения, внесенного в список исключений;
3) область просмотра, обнаруженного не разрешенного программного обеспечения.

На рис. 6 представлена область просмотра событий, на которой можно отфильтровать события по названию, а также произвести фильтрацию по времени их возникновения, после чего можно просмотреть все собранные события и сохранить их в журнал для подробного просмотра.

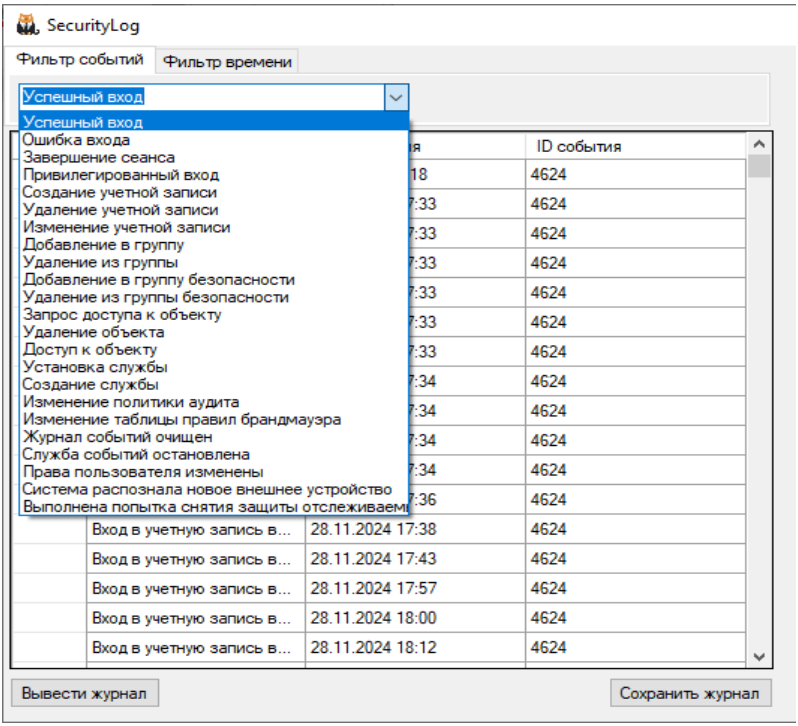


Рис. 6. Область просмотра событий (экранная копия)

В ходе разработки программного комплекса проведена серия экспериментов, программа экспериментальных исследований представлена в табл. 5.

Таблица 5

План экспериментальных исследований

№	Цель эксперимента	Входные данные
1	2	3
1	Определение неудачных попыток входа в систему	Учетная запись User2
2	Выявление несанкционированного изменения прав пользователя	Учетная запись User2 без прав администратора

Эксперимент №1:

По условию эксперимента в системе установлен программный комплекс. В ходе эксперимента была создана учетная запись пользователя, в которую была совершена попытка неудачного входа. На рис. 7 представлена работа программного комплекса.

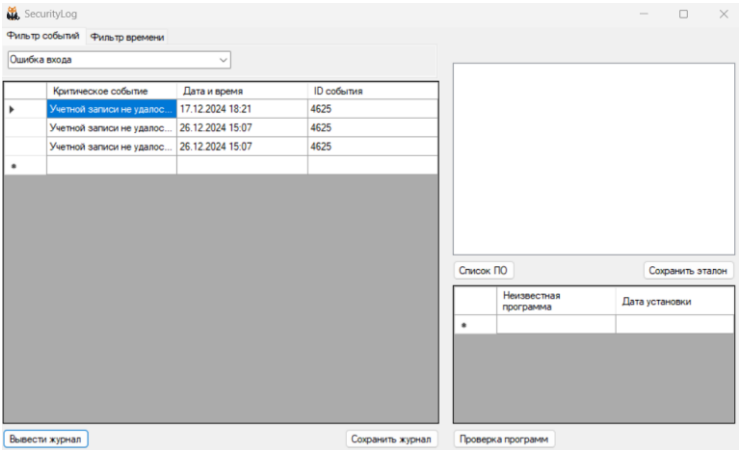


Рис. 7. Работа программного комплекса (экранная копия)

В результате работы программного комплекса были обнаружены 2 попытки неудачного входа в систему, а также был сформирован подробный отчёт об ошибках, представленный на рис. 8.

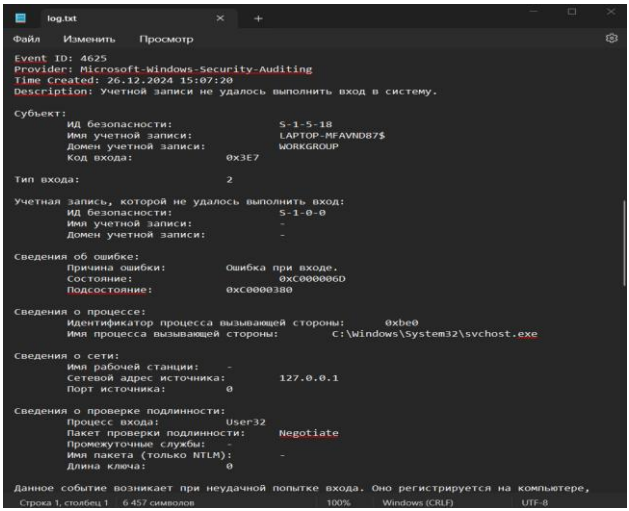


Рис. 8. Отчет об ошибках (экранная копия)

Эксперимент №2:

По условию эксперимента в системе установлен программный комплекс. В системе имеются две учетные записи со следующими правами:

User1: Администратор.

User2: Стандартный пользователь.

В ходе эксперимента было произведено несанкционированное изменение прав пользователя User2 на «Администратор». На рис. 9 представлена работа программного комплекса:

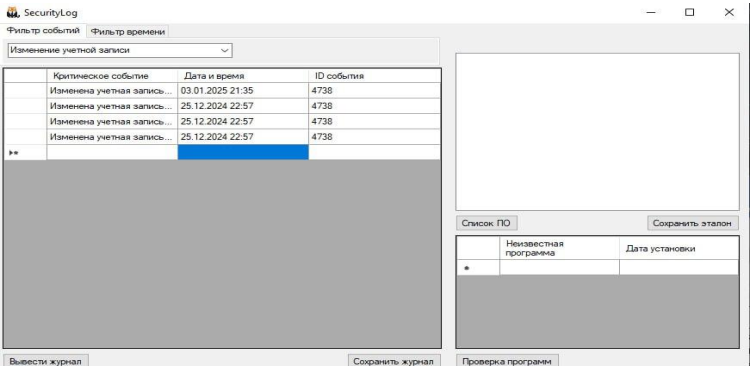


Рис. 9. Обнаружение несанкционированного изменения прав доступа (экранная копия)

В результате анализа программный комплекс выявил изменение прав учетной записи, сформировал и отправил отчет об этом на свою серверную составляющую (рис. 10).

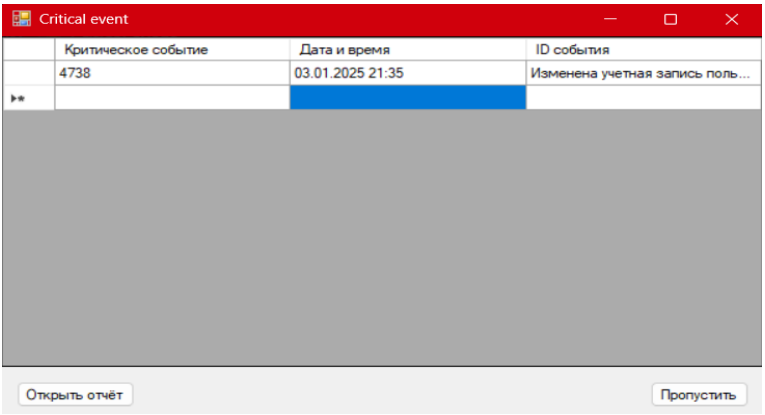


Рис. 10. Отчет о выявленном несанкционированном изменении прав пользователя (экранная копия)

В процессе проведения экспериментальных исследований проведен анализ системы для выявления аномального поведения пользователей. В ходе исследования было проведено 2 эксперимента.

В результате эксперимента №1 были зафиксированы неудачные попытки входа. Программный комплекс произвел анализ системы, выявил аномалию в поведении пользователя при попытке входа в систему, сообщил об этом и сформировал отчет.

В результате эксперимента №2 выявлено несанкционированное изменение прав пользователя. Программный комплекс определил несанкционированное изменение прав пользователя, сформировал отчет о выявленной аномалии и отправил данные на сервер администратора.

Анализ результатов экспериментальных исследований показал, что система может подвергаться воздействию со стороны внутренних нарушителей. Программный комплекс помогает выявить аномалии в поведении пользователей, как в ручном режиме, так и в автоматическом, что позволяет своевременно устранить возможную угрозу утечки информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Positive Technologies. Анализ утечек данных за третий квартал 2024 года [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com, свободный (дата обращения: 12.03.2025).

2. *Гостев А.* Методы обнаружения аномалий в информационных системах. – М.: Инфра-М, 2023. – 312 с. (дата обращения: 12.03.2025).
3. *Ласков П., Шлегель Р.* Машинное обучение в анализе безопасности: методы и подходы // Journal of Information Security. – 2023. – Т. 14. – № 4. – С. 12-29 (дата обращения: 12.03.2025).
4. Современные методы анализа поведения пользователей: материалы международной конференции / под ред. И.В. Петрова. – Казань: Казанский федеральный университет, 2023. – 198 с. (дата обращения: 12.03.2025).
5. Касперский Е. Киберугрозы и способы их предотвращения. – СПб.: Питер, 2022. – 256 с. (дата обращения: 12.03.2025).

УДК 004.056+343.98

Н.Б. Ельчанинова, Н.Н. Сероштан

Южный федеральный университет, Россия, г. Таганрог

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ ИБ: ИНСТРУМЕНТЫ И МЕТОДЫ ДЛЯ УСКОРЕНИЯ АНАЛИЗА ДАННЫХ

В статье рассматриваются инструменты и подходы, которые позволяют автоматизировать некоторые процессы криминалистического расследования инцидентов информационной безопасности. Целью работы является анализ уже имеющихся инструментов автоматизации, а также разработка собственных инструментов для ускорения процесса исследования артефактов в рамках криминалистического расследования. Основным результатом работы является разработка двух программ, написанных на языке программирования Python, а также рекомендации для ускорения анализа данных.

Ключевые слова: *информационная безопасность; компьютерная криминалистика, артефакты, Visual Studio Code, Volatility, YARA-правила, Prefetch, PowerShell, дамп памяти, цифровые доказательства, автоматизация анализа, индикаторы компрометации, регулярные выражения.*

The article explores tools and approaches for automating certain processes in digital forensics investigations of cybersecurity incidents. The study aims to analyze existing automation tools and develop custom solutions to accelerate the examination of artifacts during forensic investigations. The primary outcome of this work is the development of two Python-based programs, along with recommendations for optimizing data analysis.

Keywords: *information security; digital forensics; artifacts; Visual Studio Code; Volatility; YARA rules; Prefetch; PowerShell; memory dump; digital evidence; analysis automation; indicators of compromise (IoC); regular expressions.*

Введение

Расследование инцидентов информационной безопасности в современных условиях становится всё более сложной задачей. От специалистов компьютерной криминалистики требуется быстрая и точная реакция. Успешное расследование инцидентов информационной безопасности заключается в оперативном и качественном анализе исследуемой системы.

В связи с этим возрастает необходимость в использовании инструментов и методов, которые позволяют автоматизировать рутинные этапы криминалистического анализа и снизить нагрузку на криминалиста.

В настоящее время существует широкий спектр инструментов, применяемых в компьютерной криминалистике для анализа артефактов и восстановления хронологии событий. Среди них можно выделить такие популярные решения, как Volatility [1] – фреймворк для анализа дампов оперативной памяти, FTK Imager [2] – средство для изучения образов носителей информации, Arsenal Image Mounter [3] – инструмент для монтирования образов дисков для исследования.

Несмотря на то, что функциональность существующих решений обширна, в некоторых случаях возникает необходимость в разработке собственных утилит, адаптированных под конкретные задачи расследования и специфику цифровых артефактов.

Использование инструментов разработчиков и аналитиков

Многие криминалистические инструменты (Volatility, Regripper, MFT2csv, PECmd и другие) позволяют представить результаты своей работы в форматах типа «.csv» и «.txt». Открытие и анализ каждого отдельного файла вручную занимает слишком много времени.

При помощи Visual Studio Code [4] можно одновременно просматривать и быстро искать информацию сразу в нескольких файлах. Для этого необходимо лишь сохранить все отчеты в одном каталоге, а затем открыть его при помощи Visual Studio Code. Дополнительную гибкость этому поиску придает возможность использования регулярных выражений, которые позволяют задавать сложные шаблоны для поиска по содержимому файлов, что может ускорить выявление подозрительных следов (рис. 1).

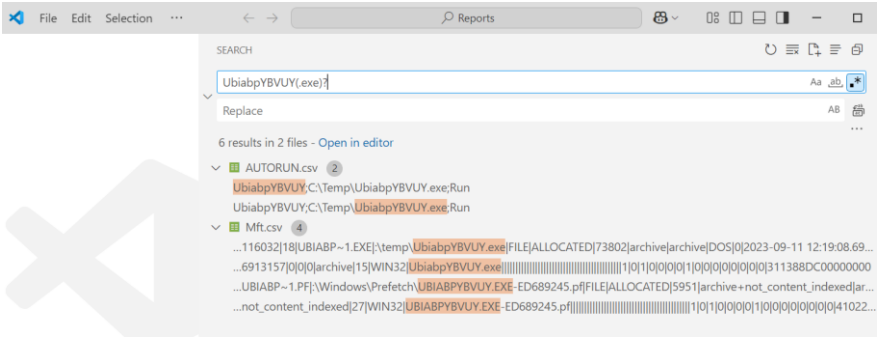


Рис. 1. Множественный поиск в Visual Studio Code

Microsoft Excel – полезный инструмент для систематизации и визуализации цифровых доказательств, особенно при работе с табличными данными. При помощи Excel можно сортировать обнаруженные доказательства по

времени, формировать таймлайн событий, строить таблицы по данным из файлов «.csv». Это помогает упорядочить и визуализировать анализируемые данные (рис. 2).

Дата и время события (UTC+00:00)	Событие
11.09.2023 12:01	Файл создан на диске "C:\Users\user-dev\Downloads\YOUR.PRIZE.HERE.rar"
11.09.2023 12:01	Первый запуск файла "C:\Users\user-dev\Downloads\YOUR.PRIZE.HERE\TEMPLATE.PSD .EXE" на исполнение.
11.09.2023 12:01	Дата последней модификации файла "C:\temp\UblabpYBVUV.exe"
11.09.2023 12:01	Файл создан на диске "C:\temp\UblabpYBVUV.exe"
11.09.2023 12:01	Последний запуск файла "C:\Users\user-dev\Downloads\YOUR.PRIZE.HERE\TEMPLATE.PSD .EXE" на исполнение.
11.09.2023 12:01	Файл создан на диске "C:\Users\user-dev\Downloads\YOUR.PRIZE.HERE\TEMPLATE.PSD .DXE"
11.09.2023 12:01	Первый запуск файла "VOLUME{00000000000000-84311583}МИМКАТZX64МИМКАТZ.EXE". Параметры запуска: "minnkatz.exe "privilege::debug""
11.09.2023 12:02	Файл создан на диске "C:\Windows\Help\Inno_update.exe"
11.09.2023 12:02	Дата последней модификации файла "C:\Windows\Help\Inno_update.exe"
11.09.2023 12:02	Файл "C:\Windows\Help\Inno_update.exe" прописался в ключе в качестве системного драйвера "vscode-updir"
11.09.2023 12:02	Файл "C:\Temp\UblabpYBVUV.exe" прописался в ключе автозагрузки "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" как "ApacheBench command line utility"
11.09.2023 12:03	Пользователь открыл файл "C:\Users\user-dev\Downloads\YOUR.PRIZE.HERE\FrontEnd.docx"
13.09.2023 20:31	Файл создан на диске "C:\Windows\Temp\svchost.exe"
13.09.2023 20:31	Дата последней модификации файла "C:\Windows\Temp\svchost.exe"
13.09.2023 22:20	Файл "C:\Windows\Temp\svchost.exe" прописался в ключе автозагрузки "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit" как "ApacheBench command line utility"

Рис. 2. Timeline в Excel

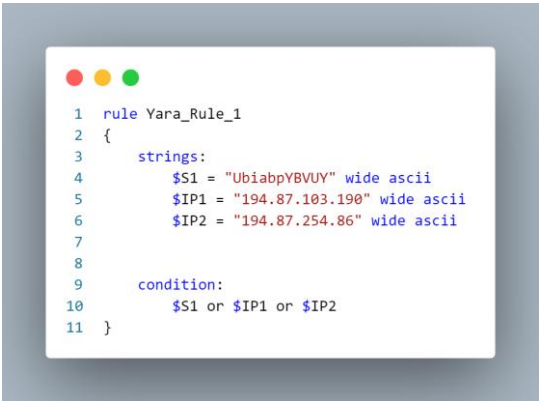
Также Excel позволяет выявлять закономерности и хронологические зависимости между действиями пользователя и событиями в системе и поддерживает условное форматирование, фильтрацию и построение графиков, что делает его удобным средством для первичного анализа временных шкал, сетевой активности, журналов входа в систему и других цифровых артефактов.

Разработка и использование YARA-правил для Volatility

YARA-правила [5] – это шаблоны, используемые для идентификации файлов, процессов или участков памяти по характерным сигнатурам, основанным на строках и бинарных шаблонах. Написание и использование YARA-правил с фреймворком для криминалистического анализа оперативной памяти Volatility позволяют повысить эффективность анализа исследуемой системы [6].

При помощи собственных сигнатур можно оперативно детектировать потенциально вредоносные следы в дампе памяти, такие как: запуски процессов; открытые файлы; сетевые соединения; модули ядра и драйверы; инъекции кода и иные следы вредоносной активности.

Yara-правило выглядит и строится, как показано на рис. 3.



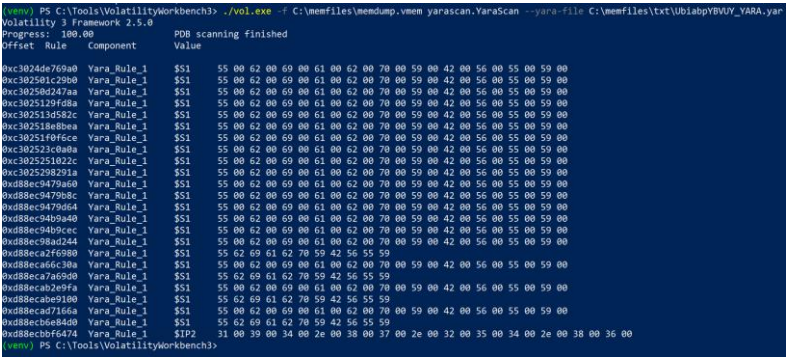
```
rule Yara_Rule_1
{
    strings:
        $S1 = "UbiabpYBVUY" wide ascii
        $IP1 = "194.87.103.190" wide ascii
        $IP2 = "194.87.254.86" wide ascii


    condition:
        $S1 or $IP1 or $IP2
}
```

Рис. 3. YARA-правило для поиска выбранных индикаторов модулем YARAScan Volatility

Данное правило будет искать два внешних IP-адреса и название файла в дампе оперативной памяти посредством модуля Volatility YARAScan. Строки определяются как *wide* и *ascii*, что позволяет находить совпадения как в обычной, так и в UNICODE-кодировке, характерной для систем Windows. Такое правило может быть полезно, например, при анализе подозрительных соединений или следов работы вредоносного ПО, сохраняющих сетевые индикаторы или сигнатуры в памяти.

Отображение процесса работы модуля с данным правилом можно увидеть на рис. 4. Результат работы модуля YaraScan демонстрирует адреса в памяти, где обнаружены совпадения с указанными строками YARA-правила, включая как обычный ASCII, так и wide (UTF-16LE) форматы.



```
(venv) PS C:\Tools\VolatilityWorkbench3> ./vol.exe -f C:\memfiles\memdump.vmem yarascan.YaraScan --yara-file C:\memfiles\txt\UbiabpYBVUY_YARA.yar
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Offset  Rule    Component       Value

0xc3024de769a0  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xc302501c29b0  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xc30250d247aa  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xc3025129fd8a  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xc302513d582c  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xc302518e8bea  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xc30251f0f6ce  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xc302523c0a0a  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xc3025251022c  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xc3025298291a  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xd88ec9479a60  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xd88ec9479b8c  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xd88ec9479d64  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xd88ec94b9a40  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xd88ec94b9cec  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xd88ec98ad244  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xd88eca2f6980  Yara_Rule_1      $S1     55 62 69 61 62 70 59 42 56 55 59
0xd88eca66c30a  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xd88eca7a69d0  Yara_Rule_1      $S1     55 62 69 61 62 70 59 42 56 55 59
0xd88ecab2e9fa  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xd88ecabe9100  Yara_Rule_1      $S1     55 62 69 61 62 70 59 42 56 55 59
0xd88ecad7166a  Yara_Rule_1      $S1     55 00 62 00 69 00 61 00 62 00 70 00 59 00 42 00 56 00 55 00 59 00
0xd88ecb6e8400  Yara_Rule_1      $S1     55 62 69 61 62 70 59 42 56 55 59
0xd88ecbbf6474  Yara_Rule_1      $IP2    31 00 39 00 34 00 2e 00 38 00 37 00 2e 00 32 00 35 00 34 00 2e 00 38 00 36 00
(venv) PS C:\Tools\VolatilityWorkbench3>
```

Рис. 4. Результат работы модуля YARAScan

Разработка программы для автоматизации первичного анализа Prefetch

Prefetch, или компонент логической предвыборки – это часть диспетчера памяти ОС Windows. Он повышает производительность системы за счет предварительной загрузки кодовых страниц часто используемых приложений.

Система отслеживает все файлы и каталоги, на которые ссылается каждое приложение или процесс, и отображает их в файл с расширением «.pf» [7].

Каталог Prefetch находится в ОС Windows по следующему пути:

%WinDir%\Prefetch

Шаблон имени файлов Prefetch:

<EXE_NAME>-<PATH_HASH>.pf

Если говорить о метаданных артефакта, то время первого запуска исполняемого файла соответствует времени создания файла Prefetch, а дата последнего изменения – времени последнего запуска. Начиная с Windows 8+ в файле «.pf» будет содержаться 8 последних времен запуска «.exe».

Таким образом, Prefetch фиксирует факт запуска исполняемых файлов в системе, и может быть проанализирован на предмет исполнения потенциально вредоносных файлов [8].

Чтобы ускорить процесс анализа и выявления предположительно опасных файлов в Prefetch, была разработана программа на языке программирования Python (рис. 5).

```python
from pathlib import Path
from rich import print

# Путь к каталогу Prefetch на исследуемом образе
PREFETCH_DIR_PATH = Path(r"E:\Windows\Prefetch")
# Набор имен файлов, которые будут детектироваться
MALICIOUS_NAMES = (
    "mimikatz",
    "anydesk",
    "nmap",
    # и ... список расширяемый
)
for filepath in PREFETCH_DIR_PATH.iterdir():

    for malicious_name in MALICIOUS_NAMES:

        if malicious_name.lower() in filepath.name.lower():
            print (filepath)
```

Рис. 5. Программный код для первичного анализа файлов в Prefetch

Данная программа состоит из двух модулей. Первый модуль содержит динамически заполняемый список названий потенциально опасных файлов, индикаторов компрометации и иных объектов, который может быть заполнен и расширен криминалистом. Второй модуль сопоставляет имена файлов Prefetch и имена файлов из первого модуля. Таким образом, происходит первичный анализ и выявление потенциально опасных файлов на исследуемой системе.

Пример вывода результатов работы данной программы представлен на рис. 6. Здесь мы видим доказательства сработки на запуск пользователем в системе средства удаленного доступа AnyDesk и Mimikatz.

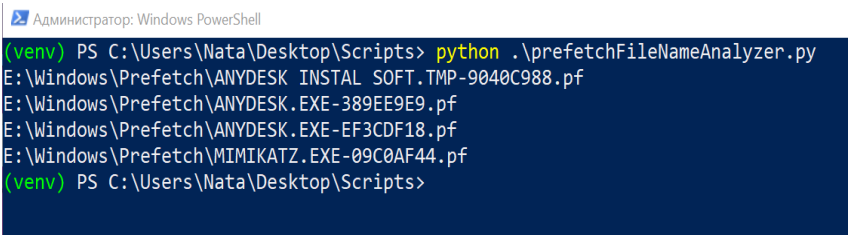


Рис. 6. Результат работы программного кода для анализа Prefetch

Разработка программы для автоматизации первичного анализа ConsoleHost_history

Все команды, которые вводятся в консоли PowerShell, записываются в текстовый лог-файл «ConsoleHost_history.txt».

Расположение данного файла в ОС Windows:

%userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

Функционал хранения истории команд в PowerShell основан на дополнительном модуле PSReadLine, который расширяет функционал консоли PowerShell.

Файл ConsoleHost_history.txt также можно анализировать на предмет запуска потенциально опасных программ. Для ускорения первичного анализа данного файла и выявления следов запуска нелегитимных процессов была разработана специальная программа (рис. 7).

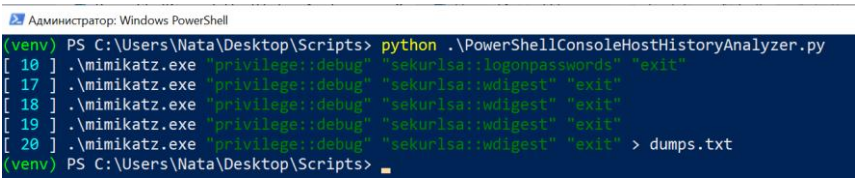
После запуска программы получаем доказательства сработки на запуск Mimikatz с соответствующими параметрами (рис. 8).

```python
from pathlib import Path
from rich import print

# Путь к лог-файлу на исследуемой системе
CONSOLE_HOST_HISTORY_PATH = Path(
    r"E:\Users\andrewww-dev\AppData\Roaming"
    r"\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt"
)
# Набор строк, которые будут детектироваться
MALICIOUS_NAMES = (
    "mimikatz",
    "anydesk",
    "nmap",
    # и ...
)
console_host_history = CONSOLE_HOST_HISTORY_PATH.read_text()
console_host_history_lines = console_host_history.splitlines()
for line_number,line in enumerate(console_host_history_lines,start=1):
    for malicious_name in MALICIOUS_NAMES:

        if malicious_name.lower() in line.lower():
            print ("[",line_number,"]", line)
```

Рис. 7. Программный код для первичного анализа файла истории команд PowerShell



```
Администратор: Windows PowerShell
(venv) PS C:\Users\Nata\Desktop\Scripts> python .\PowerShellConsoleHostHistoryAnalyzer.py
[ 10 ] .\mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit"
[ 17 ] .\mimikatz.exe "privilege::debug" "sekurlsa::wdigest" "exit"
[ 18 ] .\mimikatz.exe "privilege::debug" "sekurlsa::wdigest" "exit"
[ 19 ] .\mimikatz.exe "privilege::debug" "sekurlsa::wdigest" "exit"
[ 20 ] .\mimikatz.exe "privilege::debug" "sekurlsa::wdigest" "exit" > dumps.txt
(venv) PS C:\Users\Nata\Desktop\Scripts>
```

Рис. 8. Результат работы программы для анализа ConsoleHost_history.txt

Выводы

В рамках выполненной работы проведён анализ существующих инструментов автоматизации криминалистического анализа, а также разработаны собственные программные решения, направленные на ускорение и повышение эффективности анализа некоторых артефактов ОС Windows в процессе расследования инцидентов информационной безопасности.

В работе продемонстрировано, что использование общедоступных инструментов, таких как Visual Studio Code и Excel, позволяет упростить и ускорить процесс поиска и визуализации информации в обширных массивах файловых данных. Применение множественного поиска с использованием регулярных выражений и сортировки событий по временным меткам существенно повышают удобство первичного анализа. Также были разработаны

и протестированы YARA-правила для использования с фреймворком Volatility. Данные правила позволяют эффективно идентифицировать вредоносную активность в дампах оперативной памяти.

Также в работе представлены две самостоятельно разработанные программы, написанные на языке программирования Python. Первая – для автоматического анализа содержимого каталога Prefetch с целью выявления следов запуска подозрительных исполняемых файлов. Вторая – для анализа истории команд PowerShell из файла ConsoleHost_history.txt, позволяющая обнаруживать факты выполнения потенциально вредоносных скриптов или программ, таких как Mimikatz.

Обе разработанные программы обеспечивают расширяемость за счёт возможности пополнения списков потенциально опасных файлов, индикаторов компрометации, что делает их удобными и гибкими средствами в рамках криминалистического расследования компьютерного инцидента.

Таким образом, разработанные решения позволяют автоматизировать некоторые этапы первичного анализа цифровых доказательств и снижают время, затрачиваемое на анализ данных большого объема. Предложенный подход может быть использован как база для дальнейшего развития систем автоматизации расследований инцидентов, а также как вспомогательный инструмент в рамках оперативного реагирования на угрозы информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Volatility Foundation. Volatility Framework: Memory Forensics [Электронный ресурс]. – Режим доступа: https://github.com/volatilityfoundation/volatility (дата обращения: 05.02.2025).
2. Clingeric. Forensic Toolkit [Электронный ресурс]. – Режим доступа: https://github.com/clingeric/forensic-toolkit (дата обращения: 05.02.2025).
3. Arsenal Recon. Arsenal Image Mounter and Digital Forensics Tools [Электронный ресурс]. – Режим доступа: https://arsenalrecon.com/ (дата обращения: 05.02.2025).
4. Microsoft. Visual Studio Code [Электронный ресурс]. – Режим доступа: https://code.visualstudio.com/ (дата обращения: 05.02.2025).
5. YARA Documentation. Writing YARA Rules [Электронный ресурс]. – Режим доступа: https://yara.readthedocs.io/en/stable/writingrules.html (дата обращения: 05.02.2025).
6. *Nyholm H., Monteith K., Lyles S., Gallegos M.* The Evolution of Volatile Memory Forensics // Journal of Cybersecurity and Privacy. – 2022. – Vol. 2, No. 3. – P. 556-572. – DOI: 10.3390/jcp2030028. – License: CC BY 4.0.
7. *Руссинович М.* Внутреннее устройство Windows. – М.: Вильямс, 2012. – 752 с.
8. *Heriyanto A.* Forensic Examination and Analysis of the Prefetch Files on the Banking Trojan Malware Incidents // Proceedings of the 12th Australian Digital Forensics Conference (5-6 December 2014, ECU Joondalup Campus, Perth, Western Australia). – Perth: Edith Cowan University, 2014. – P. 2-6. – DOI: 10.13140/2.1.2460.5767.

УДК 33

А.В. Иванов, Ю.Д. Любо

Финансовый университет, Россия, г. Москва

ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКАЯ ИНФРАСТРУКТУРА ДОВЕРИЯ И БЕЗОПАСНОСТИ В СИСТЕМЕ ЦИФРОВОГО РУБЛЯ

Целью исследования является построение информационно-технологической инфраструктуры доверия и безопасности в системе цифрового рубля. В рамках обозначенной цели выполнены задачи по изучению понятия «цифровой рубль», его характеристик и свойств для обоснования необходимости построения инфраструктуры доверия и ее безопасности в системе цифрового рубля. Для подтверждения обоснованности проектирования подобной инфраструктуры проведён анализ опросов Всероссийского центра изучения общественного мнения (ВЦИОМ) о доверии российских граждан системе цифрового рубля для проектирования целостной инфраструктуры ее безопасности. При построении информационно-технологической инфраструктуры учитывалось мнение граждан относительно потенциальных преимуществ и угроз использования цифрового рубля. Кроме того, определены характеристики цифрового рубля для определения базисных и структурных элементов информационно-технологической инфраструктуры доверия и инструментов ее безопасности в системе цифрового рубля. На основе полученных данных, проведена подробная аналитика по определению и описанию взаимосвязей между доверием в системе цифрового рубля и обеспечением её безопасности. Сформулированы некоторые предложения по внедрению информационно-технологической инфраструктуры доверия и ее безопасности в системе цифрового рубля с применением современных отечественный средств криптографической защиты информации.

Ключевые слова: *инфраструктура, инфраструктура доверия, информационно-технологическая инфраструктура доверия, безопасность инфраструктуры доверия, цифровой рубль система цифрового рубля, средства криптографической защиты, коммерческий банк, национальная валюта, платформа цифрового рубля.*

The purpose of the research is to build an information technology infrastructure of trust and security in the digital ruble system. Within the framework of this goal, the tasks of studying the concept of the "digital ruble", its characteristics and properties have been completed to justify the need to build an infrastructure of trust and its security in the digital ruble system. To confirm the validity of designing such an infrastructure, an analysis of surveys by the All-Russian Center for the Study of Public Opinion (VTsIOM) on the trust of Russian citizens in the digital ruble system for designing an integrated infrastructure for its security was conducted. When building the information technology infrastructure, the opinion of citizens regarding the potential advantages and threats of using the digital ru-

ble was taken into account. In addition, the characteristics of the digital ruble have been determined to determine the basic and structural elements of the information technology infrastructure of trust and its security tools in the digital system.

Keywords: *infrastructure, trust infrastructure, information technology infrastructure of trust, security of trust infrastructure, digital ruble digital ruble system, cryptographic protection tools, commercial bank, national currency, digital ruble platform*.

Введение

Для понимания необходимости проектирования информационно-технологической инфраструктуры доверия и безопасности в системе цифрового рубля важное значение имеет его определение в соответствие с указанием Центрального Банка Российской Федерации. Цифровой рубль – это цифровая форма российской национальной валюты, которую Банк России планирует выпускать в дополнение к существующим формам денег [1]. Исходя из данного определения, можно полагать, что внедрение цифровой формы национальной валюты требует проектирования информационно-технологической инфраструктуры доверия и ее безопасности на основе современных средств криптографической защиты. Для обеспечения качественной криптографической защиты, система цифрового рубля должна иметь целостную инфраструктуру доверия, соответствующая требованиям безопасности со стороны всех её основных стейкхолдеров. Это условие является необходимым, так как государство и граждане должны быть уверены в том, что используемая ими валюта, в том числе цифровой рубль имеет высокий уровень безопасности и защищенности.

Основная часть

В целях исследования формирования информационно-технологической инфраструктуры доверия и безопасности в системе защищенности цифрового рубля важен научный подход. Например, ряд ученных акцентируют внимание на проблемах и перспективах обеспечения безопасности цифрового рубля, основанной на «применении криптографических методов шифрования данных, подписей электронных транзакций и мультифакторной аутентификации, а также анализе преимуществ использования гражданами и бизнесом цифрового рубля» [2, 3]. В отдельных работах рассматривает связь между моделями доверия и архитектурой инфраструктуры открытых ключей, которая для шифрования и расшифрования использует ключевую пару: секретный ключ (private key) и открытый ключ (public key). В этой связи рассматриваются две модели использования ключевых пар и сертификатов: децентрализованная модель сетей доверия, создаваемых на основе соглашений доверия удостоверяющих центров (УЦ), не прошедших аккредитацию; модель квалифицированного единого пространства доверия, в основу которой положена

система аккредитованных УЦ и развёрнутая на их базе инфраструктуры открытых ключей (ИОК). Архитектура ИОК определяет структуру отношений доверия между УЦ и другими субъектами инфраструктуры, а также количество удостоверяющих центров, которые непосредственно доверяют друг другу. В системе удостоверяющих центров могут быть выделены УЦ по признаку доверия: корневые центры сертификации – удостоверяющие центры, которым доверяет всё сообщество пользователей, руководствуясь совместной политикой доверия; доверенные центры сертификации – центры сертификации, которым доверяют владельцы сертификатов, образуя свои домены доверия. При потере доверия к начальному звену цепочки (корневому центру сертификации) теряется доверие ко всей цепочке, т.е. ко всем выданным данным центром сертификатам. Выделяются различные модели доверия, такие как: иерархическая, браузерная, сетевая и кросс-сертификационные модели доверия. «Иерархическая модель доверия определяет организационное построение системы удостоверяющих центров (СУЦ) в виде иерархической структуры. Во главе всей структуры СУЦ стоит один УЦк (корневой центр сертификации), которому доверяет всё сообщество пользователей [4].

Мельников Д.А. на основе математического аппарата субъективной логики криптографических средств защиты информации в инфраструктуре открытых ключей предлагает «объединить все существующие удостоверяющие центры инфраструктуры открытых ключей в единую инфраструктуру открытых ключей Российской Федерации, а также сформировать технологическую основу доверия для различных прикладных автоматизированных информационно-технологических систем» [5]. Отдельные работы посвящены исследованию доверия при безопасной разработке программного обеспечения. «Безопасная разработка программного обеспечения является основой доверия к информационно-коммуникационным технологиям в условиях современных киберугроз на объектах критической информационной инфраструктуры [6].

Важное значение имеют практические рекомендации по формированию инфраструктуры доверия в системе цифрового рубля. Основными элементами такой модели являются: «репозитарий цифровых рублей, которые выпущены Банком России; корневой удостоверяющий центр Банка России; территориальные удостоверяющие центры Банка России; головной центр подтверждения подлинности цифрового рубля и платёжных операций, принадлежащий Банку России; территориальные центры подтверждения подлинности цифрового рубля и платёжных операций, принадлежащие банкам; центры подтверждения подлинности цифрового рубля и платёжных операций, принадлежащие банкам, обслуживающим организации (например, Интернет-магазины), которые принимают цифровые рубли в качестве оплаты

товаров и услуг; удостоверяющие центры банков, образующие второй уровень иерархии удостоверяющих центров; физические и юридические лица, которые являются владельцами цифровых рублей на основании соответствующих договоров с КФО (банками), аккредитованными Банком России [7].

Информационную компоненту технологической инфраструктуры доверия в системе цифрового рубля составляют результаты различных опросов граждан Российской Федерации по их отношению по поводу внедрения цифрового рубля. Например, Всероссийский центр изучения общественного мнения (ВЦИОМ) в августе 2024 года провёл по данной проблеме опрос населения граждан России. По данным опроса, почти 50% россиян не хочет пользоваться цифровым рублём. Основными причинами недоверия цифровому рублю, является недостаточная защищенность и возможное мошенничество в системе цифрового рубля. Второй причиной граждане выделяют повышенный контроль со стороны государства [8]. Результаты исследований отображены в Диаграмме 1.

Диаграмма 1

Источник: Официальный сайт ВЦИОМ. ВЦИОМ.Новости https://wciom.ru/.

Можно полагать, что отношение граждан к внедрению цифрового рубля составляют информационную компоненту технологической инфраструктуры доверия в системе цифрового рубля. В то же время, характеристики системы безопасности цифрового рубля регулируются Банком России. Например, Центральный Банк Российской Федерации выделяет следующие его характеристики [9]: отсутствие рисков, присущих наличному или безналичному рублю. То есть, Цифровой рубль не может быть украден физически, или ликвидирован при банкротстве коммерческого банка; эквивалентность наличному и безналичному рублю без обменного курса; более надёжный доступ к средствам владельца Цифрового рубля через независимость от

конкретного коммерческого банка. Представленные характеристики позволяет определить Цифровой рубль, как национальную валюту без привязки к коммерческим банковским организациям, с возможностью обменивать Цифровой рубль 1:1 с наличным или безналичным рублём.

Таким образом, можно сказать, что информационно-технологическая инфраструктура доверия должна обладать современными технологическими аппаратами, позволяющими обеспечить защищённость данных граждан путём криптографических методов шифрования. Методы шифрования должны обеспечивать невозможность достичь средств граждан злоумышленниками. Определив информационно-технологическую инфраструктуру доверия, стоит изучить криптографические методы, необходимые для обеспечения безопасности платформы Цифрового рубля. В первую очередь, Цифровой рубль обладает системой шифрования с использованием сертификатов безопасности и усиленных неквалифицированных электронных подписей (УНЭП). Последний вариант уже прошёл проверку через государственное приложение «Госключ». Таким образом, для работы с Цифровым рублём, будет необходимо обладать сертификатами безопасности банка, для защищённого двустороннего соединения мобильного приложения клиента и банком, а также, подтверждать свои действия при помощи УНЭП [10]. Процессы взаимодействия клиента с банком описан в Схеме 1.

Схема 1

Источник: Составлено автором

Для безопасности информационно-технологической инфраструктуры доверия в системе цифрового рубля необходимо применение API (прикладные программные приложения) Банком России и кредитными организациями. Основу безопасности API составляет шифрование, под которым понимается преобразование исходных данных в зашифрованный вид, который должен быть расшифрован с помощью специального ключа. Выделяют два метода шифрования, а именно: симметричное и асимметричное. Например, симметричное шифрование предполагает использование одного ключа как

для шифрования, так и для расшифрования. В этом случае, используется один ключ, этот метод отличается высокой скоростью работы и эффективностью, в то же время, это создает дополнительные риски при использовании в открытых сетях. Наиболее распространённые симметричные алгоритмы – AES (Advanced Encryption Standard), который является стандартом из-за своей устойчивости к криптоанализу, 3DES (Triple DES). Существует два основных типа такого вида шифрования: блочные и потоковые шифры. Упоминаемый выше AES является блочным шифром. Это означает, что он работает с блоками данных, и это обеспечивает более высокую криптографическую стойкость. В асимметричном шифровании используется два различных ключа: один из них – открытый, им информация шифруется, другой – закрытый, который используется для расшифрования сообщения. Российским аналогом является алгоритм Кузнечик (ГОСТ Р 34.12-2015), который применяется в национальных стандартах шифрования и обеспечивает высокий уровень защиты данных в финансовых учреждениях и государственных системах [11].

Криптографические методы применяются и в банковской сфере. Например, при совершении онлайн-платежей с использованием платежной система МИР, данные передаются через защищённые каналы с использованием протоколов TLS, которые позволяют обеспечить надежную и эффективную защиту информации. Решение процедур аутентификации и авторизации осуществляется на основе использования токенов доступа в целях управления сессиями и обеспечения безопасного доступа к ресурсам. Токены позволяют проверять подлинность пользователей без необходимости повторной авторизации при каждом запросе. Токены доступа делятся на несколько типов, наиболее распространённые из них – OAuth-токены и JWT (JSON Web Tokens). OAuth-токены используются для делегированной авторизации, при которой одно приложение может получать ограниченный доступ к ресурсам пользователя, находящимся на сервере другого приложения. Данная процедура применяется для интеграции сторонних сервисов, когда они могут выполнять операции от имени пользователя, но без доступа к его логину и паролю. Данная технология начинается с аутентификации пользователя на сервере авторизации, после чего выдается токен доступа, который клиент использует для взаимодействия с API. Российским аналогом в финансовой сфере является ГОСТ OAuth 2.0, который разрабатывается в рамках отечественных стандартов безопасности для защиты персональных данных при авторизации пользователей. JWT (JSON Web Tokens) – это компактные токены, в которых полезная нагрузка (payload) кодируется в формате JSON. Каждый такой токен содержит информацию о пользователе, его правах доступа, а также времени действия. Подпись токена выполняется с использованием как асимметричных, так и симметричных ключей, что позволяет убедиться в его подлинности и целостности.

Управление сессиями с использованием токенов доступа включает несколько ключевых аспектов. Во-первых, необходимо контролировать время жизни токенов. Если не ограничивать срок действия токенов, то существуют огромные риски компрометации. В то же время для выпуска нового токена необходимо повторное подтверждение пользователя, что повышает уровень безопасности. Во-вторых, важным аспектом является безопасное хранение токенов на клиентской стороне, так как злоумышленник не должен иметь возможности добраться до токенов, даже если получил доступ к устройству пользователя. Для этого необходимо использовать безопасные каналы связи (HTTPS, TLS 1.3) для передачи токенов, чтобы исключить возможность их перехвата злоумышленниками. В-третьих, если злоумышленник получил токен, необходимо иметь механизм его немедленного аннулирования. Для этого существуют чёрные списки (blacklists), при каждом запросе сервер проверяет, не входит ли полученный токен в список отозванных. Однако у этого метода есть серьезные недостатки: передача учетных данных в каждом запросе увеличивает риск их компрометации. Поэтому были разработаны более безопасные альтернативы, такие как аутентификация через API-ключи, которые представляют собой уникальные идентификаторы, выдаваемые клиентам для доступа к ресурсам API.

Дополнительную защиту API обеспечивает многофакторная аутентификация (MFA), при которой пользователь должен подтвердить свою личность несколькими способами (например, паролем и одноразовым кодом). Это значительно снижает вероятность несанкционированного доступа, даже если злоумышленник получил учетные данные пользователя. OAuth 2.0 предоставляет возможность делегированной авторизации, разделяя процесс доступа на три компонента: Ресурсный сервер – хранит защищенные данные. Сервер авторизации – выдает токены доступа после успешной аутентификации. Клиент – запрашивает доступ к данным.

API активно используются в автоматизированных банковских системах (АБС) и системах дистанционного банковского обслуживания (ДБО). В АБС обеспечивается управление счетами, кредитами и платежами, а в ДБО пользователи взаимодействуют с банковскими сервисами через интернет и мобильные приложения. Надежность API-контроля в этих системах напрямую влияет на безопасность операций. Технология защиты и безопасности API включает четыре компонента: пользователь, клиент (запрашивает доступ), сервер авторизации (выдаёт токен), ресурсный сервер (предоставляет доступ при наличии токена). Эти элементы создают многослойную систему безопасности, в которой каждая роль строго определена, однако безопасность API зависит не только от их взаимодействия, но и от того, какие используются инструменты.

API Gateway играет важную роль в архитектуре API: он управляет потоком данных, организует маршруты запросов и защищает систему от угроз. Он принимает входящие запросы, проверяет их подлинность, маршру-

тизирует их к соответствующим ресурсам и возвращает ответы клиентам. В сущности, это интеллектуальный диспетчер, определяющий, куда направить каждый запрос, чтобы система работала эффективно.

Для безопасности API применяются различные инструменты: SAST (Статический анализ); DAST (Динамический анализ); IAST (Интерактивное тестирование); Фаззинг. Сравнительный анализ таких инструментов представлен в табл. 1.

Таблица 1

Сравнение методов тестирования безопасности API

Метод	**Как работает**	**Когда применять**	**Преимущества**	**Ограничения**
SAST (Статический анализ)	Анализирует исходный код без его выполнения	На этапе разработки, перед развертыванием API	Позволяет находить ошибки раньше всех, не требует работающей системы	Высокий процент ложных срабатываний, не выявляет конфигурационные уязвимости
DAST (Динамичес-кий анализ)	Отправляет запросы к API, анализируя ответы без доступа к коду	Для готовых API, тестирования безопасности продакшена	Идеален для анализа конфигурационных проблем, не требует изменений в коде	Не показывает, где в коде находится уязвимость, сложнее автоматизировать
IAST (Интерактивное тестирование)	Встраивает агент в API, отслеживая выполнение кода в реальном времени	Для интеграции безопасности в CI/CD, глубокого тестирования	Детализированные отчёты, меньше ложных срабатываний, обнаруживает ошибки в коде и в среде выполнения	Требует развернутого API, влияет на производительность
Фаззинг	Генерирует и отправляет случайные некорректные данные в API	Для поиска неожиданных ошибок, тестирования на отказоустойчивость	Обнаруживает скрытые баги, выявляет критические сбои в обработке данных	Может быть ресурсоёмким, требует мощных тестовых сред

Источник: составлено автором

По результатам сравнительного анализа, приведённые в табл. 1 можно сделать следующие выводы: SAST лучше всего подходит для ранних этапов разработки, когда важно обнаружить ошибки в коде до его развертывания. Он помогает находить логические уязвимости и проблемы в управлении памятью. DAST необходим для тестирования готовых API, он особенно полезен для анализа конфигурационных ошибок, утечек данных и проблем аутентификации. IAST нужен, когда важно понимать, как API ведёт себя в рабочей среде. Он даёт точную информацию о причинах уязвимостей и позволяет тестировать API во время его работы. Фаззинг применяется для поиска нестандартных уязвимостей, помогая выявлять неожиданные ошибки в обработке входных данных, отказоустойчивости API и механизмов защиты.

В целях защиты и безопасности API в России действуют стандарты для финансовых API. Например, Приказ ФСТЭК № 17 определяет требования к защите информации в государственных и корпоративных системах [12], Приказ ФСТЭК № 21 регулирует вопросы безопасности государственных информационных систем, включая требования к API, используемым в электронном документообороте [13]. В финансовом секторе также применяются требования ФСБ РФ, в частности Приказ № 378, который касается использования средств криптографической защиты информации (СКЗИ) при передаче данных через API [14]. ГОСТ Р 57580.1-2017 обязывает компании в банковской сфере проводить сертификацию API перед запуском в эксплуатацию, используя сертифицированные средства криптографической защиты информации [15]. Организации должны внедрять системы обнаружения аномалий в API-трафике и анализировать аутентификацию пользователей на предмет аномального поведения.

Компания «ИнфоТеКС» уже интегрировала продукты ViPNet в систему криптографической защиты участников платформы цифрового рубля, что было интегрировано в систему «iBank» компании «БИФИТ». Эта система позволяет коммерческим банкам получать готовое решение, обеспеченное защитой внутренней инфраструктуры платформы цифрового рубля. Система защиты реализована по запросу Центрального Банка через сертифицированное средство криптографической защиты информации (СКЗИ) ViPNet OSSL. Это СКЗИ позволяет пользователю взаимодействовать с коммерческими банками через мобильное приложение со встроенным модулем Для процедуры взаимодействия, «ИнфоТеКС» также реализовал собственный сервер подписи ViPNet PKI Service, реализованный на собственной криптографической платформе ViPNet HSM. Также, был внедрён шлюз безопасности ViPNet TLS Gateway для подключения к системе «iBank» по протоколу TLS с использованием отечественных криптоалгоритмов [16]. В рамках существующих методов шифрования данных для информационного обмена, протокол TLS является передовым в рамках работы с цифровой валютой. Такая технология позволяет шифровать данные посредством

шифровки передаваемых данных в скрытых пакетах для дальнейшей передачи. Все эти скрытые пакеты имеют общий ключ шифрования и подтверждаются электронной подписью, что усложняет взлом аккаунта в несколько раз. В перспективе система цифрового рубля будет развиваться и уже с 25 августа 2025 года планируется запуск тестовых выплат в цифровых рублях. Это является благоприятным знаком, так как подобные системы, особенно напрямую связанные с национальной валютой и деньгами требует тщательной защиты и безопасности. Также, подобные средства защиты направлены на более толерантное отношение к системе со стороны граждан Российской Федерации. После полноценного тестирования и устранения всех возможных потенциальных угроз, система цифровой валюты имеет высокую вероятность повысить доверие к себе и войти в полноценный оборот.

Заключение

По результатам исследования можно полагать, что информационно-технологическая инфраструктура в системе цифрового рубля безусловно нуждается в ее дополнительной инфраструктурной доработке, в части повышения доверия как с технической компоненты (инфраструктура доверия), так и информационной (отношение граждан) и безопасности в системе цифрового рубля. Как уже было отмечено, самым передовым методом обеспечения подобной инфраструктуры является ассиметричное шифрование трафика и передачи данных. Сейчас Центральный Банк Российской Федерации смог найти такой способ в шифровании с использованием TLS протокола и УНЭП. В обеспечении такого шифрования и защиты, смогла помочь компания «ИнфоТеКС», которая имеет различные продукты для обеспечения защищённой передачи, шифрования и получения данных. Подобные средства криптографической защиты информации крайне необходимы для запуска такой системы цифрового рубля, так как интерес злоумышленников к ней будет крайне высоким. Это суждение также подтверждается опасениями граждан Российской Федерации на основе исследований ВЦИОМ. Помимо всего прочего, государство активно разрабатывает и перепроверяет существующие средства криптографической защиты информации для увеличения безопасности и доверия со стороны граждан. В самое ближайшее время планируется тестовый запуск Цифрового рубля при поддержке Банка России и Федерального казначейства.

Предложения по набору работ, связанных с внедрением инфраструктуры доверия системы цифрового рубля. Минимальный и оптимальный набор работ:

1. *Удостоверяющие центры (УЦ), средства защиты информации (СЗИ), средства криптографической защиты информации (СКЗИ):* – проектирование архитектуры решения и разработка проектной и эксплуатационной документации; – монтаж серверов и автоматизированных рабочих

мест (АРМ) обслуживающего персонала, настройка и конфигурация операционной системы (ОС); – развёртывание и конфигурация Удостоверяющих Центров (включая HSM и сервер точного времени); – установка и настройка средств защиты информации и средств критической защиты информации на серверах; – установка и настройка межсетевых экранов, коммутаторов и TLS-шлюзов; – разработка организационно-распорядительной документации; – установка решения для автоматизации выпуска сертификатов; – установка и настройка решения для мониторинга работоспособности Удостоверяющих Центров.

2. *Автоматизация банковской системы (АБС), дистанционное банковское обслуживание (ДБО), Мобильное приложение:* – развёртывание решения для взаимодействия с платформой цифрового рубля (Контур контроля и контур обработки); – доработка автоматизированной банковской системы (квитовка платежей (ED101), изменение статуса и баланса цифрового рубля клиента, изменение реквизитов клиента, проверки ПОД / ФТ и проверки АБС, бух. учет по новым счетам 30502-30504; – API для дистанционного банковского обслуживания физических и юридических лиц; - доработка дистанционного банковского обслуживания физических и юридических лиц (ПМ БР, экраны для веб-клиента, интеграция с АБС).

3. Интеграция с единой системой идентификации и аутентификации информационного (ЕСИА) и системы быстрых платежей (СБП): – встраивание программного модуля Банка России (ПМБР) в мобильное приложение (при наличии мобильного приложения).

4. *Оценка и аудит:* – оценка влияния для ПМ БР в мобильное приложение; – оценка влияния для контура контроля и контура обработки; - аудит на соответствие ГОСТ Р 57580.1-2017; – аудит на соответствие для дистанционного банковского обслуживания и программного обеспечения в контуре контроля и контуре обработки; – оценка влияния для решения автоматизации выпуска сертификатов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Официальный сайт ЦБ РФ https://cbr.ru/.
2. *Осипова В.С.* Безопасность цифрового рубля // Экономические науки. – 2024. – № 7 (236).
3. *Саадулаева Т.А., Шляхтина И.А.* Цифровой рубль как механизм обеспечения финансовой безопасности государства // Экономика и бизнес: теория и практика. – 2022. – № 13. – С. 111-116.
4. *Королёв В.И.* Архитектурное построение инфраструктуры открытых ключей интегрированного информационного пространства // Безопасность информационных технологий. – 2015. – Т. 22, № 3.
5. *Мельников Д.А.* Методы и средства построения системы управления криптографической защитой на основе инфраструктуры открытых ключей для широкомасштабных информационнотелекоммуникационных систем: автореферат. дисс. … д-ра техн. наук. – М., 2022.

6. *Грачков И.А., Малюк А.А.* Проблемы разработки доверенного программного обеспечения, применяемого на объектах критической информационной инфраструктуры (организационные и методические аспекты) // Безопасность информационных технологий, [S.l.]. – 2019. – P. 56-63.
7. *Мельников Д.А. и др.* Рекомендации по созданию инфраструктуры доверия системы цифрового рубля // Безопасность информационных технологий, [S.l.]. – 2024. – Т. 31, № 3. – С. 43-63.
8. Официальный сайт ВЦИОМ. ВЦИОМ.Новости. – https://wciom.ru/.
9. Концепция цифрового рубля. Банк России. 2021.
10. PKI-кластер. – https://pki-forum.ru/.
11. Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Блочные шифры. ГОСТ Р 34.12─2015.
12. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК от 11 февраля 2013 г. N 17.
13. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Приказ ФСТЭК от 18 февраля 2013 г. N 21.
14. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности. Приказ ФСБ России от 10 июля 2014 г. N 378.
15. ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер". Утверждён Приказом Росстандарта от 08.08.2017 N 822-ст.
16. Официальный сайт ИнфоТеКС. – https://infotecs.ru/.

УДК 004.056

А.Е. Коклянов

Саратовский технический университет имени Гагарина Ю.А.,
Россия, г. Саратов

РАЗРАБОТКА КИБЕРПОЛИГОНА ДЛЯ МОДЕЛИРОВАНИЯ И АНАЛИЗА АТАК НА СЛУЖБУ ACTIVE DIRECTORY

В связи с серьезным увеличением количества инцидентов информационной безопасности и острой нехваткой профильных специалистов возникает потребность в подготовке специалистов по информационной безопасности с практическими навыками работы реагирования на инциденты и нейтрализации уязвимостей – специалистов «Blue Team», а также тех, кто способен понимать действия злоумышленников во время атаки, проверять существующие информационные системы на наличие уязвимостей и имитировать действия злоумышленника – специалистов «Red Team». Для отработки подобных навыков используются киберполигоны, которые представляют из себя систему моделирования компьютерных атак и защиты от них. Данная работа посвящена разработке киберполигона для моделирования и анализа атак на службу Active Directory.

Ключевые слова: *киберполигон, Active Directory, компьютерная атака, домен.*

Due to the major level of information security incidents and the acute shortage of specialized specialists, there is a need to train information security specialists with practical skills in incident response and vulnerability mitigation – Blue Team specialists, as well as those who understand the actions of intruders during detection, determining system indicators for vulnerabilities and simulating the actions of an intruder – Red Team specialists. Cyber-polygon tools were used for testing, which are a system for simulating computer attacks and protecting against them. This work is devoted to the development of a cyber-polygon for simulating and analyzing attacks on Active Directory services.

Keywords: *cyber-polygon, Active Directory, computer attack, domain.*

Киберполигон – это искусственно сконструированная виртуальная среда, которая имитирует реалистичные сети и системы и может применяться для обучения, тестирования, проведения учений или исследований в киберпространстве. Киберполигон имитирует инфраструктуры операционных технологий, критические инциденты безопасности в информационных системах и используемые в обучении информационной безопасности, тренировках и учениях по кибербезопасности. Основное преимущество использования киберполигона заключается в возможности протестировать в безопасной и изолированной виртуальной среде ситуации и стратегии обороны/нападения от кибератак [1].

В киберучениях принимают участие две команды: атакующих («Red Team») и защитников («Blue Team»).

Команда атакующих проводит тестирование на проникновение информационной системы, представленной на киберполигоне. Это является примером наступательной безопасности (Offensive Security) – стратегии, направленной на применении активных мер взлома с целью нахождения уязвимостей компьютерных систем.

Тестирование на проникновение представляет собой тестирование системы на наличие критических уязвимостей и проблем. Данная методика позволяет определить уровень безопасности и оценить устойчивость информационной системы за счет полноценного моделирования атаки хакеров. Пентест проводит атакующая сторона, применяя специализированные программные средства, уязвимости серверов, операционных сред и пр.

Команда защитников занимается вопросом обнаружением, анализом инцидентов кибербезопасности, оперативным реагированием, предотвращением их возникновения и составлением отчетности, также ее называют командой SOC (Security Operation Center/Центр обеспечения безопасности). Необходимостью обучения сотрудников SOC является то, что специалисты получают опыт только из реальных инцидентов, количество которых может быть не так велико.

Функции центра мониторинга безопасности могут отличаться в зависимости от масштаба предприятия и его организационной структуры. Обычна они состоят из этапов, продемонстрированных на рис. 1.

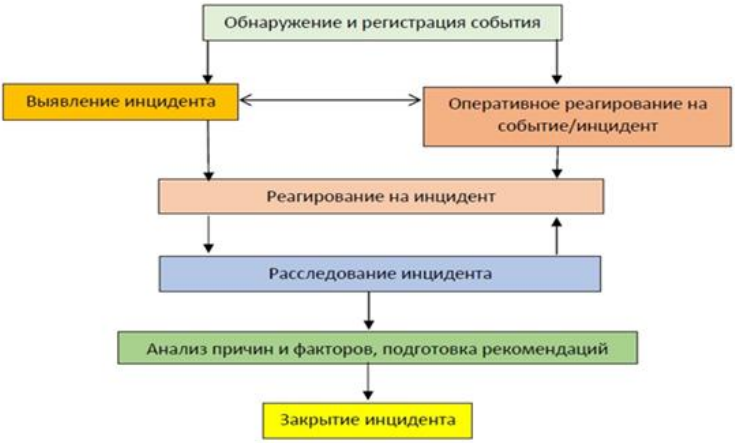


Рис. 1. Схема работы центра мониторинга

Для разработки киберполигона была выбрана примерная архитектура небольшой компании на базе службы Active Directory. Для дальнейшей работы необходимо подробнее рассмотреть понятия Active Directory.

Active Directory – это технология Microsoft, которая представляет собой распределенную базу данных, в которой хранятся объекты в иерархическом, структурированном и безопасном формате. Объекты AD обычно представляют пользователей, компьютеры, периферийные устройства и сетевые службы. Каждый объект уникально идентифицируется своим именем и атрибутами. Домен, лес и дерево представляют собой логические подразделения инфраструктуры AD.

Домены Windows обычно используются в больших сетях – корпоративных сетях или государственных организациях.

В рамках киберучений Active Directory используется как самый популярный инструмент построения работы корпоративных сетей. Главной целью атакующей команды является захват контроллера домена путем эксплуатации уязвимостей и повышения привилегий различными способами.

Домен – это логическая совокупность пользователей и компьютеров, которыми можно централизованно управлять. Доменные имена обычно назначаются с помощью службы доменных имен (DNS), например, xyz.com. [2].

Доверие – это соглашение между двумя доменами, которое определяет разрешения на доступ к объектам в другом домене.

Дерево доменов – это группа доменов, которые совместно используют связанные пространства имен. Например, дочерний домен с именем comp может быть создан в домене sources.com, что приведет к полному имени comp.sources.com. Дочерний домен автоматически формирует двусторонние доверительные отношения с родительским доменом. Однако домен comp.sources.com остается независимым с точки зрения безопасности и репликации. Администраторы домена sources.com не могут управлять доменом comp.sources.com, если им явно не предоставлены необходимые разрешения.

Лес – это крупнейшая организационная структура в Active Directory, состоящая из деревьев доменов, которые совместно используют общую схему (определяющую типы объектов, которые могут быть созданы). Все деревья в лесу связаны двунаправленными доверительными отношениями, что позволяет пользователям в любом дереве получать доступ к ресурсам в других деревьях при наличии соответствующих разрешений. Первый домен, созданный в лесу, назначается корневым доменом и по умолчанию хранит схему. Корневой домен нельзя переименовать или удалить, поскольку это приведет к уничтожению всего леса Active Directory. В отличие от доменов и доверительных отношений, лес не является контейнером или объектом в Active Directory.

Отношения доверия в Active Directory (AD) – это механизмы, которые обеспечивают связь и доверие между различными доменами или лесами. Эти отношения позволяют совместно использовать учетные данные и доступ к ресурсам между доменами или лесами.

Active Directory поддерживает следующие типы отношений доверия:

Двунаправленные доверительные отношения: оба домена или леса доверяют друг другу, что позволяет пользователям и ресурсам беспрепятственно взаимодействовать между собой.

Односторонние доверительные отношения: один домен или лес доверяет другому, но доверие не является взаимным. Например, домен A доверяет домену B, но домен B не доверяет домену A.

Перекрестные доверительные отношения: Active Directory позволяет устанавливать доверительные отношения между различными лесами, расширяя возможность доступа к ресурсам и пользователям через леса.

В контексте Active Directory доверие определяет действия, которые разрешено выполнять объектам безопасности (например, пользователям или группам) из одного домена или леса при доступе к объектам в другом домене или лесу. На рис. 2 указана структура лесов и доменов.

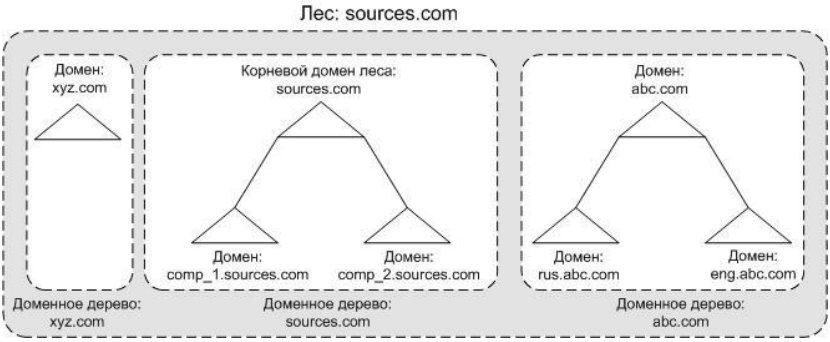


Рис. 2. Структура леса

В работе будут использоваться несколько контроллеров домена, сервер веб-приложений, файловый сервер, сервер баз данных и рабочая станция пользователя.

На рис. 2 представлена схема сети разрабатываемого киберполигона. Киберполигон использует подсеть 10.0.0.0 с маской 255.255.255.0. На киберполигоне используется 3 домена: bank.local, amsterdam.bank.local, secure.local, при этом у домена bank.local есть дочерний домен amsterdam.bank.local, в свою очередь, домен имеет внешнее двустороннее доверие к домену secure.local. Сервер WEB01 будет выполнять роль веб-сервера, на нем будет установлен IIS и SQL-сервер. Сервер FILE01 будет выполнять роль файлово-

го сервера. Сервер DATA01 будет выполнять роль файлового сервера и сервера баз данных. Рабочая станция WS01 может быть доступна удаленно при помощи PSRemoting.

Для проведения атак атакующей машине так же потребуется сетевой доступ к подсети киберполигона.

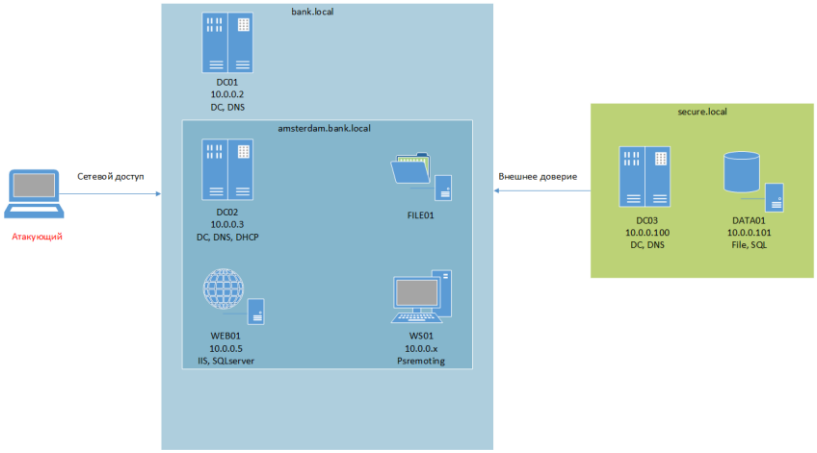


Рис. 3. Схема сети

Сервер DC01 будет выполнять роль контроллера домена и DNS-сервера для домена bank.local. Сервер DC02 будет выполнять роль контроллера домена, DHCP и DNS-сервера для домена amsterdam.bank.local. Сервер DC03 будет выполнять роль контроллера домена и DNS-сервера для домена secure.local.

Контроллер домена (domain controller) – сервер, управляющий доступом к сетевым ресурсам в рамках одного домена (группы сетей или хостов, объединенных общими политиками безопасности).

Контроллер домена осуществляет аутентификацию пользователя в домене, то есть позволяет ему входить в сеть с помощью одной и той же пары логин-пароль с любого включенного в домен компьютера, на котором это не запрещено политиками безопасности или локальными настройками.

Итогом проведения атаки на инфраструктуру является полный захват леса путем получения учетных данных администраторов доменов. Полная структура атаки продемонстрирована на рис. 4.

Для выполнения атак участники команды «Red team» могут использоваться различный утилиты для пентеста, такие как: nmap, crackmapexec, kerbrute, impacket, metasploit. Большинство утилит доступны изначально в специальной операционной системе Kali Linux [3].

Nmap (Network Mapper) представляет собой один из наиболее популярных инструментов для сетевого сканирования и разведки. Он позволяет выявлять активные узлы в сети, определять открытые порты, запущенные сервисы и версии используемого программного обеспечения. Благодаря возможностям скриптового движка (NSE) Nmap также может использоваться для выявления специфических уязвимостей в инфраструктуре.

CrackMapExec (CME) – мощный инструмент для атак на сетевые службы Windows, в частности, для работы с Active Directory. Он позволяет проводить массовый перебор учетных данных, проверять слабые пароли, выявлять доверенные отношения между системами, а также выполнять команды на удаленных хостах при наличии соответствующих привилегий. CrackMapExec является особенно эффективным при эксплуатации уязвимостей, связанных с неправильной конфигурацией протоколов SMB, LDAP и WinRM.

Kerbrute используется для атак на аутентификацию Kerberos. Этот инструмент позволяет осуществлять брутфорс-атаки на учетные записи домена, а также выявлять пользователей, у которых отключена предварительная аутентификация (что делает их уязвимыми к AS-REP Roasting). Kerbrute полезен на начальном этапе атаки, когда необходимо получить список пользователей Active Directory и проверить их пароли.

Impacket представляет собой набор инструментов для работы с сетевыми протоколами, включая SMB, LDAP, RPC и Kerberos. Одним из наиболее известных модулей Impacket является secretsdump.py, который позволяет извлекать хэши паролей из базы данных SAM и реестра Windows. Также в составе Impacket присутствуют утилиты для атак на доверенные отношения в домене, такие как mimikatz-like wmiexec.py и dcomexec.py, обеспечивающие удаленное выполнение команд без необходимости интерактивного входа в систему.

Metasploit Framework – один из наиболее мощных и гибких инструментов для тестирования на проникновение. Он включает в себя обширную базу эксплойтов, полезных нагрузок (payloads) и вспомогательных модулей, позволяющих автоматизировать эксплуатацию уязвимостей. В контексте атак на Active Directory Metasploit может использоваться для эксплуатации уязвимостей SMB (например, EternalBlue), выполнения атак на учетные записи Kerberos, а также для пост-эксплуатации после успешного получения доступа к системе.

При помощи, подключенной к инфраструктуре SIEM системе можно отслеживать шаги проводимой атаки, это необходимо для расследования инцидентов командой «Blue team», а также для анализа действий «Red team», что поможет развитию навыком участников киберучений на киберполигоне.

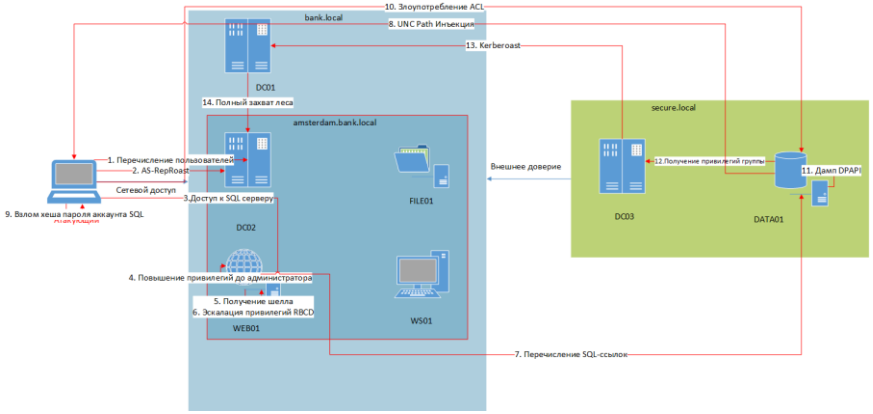


Рис. 4. Структура атаки

Рассмотрим этапы атаки на инфраструктуру подробнее.

Атака начинается с разведки, в ходе которой злоумышленник собирает сведения о пользователях, группах безопасности и сетевых сервисах. Это может быть осуществлено путем отправки LDAP-запросов, анализа RPC-интерфейсов или использования инструментов, таких как BloodHound, позволяющих построить карту сетевого взаимодействия. Полученная информация дает возможность идентифицировать учетные записи, обладающие особыми привилегиями, и определить возможные пути эскалации прав.

Одним из распространенных методов атак на учетные записи является AS-REP Roasting. В случае если у пользователя отключена предварительная аутентификация в Kerberos, злоумышленник может запросить для него AS-REP билет и извлечь его хэш. Данный хэш может быть подвергнут офлайн-атаке перебором, что позволяет восстановить исходный пароль. Подобным образом функционирует атака Kerberoasting, но в данном случае целью становятся сервисные учетные записи, для которых злоумышленник получает билеты TGS, содержащие их пароли в зашифрованном виде. Обе атаки эффективны в условиях слабой парольной политики и отсутствия мониторинга аномальных запросов Kerberos.

SQL Server, часто используемый в корпоративных средах, представляет собой еще один важный элемент атаки. Получение доступа к нему может быть осуществлено различными способами, включая перехват учетных данных, эксплуатацию слабых паролей или уязвимостей. Если атакующему удается повысить свои привилегии до уровня системного администратора (sysadmin), он получает возможность выполнять произвольные команды на сервере. Это делает SQL Server удобной точкой для горизонтального пере-

мещения по сети. В частности, злоумышленник может использовать функции xp_cmdshell или SQL Server Links для выполнения команд в контексте другого сервера, что позволяет расширять контроль над инфраструктурой.

Одной из критически опасных атак является эксплуатация механизма Resource-Based Constrained Delegation (RBCD). Эта уязвимость позволяет атакующему управлять учетными данными других сервисов, перенаправляя аутентификацию Kerberos в свою пользу. В сочетании с манипуляцией списками управления доступом (ACL), это может привести к получению контроля над ключевыми учетными записями домена. В дальнейшем злоумышленник может использовать инструменты DCSync или DCShadow для кражи данных из контроллеров домена или даже модификации их структуры.

Заключительным этапом атаки становится установление полного контроля над доменом или лесом Active Directory. На данном этапе атакующий получает возможность создавать новые учетные записи, изменять политики безопасности, скрывать свою активность и обеспечивать постоянное присутствие в системе. Такой сценарий представляет наибольшую угрозу, так как может привести к компрометации всей корпоративной сети.

Для защиты от подобных атак необходимо реализовывать комплексный подход, включающий усиление аутентификации, ограничение привилегий учетных записей, мониторинг активности в сети и своевременное выявление аномальных действий. Использование современных механизмов защиты, таких как многофакторная аутентификация, контроль запросов Kerberos и мониторинг событий безопасности в AD, значительно снижает вероятность успешной реализации атаки.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Киберполигон — мультифункциональный комплекс для проведения киберучений // habr.com: сайт. – URL: https://habr.com/ru/articles/80586/ (дата обращения: 20.02.2025).
2. Active Directory. Леса, домены и доверительные отношения // sources.ru: сайт. – URL: https://sources.ru/magazine/1207/2.html (дата обращения: 20.02.2025).
3. *Журавлева В.В., Ткаченко А.Л.* Пентест и его особенности // Дневник науки. – 2023. – № 11 (83). – EDN LVKQBS.
4. Hacker, Ralf Active Directory глазами хакера / Ralf Hacker. – СПб.: БХВ-Петербург, 2021. – 176 с.

УДК 004.056.2

Д.Р. Кулиш, Е.А. Маро

Южный федеральный университет, Россия, г. Таганрог

ПАРАМЕТРЫ И ИНСТРУМЕНТЫ ДЕТЕКТИРОВАНИЯ DEEPFAKE ИЗОБРАЖЕНИЙ

Инструменты, основанные на искусственном интеллекте (ИИ), имеют важное значение в современном мире информационных технологий и пользуются популярностью не только в области повышения производительности и качества труда ИТ-специалистов, но и в задачах киберпреступников. Повышенное внимание и востребованность решений на базе ИИ приводит к быстрому развитию методов и алгоритмов обучения подобных систем. Как результат, некоторые из инструментов на базе ИИ стали неотъемлемой частью жизни пользователей в наше время. В последние годы технологии DeepFake являются предметом высокого беспокойства по поводу их потенциального использования злоумышленниками для дезинформации и манипуляции общественным мнением, а также мошенничества и влияния на механизмы безопасности информационных систем (например, методы аутентификации, мониторинг уязвимостей и т.д.). Данная статья посвящена исследованию параметров, используемых для обнаружения изображений, сгенерированных с помощью инструментов DeepFake, а также сравнительному анализу существующих инструментов детектирования подобных изображений.

Ключевые слова: *DeepFake, информационная безопасность, поддельное изображение, обнаружение манипуляций с изображением.*

Artificial intelligence (AI)-based tools play a crucial role in the contemporary landscape of information technology, gaining popularity not only in enhancing the productivity and quality of work among IT professionals but also in the activities of cybercriminals. The increased attention and demand for AI-driven solutions have led to the rapid development of methods and algorithms for training such systems. As a result, some AI-based tools have become an integral part of users' lives today. In recent years, DeepFake technologies have raised significant concerns regarding their potential misuse by malicious actors for disinformation and manipulation of public opinion, as well as for fraud and undermining the security mechanisms of information systems (e.g., authentication methods, vulnerability monitoring, etc.). This article is dedicated to the investigation of parameters used for detecting images generated by DeepFake tools, as well as a comparative analysis of existing detection tools for such images.

Keywords: *DeepFake, information security, fake image, image manipulation detection.*

Введение

В последнее время активное развитие получили технологии, связанные с искусственным интеллектом. Обычный пользователь регулярно сталкивается с интеллектуальными системами работы с изображениями: поиск по изображению и распознавание текста или отдельных блоков изображений на них, персонализация социальных сетей под пользователя и так далее. Также подходы на основе использования ИИ имеет широкое применение в таких областях, как здравоохранение, образование, транспорт, культура и многих других. Однако достижения в области Deep Learning алгоритмов стали использовать в программном обеспечении, создающем потенциальные угрозы с точки зрения информационной безопасности.

DeepFake – это технология, которая использует методы искусственного интеллекта для создания видео, аудио или другого цифрового контента, который выглядит аутентичным, но на самом деле является поддельным (полностью или частично). При помощи технологии DeepFake можно в высокой степенью реалистичности заменить на фотографиях или видеоконтенте лицо одного субъекта на лицо другого субъекта и/или синтезировать речь (имитация голоса), имея в распоряжении достаточно короткую запись видеозапись (образцы лица и голоса). Злоумышленники могут использовать разработки инструментов DeepFake для получения материала, который позволит манипулировать общественным мнением и сознанием, приведет к дискредитации субъектов или мошенничеству [1, 2]. Подходы на основе использования DeepFake инструментов могут применяться в преступлениях в политической сфере: пропаганда, продвижение террористических идей, подрыв суверенитета страны и многих других.

По прогнозам компании Gartner [3], к 2026 году атаки с использованием DeepFake, созданных с помощью искусственного интеллекта, на биометрические данные лица приведут к тому, что 30% предприятий перестанут рассматривать такие решения для верификации и аутентификации личности как надежные при использовании в дистанционном формате. Процессы верификации и аутентификации личности с использованием биометрических данных лица в настоящее время опираются на presentation attack detection (PAD) для оценки живости пользователя. Современные стандарты и процедуры тестирования, предназначенные для определения и оценки механизмов PAD, не охватывают атаки цифровой инъекции, использующие DeepFake, созданные с помощью искусственного интеллекта, которые могут быть сгенерированы в настоящее время. По данным из отчета компании iProov [4], занимающейся разработкой решений биометрической аутентификации для обеспечения безопасности в сети интернет, в 2023 году использование DeepFake и инструментов для подмены метаданных выросло на 672%. Суммарно с остальными типами атак, на мобильных платформах

число подобных атак увеличилось на 255%. Данные показатели свидетельствуют об активном развитии киберпреступности в области применения DeepFake инструментов. Данная тенденция во многом обусловлена стремительным эволюционирование генеративных нейронных сетей и технологий обучения. При этом подобные технологии достаточно легкодоступны, их производительность увеличивается год от года, а результаты генерации цифрового контента все сложнее отличимы от достоверных образцов.

В некоторых случаях для того, чтобы проверить достоверность и целостность объекта при его обработке с помощью технологии DeepFake, достаточно визуального контроля пользователя по ключевым признакам. Однако инструменты для DeepFake постоянно совершенствуются, усложняя задачу выявления поддельных изображений только визуально. С целью повышения уровня качества и эффективности детектирования сгенерированных фото, видео и аудио материалов разрабатывается программное обеспечение, анализирующее такие параметры цифрового контента, как аномалии данных, наличие артефактов сжатия и другие характерные признаки, свойственный распространенным инструментам DeepFake.

В рамках данной статьи представлен обзор существующих параметров выявления наличия вмешательства DeepFake инструментов на изображениях и способы их обнаружения. Приведено подробное описание признаков наличия сгенерированного контента с помощью визуального контроля оператором (субъектом). Представлены технические характеристики изображений, по которым осуществляется детектирование DeepFake вмешательства. Проведен обзор существующих инструментов детектирования сгенерированных изображений.

Методы обнаружения DeepFake: визуальный контроль оператором

Некоторые нейронные сети, используемые для генерирования DeepFake изображений, недостаточно корректно разработны алгоритмически, либо содержат ошибки (неполное описание) в обучающих наборах. Качество создаваемого контента во многом зависит от имеющейся базы данных (обучающего набора). Ограниченный набор, состоящий из некачественных сведений, не предоставляет возможности достаточно детально обучить систему. Также часто пользователи сталкиваются с проблемой недообучения или переобучения в DeepFake инструментах. В первом случае система упускает особенности медиа контента, во втором – возникают проблемы обобщения при расширении баз данных [5]. Эти и другие недостатки могут встречаться как по отдельности, так и в комбинациях для анализируемых средств генерации цифрового контента.

Сгенерированные с помощью ИИ (с низким качеством обучения) изображение человек способен распознать, не прибегая к специализированным программным продуктам. Для этого ему достаточно использовать органы зрения и методики, специализированные под дефекты обучения DeepFake системы. Рассмотрим признаки, на которые оператору необходимо обращать внимание для предположения о вероятной подделке изображений.

Первая особенность фотографий, обработанных или сгенерированных с помощью распространенных нейронных сетей, касается проработки текстур. Превалирующая доля технологий DeepFake имеют недостаточный объём сведений или степень обученности на построение различных типов кожи. Кожа субъекта на поддельном изображении получается неестественного цвета, её структура чрезмерно сглажена либо наоборот имеет нереалистичный рельеф. Несмотря на количество высококачественных образцов цифровой информации о тканях и всевозможных покрытиях возникают некорректные ситуации при генерации данных текстур: внезапные нитки в некорректных сегментах покрытия, видоизмененные швы, неравномерные блики. В зависимости от уровня совершенствования обученности нейронной сети подобные детали либо сразу же заметны невооруженным взглядом, некоторые требуют более внимательного рассмотрения изображения.

Следующий факт подделки касается глаз. Неестественные, толстые веки, склеенные ресницы, отсутствие бликов – довольно заметны простому человеческому взгляду. Отдельное внимание стоит уделить зрачкам. Не чёткий контур, отличие в размере, форме, отклонение от норм положения. По ним достаточно легко определить фальсифицировано изображение или нет.

При оценке достоверности и подлинности изображения не стоит забывать о анатомической правильности построения пропорций и тела человека в целом. Инструментам DeepFake, в особенности низкого уровня обученности, свойственно формировать специфические ошибки (обусловленные алгоритмом генерации), например, в количестве пальцев, положении конечностей и так далее. Многие инструменты DeepFake выделяются неправильным воспроизведением пропорций тела субъекта [6].

В качестве примера генерируемого изображения рассмотрим представленное на рис. 1 фото девушки. Из наиболее очевидных признаков, заметных при первом взгляде на изображении, частичное размытие рукавов одежды, хаотичные волоски на лбу, анатомически неправильное положение пальцев рук и их пропорции. Также кожа на изгибах имеет неестественные заломы. При более детальном рассмотрении, обнаруживается нарушение структуры вязанного ряда: нарушение последовательности петель, либо переход в нечеткий образ, в котором повторяется изначальная текстура.

Рис. 1. Пример анализируемой фотографии, сгенерированной с помощью DeepFake инструмента

Заключительным из обсуждаемых параметров сгенерированных DeepFake изображений, которые легко обнаружить без использования специализированного программного обеспечения, является искажение свойств и смысла изображенных объектов. Зависшая в воздухе бутылка масла, дорожный знак по середине парка, бессмысленные наборы букв – подобные характеристики выдают недостоверный цифровой контент.

Как видно из описания выше, критерии, указывающие на применение DeepFake инструментов, достаточно разнообразны. Для более качественной проверки подлинности изображения проводится анализ цифровых следов и артефактов, описание которых представлено в следующем разделе.

Методы обнаружения DeepFake: цифровые следы

Для развития нейронных сетей разрабатываются новые архитектуры, эффективные методы обучения, подбираются расширенные базы их качественных материалов. Тем не менее, технология deepfake оставляет следы своего воздействия, по которые выявляются с помощью специализированного программного обеспечения. Такие отпечатки затрагивают структуру, деформации, параметры сжатия. Среди наиболее распространенных и достоверных методов по обнаружению DeepFake выделяются анализ шумов.

Каждое устройство обработки изображений (например, фотоаппарат) оставляет уникальный и устойчивый рисунок на каждом изображении из-за несовершенства различных этапов процесса получения изображения. Такие паттерны известны как паттерны неоднородности фотореакции (PRNU) [7]. Чаще всего паттерны выглядят как различные закономерности в шумах. Обычно шумы образуются по причине низкого освещения, высокого значения ISO или технических ограничений камеры. Их положение случайно и равномерно по всему объекту в виде зернистости или мелких точек. Шумы,

возникшие при генерации изображений с помощи CNN и GAN, чаще распределены неравномерно, создавая сетку или повторяющиеся узоры в критических зонах: глаза, рот, руки и т.д. [8]. На рис. 2 представлено сравнение отпечатков нескольких моделей камер и генеративных сетей.

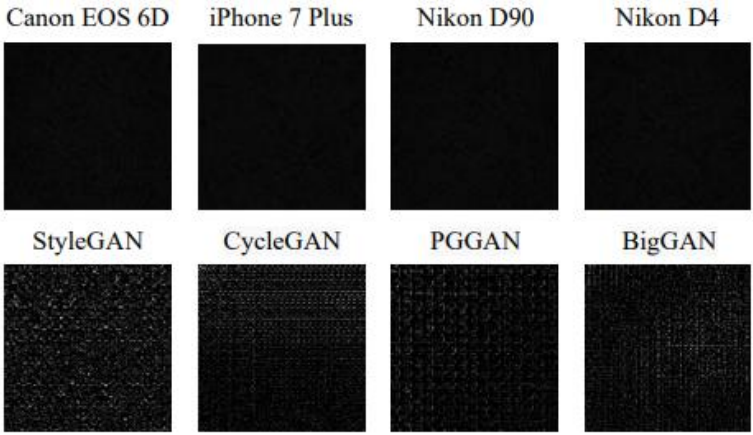


Рис. 2. Отпечатки при анализе шума на изображениях

У созданных с помощью инструментов DeepFake изображений шумы образуют некоторую структуру, напоминающую шахматную доску. Это связано со слоями деконволюции, которые являются основными образующими компонентами в GAN. Подобные узоры складываются из-за наложения, которое возникает, когда размер ядра окна проекции транспонирующей свертки не делится на шаг. Рисунок усиливается при наложении нескольких слоёв.

Есть технические параметры DeepFake объектов, обнаружение которых требует сложных преобразований, однако они позволяют с высоким уровнем точности детектировать генерацию и вмешательство в изображение. Частоты, возникающие при дискретном преобразовании Фурье, позволяют анализировать различные составляющие элементы изображения. Они подразделяются на низкие, средние и высокие частоты, описывающие скорость изменения яркости изображений. В первую группу входят большие поверхности сплошного цвета, содержащие информацию о крупных формах и общих структурных элементах композиции. Детализацию, объём, глубину и сложность изображению придают представители средней группы частот. Они применимы в областях разных структур: кожа, ткани, фактурные элементы и т.д. Четкость и резкость изображений определяют высокие частоты. Они располагаются в местах быстрой смены скорости света, что позволяет воспроизводить мелкие компоненты. Именно высокочастотные показа-

тели чаще всего указывают на вмешательство с помощью технологий DeepFake и выделяются на частотном портрете аномалиями. Спектрограммы достоверной фотографии и сгенерированного изображения будут значительно отличаться (рис. 3, 4).

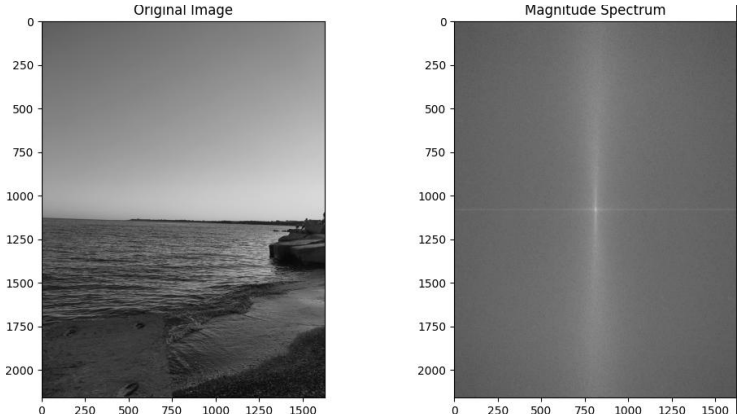


Рис. 3. Спектрограмма реальной фотографии

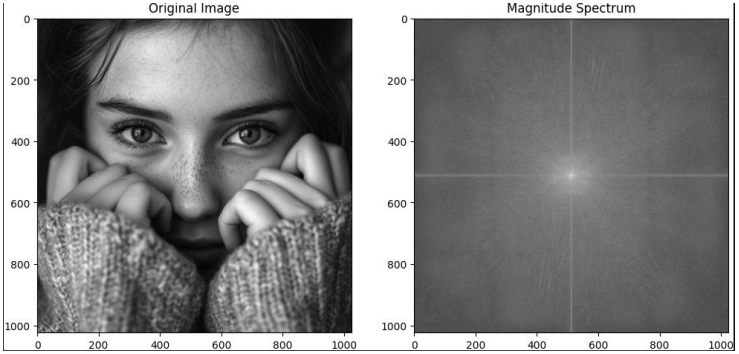


Рис. 4. Спектрограмма сгенерированного изображения

Схема реальной фотографии отражает равномерное распределение частот. Спектрограмма DeepFake изображения отличается от реального снимка наличием всплесков высоких показателей в различных зонах. Данные всплески иногда формируют некоторый рисунок или узор. Подобные скачки на спектрограммах свидетельствуют о модификации или недостоверности исходного цифрового объекта.

Инструменты автоматизированного выявления DeepFake изображений

Рынок автоматизированных инструментов по детектированию изображений, сгенерированных с помощью deepfake инструментов, непрерывно развивается. Они разделяются на продукты общего и узконаправленного пользования.

К продуктам общего назначения можно отнести следующие 10 программных решений (рис. 5) в области выявления использования DeepFake инструментов [9]:

1. Sentinel.
2. Sensity.
3. Oz Liveness.
4. WeVerify.
5. HyperVerge.
6. Intel's FakeCatcher.
7. Microsoft Video AI Authenticator.
8. Deepware.
9. Phoneme-Viseme Mismatches.
10. DuckDuckGoose.

Рис. 5. Автоматизированные решения в области выявления использования DeepFake инструментов

Среди специализированных сервисов выделяются разработки российской компании «ОТ-КОНТАК», представляющие комплекс средств по криминалистическому анализу разных типов медиа контента. Особый интерес вызывает система профессиональных инструментов «VD Expert». В ней предоставляется ряд инструментов, позволяющих проводить экспертизы и сбор доказательств с изображений: гистограммы цветовых каналов, интегральной яркости, градиентные, медианные, автодиапазонные фильтры, анализ ELA. Разработка предоставляет экспертам возможности по повышению качества изображений, установлению источника материала, идентифи-

кации устройства и т.д. Функционал оформлен в удобном и интуитивно понятном графическом интерфейсе. Компания предоставляет необходимые материалы и обучение использованию продукта, что повышает удобство пользователей. Также на платформе представлены системы по работе с видео и аудио контентом.

Научным сообществом разрабатываются новые технологии и способы детектирования DeepFake. Наиболее распространенными и активно развивающимися направлениями являются две категории подходов: базирующихся на алгоритмах глубокого обучения и алгоритмах машинного обучения.

Современные модели, связанные с системой компьютерного зрения на основе глубокого обучения (Vision Transformer, ViT), обладают рядом преимуществ, а именно имеют более высокую способность к изучению сложных признаков, низкую индуктивную предвзятость, используют механизмы самовнимания. Решение Xception является сверточной нейронной сетью, глубиной в 71 слой. Она отличается повышенной точностью при распознавании объектов с компактной архитектурой. Данные решения были в 2022 году объединены во фреймворк ViXNet [10].

Каждая из рассмотренных платформ активно развивается, собираются новые сведения для формирования баз данных об артефактах различных DeepFake алгоритмов, усложняется архитектура, добавляются новые комплексные подходы и методы детектирования.

Заключение

Технологии, работа которых основана на искусственном интеллекте, активно развиваются и распространяются в разные сферы жизни общества. Им нашли как положительные, так и негативные способы применения. Сгенерированные с помощью DeepFake изображения используют для шантажа, манипуляций общественным мнением, дискредитации граждан и отдельных слоев населения. Однако синтезирующие изображения сети не являются совершенными. Недостаточные базы данных, непроработанные архитектуры, ненормированная степень обученности – подобные качества оставляют следы на цифровых объектах, подвергнутых обработке. Среди них искажение пикселей, неоднородные шумы, складывающиеся в различные узоры, поврежденные метаданные и тому подобное.

На данный момент имеются программные продукты, позволяющие детектировать DeepFake, предоставляющие собой системы инструментов по анализу цифровых следов, артефактов, неестественности текстур, положения объектов на изображениях. Для повышения эффективности и качества решений в качестве основных технологий используются предобученные свёрточные и генеративно-состязательные нейронные сети.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Исакова А.Г., Осин А.В.* Применение искусственного интеллекта в расследовании преступлений с использованием технологии «Дипфейк» // Международный научный журнал «ВЕСТНИК НАУКИ». – 2024. – Т. 3, № 1 (70). – С. 235-242.
2. *Довгаль В.А.* Применение глубокого обучения для создания и обнаружения поддельных изображений, синтезированных с помощью искусственного интеллекта // Научный журнал «Вестник АГУ». – 2021. –№ 4 (291). – С. 82-94.
3. Gartner Press Release. – https://www.gartner.com/en/newsroom/press-releases/2024-02-01-gartner-predicts-30-percent-of-enterprises-will-consider-identity-verification-and-authentication-solutions-unreliable-in-isolation-due-to-deepfakes-by-2026.
4. «New threat intelligence report reveals 704% increase in face swap attacks» [Электронный ресурс]. – Режим доступа: https://fintech.global/2024/02/07/new-threat-intelligence-report-exposes-the-impact-of-genai-on-remote-identity-verification/, свободный (дата обращения: 01.03.2025).
5. *Yuanchen Niu, Yuanman Li, Bin Li, Xia Li*. Deepfake:A Comprehensive Survey of Generation and Detection Methods // Chinese Computer Sciences Review. – 2024. Vol. 2 (3). – P. 24-37. – doi: 10.48014/ccsr.20240102002 (in Chinese).
6. «Как определить сгенерированное изображение: Полное руководство» [Электронный ресурс]. – Режим доступа: https://vc.ru/life/1129222-kak-opredelit-sgenerirovannoe-izobrazhenie-polnoe-rukovodstvo/, свободный (дата обращения: 01.03.2025).
7. *Jiameng Pu, Neal Mangaokar, Bolun Wang, Chandan K. Reddy, Bimal Viswanath*. NoiseScope: Detecting Deepfake Images in a Blind Setting [Электронный ресурс]. – Режим доступа: https://people.cs.vt.edu/~reddy/papers/ACSAC20.pdf, свободный (дата обращения: 09.03.2025).
8. *Patel Y. et al.* An Improved Dense CNN Architecture for Deepfake Image Detection // in IEEE Access. – 2023. – Vol. 11. – P. 22081-22095. – doi: 10.1109/ACCESS.2023.3251417.
9. *Rana M.S., Nobi M.N., Murali B. and Sung A.H.* Deepfake Detection: A Systematic Literature Review // in IEEE Access. – 2022. – Vol. 10. – P. 25494-25513. – doi: 10.1109/ACCESS.2022.3154404.
10. *Fakhar Abbas, Araz Taeihagh*. Unmasking deepfakes: A systematic review of deepfake detection and generation techniques using artificial intelligence // Expert Systems with Applications. – 2024. – Vol. 252. – Part B. – https://doi.org/10.1016/j.eswa.2024.124260.

УДК 004

Ю.П. Леонтьева

ИССЛЕДОВАНИЕ СВОЙСТВ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ, ЛЕЖАЩИХ В ОСНОВЕ БЛОКЧЕЙН СИСТЕМ

В статье рассматриваются свойства эллиптических кривых, лежащих в основе криптографических алгоритмов, используемых в блокчейн-системах. Основное внимание уделено анализу порядка точек и порядка группы точек кривой над конечными простыми полями малого размера. С помощью программного моделирования проведён подбор кривых и точек, удовлетворяющих критериям криптографической стойкости, таким как большой порядок, малое отклонение от значения, предсказанного теоремой Хассе, и равномерное распределение порядков точек. Полученные результаты подтверждают наличие закономерностей, аналогичных тем, что наблюдаются в кривых над большими полями. Работа демонстрирует возможность использования малых модулей для предварительного анализа свойств кривых и выбора безопасных параметров. В дальнейшем планируется выявить и формализовать устойчивые правила выбора модулей и точек, обладающих необходимыми криптографическими свойствами.

Ключевые слова: *Эллиптические кривые, криптография, блокчейн, порядок группы точек, проблема дискретного логарифма, теорема Хассе.*

This paper explores the properties of elliptic curves that form the basis of cryptographic algorithms used in blockchain systems. The focus is placed on analyzing the order of points and the order of elliptic curve groups over small prime fields. Through programmatic modeling, curves and points satisfying key cryptographic security criteria—such as large point order, small deviation from the value predicted by Hasse's theorem, and uniform point order distribution—were identified. The results confirm the presence of patterns similar to those found in elliptic curves over large fields. The study demonstrates the feasibility of using small prime fields for preliminary analysis of curve properties and for selecting secure cryptographic parameters. Future work will aim to identify and formalize consistent rules for selecting modules and points with strong cryptographic properties.

Key words: *Elliptic curve cryptography, public-key cryptography, blockchain systems, group order of points, elliptic curve discrete logarithm problem (ECDLP), Hasse's theorem.*

Криптография – наука о методах преобразования информации для её защиты при передаче по незащищённым каналам связи и о способах практической реализации этих методов.

Криптография с открытым ключом — это метод защиты цифровой связи с помощью пары ключей: открытого ключа и закрытого ключа. В отличие от симметричного шифрования, где один и тот же ключ используется и для шифрования, и для дешифрования, шифрование с открытым ключом гарантирует, что эти процессы будут выполняться двумя отдельными, но математически связанными ключами. Открытый ключ находится в открытом доступе и используется для шифрования данных, а закрытый ключ остаётся конфиденциальным и используется для расшифровки данных.

Криптография на эллиптических кривых (ECC) – это подход к криптографии с открытым ключом, основанный на алгебраической структуре эллиптических кривых над конечными полями.

Эллиптическая кривая – это набор точек, описывающихся уравнением Вейерштрасса (1):

$$y^2 = x^3 + ax + b, \quad (1)$$

где $a, b \in \mathbb{F}_p$.

Эллиптические кривые, для которых выполняется неравенство (2), называются гладкие и используются в криптографии.

$$4a^3 + 27b^2 \neq 0. \quad (2)$$

Точка эллиптической кривой – пара координат (x; y), удовлетворяющая заданному уравнению кривой.

Группа точек эллиптической кривой — это множество точек эллиптической кривой над конечным полем порядка p ($\mathbb{F}_p$), дополненное бесконечно удалённой точкой O, вместе с операцией сложения, которая удовлетворяет следующим свойствам (где P, Q, R – точки на кривой):

1. Замкнутость – сумма двух точек на кривой также принадлежит кривой.
2. Ассоциативность – $(P + Q) + R = P + (Q + R)$
3. Наличие нейтрального элемента – бесконечно удалённая точка O действует как нулевой элемент: $P + O = P$.
4. Наличие обратного элемента – для любой точки: $P(x, y)$ существует $-P(x, -y)$, такая что $P + (-P) = O$.
5. Коммутативность – $P + Q = Q + P$.

Над точками эллиптической кривой может выполняться несколько операций. Сложение двух разных точек эллиптической кривой представляет собой отражение точки R' пересечения прямой, проходящей через P и Q, и имеет вид уравнения (3).

$$P + Q = R, \quad (3)$$

где $P(x_1, y_1) \neq Q(x_2, y_2)$ и $P, Q \in \mathbb{F}_p$.

Сложение двух одинаковых точек эллиптической кривой (сложение точки с самой собой) представляет отражение точки R' пересечения касательной, проходящей через P и имеет вид уравнения (4).

$$P + P = R, \tag{4}$$

где $P(x_1, y_1)\ \epsilon\ \mathbb{F}_p$.

Умножение точки эллиптической кривой на скаляр есть сложение точки с самой собой n раз. В уравнении (5) приведён пример умножения точки на 4.

$$4P = P + P + P + P, \tag{5}$$

Таким образом, умножение точки на скаляр n есть сложение точки с самой собой n раз [1].

Множество точек эллиптической кривой над конечным полем образует абелеву группу по операции сложения. Эта группа имеет конечный порядок, и её структура напрямую влияет на надёжность криптографических алгоритмов.

Порядок группы – это количество всех точек на кривой, включая нейтральную точку O. Обозначим это число как $E(\mathbb{F}_p)$. Существует теорема Хассе (6) [2], которая даёт оценку количества точек:

$$\left|E\left(\mathbb{F}_p\right) - (p+1)\right| \leq 2\sqrt{p}. \tag{6}$$

Порядок точки – это наименьшее положительное целое n, такое что $nP = O$. Каждая точка на кривой принадлежит циклической подгруппе, порождённой этой точкой.

Выбор криптографических параметров должен обеспечивать, чтобы порядок точки (или всей группы) был большим простым числом – это делает невозможным применение ряда атак на ECC.

Ключевая задача, определяющая безопасность ECC, – проблема дискретного логарифма на эллиптической кривой (ECDLP):

Пусть даны точка P и её кратное $Q = kP$, где k – некоторое неизвестное число. Требуется найти k.

В отличие от аналогичной задачи в мультипликативных группах (например, в RSA), задача ECDLP считается значительно более сложной при меньших длинах ключей. Не существует эффективных алгоритмов, способных решать её за разумное время, если параметры выбраны корректно (например, порядок группы – большое простое число) [3].

Для примера: при использовании кривой secp256k1 (стандарт в Bitcoin), длина скалярного множителя k составляет 256 бит. Перебор всех возможных значений k занимает $\sim 2^{256}$ шагов, что практически невозможно даже для современных суперкомпьютеров.

Таким образом, в криптографических протоколах, основанных на эллиптических кривых, основная операция – это умножение точки на скаляр: вычисление $Q = kP$, где P – базовая точка, а k – приватный ключ. Безопасность алгоритма основывается на невозможности найти k, зная только P и Q, то есть на сложности проблемы дискретного логарифма.

Однако эффективность этой задачи напрямую зависит от порядка точки P – т.е. наименьшего положительного числа n, при котором $nP = O$.

В данной работе тестируется гипотеза о том, что свойства малых чисел так же присущи и большим числам, используемым в реальной криптографии. Анализ «плохих точек» для малых простых модулей позволит выявить закономерности, в дальнейшем применимые к большим числам. Под «плохой точкой» понимается такая точка на кривой, которая, будучи последовательно сложенной сама с собой, возвращается к исходному значению за малое число шагов. Это значит, что её порядок n мал. Такая точка порождает малую циклическую подгруппу, и все значения kP для неё будут лежать в пределах всего n возможных значений.

Посредством программного кода на для всех простых модулей $p \leq 500$ были получены:

- Порядок группы $E(\mathbb{F}_p)$.
- Порядок точек n.

На рис. 1 представлен график зависимости количества точек на эллиптической кривой от модуля p. Мы видим, что, количество точек колеблется вблизи значения p, как и предсказывает теорема Хассе. Наблюдается прямая зависимость роста порядка от модуля.

Рис. 2. Зависимость порядка группы $E(\mathbb{F}_p)$ от модуля p

Однако, больший интерес представляет отклонение порядка группы от модуля, график которого представлен на рис. 2. Если порядок сильно меньше модуля, это это представляет угрозу для безопасности, поскольку:

- Малая группа элементов приводит к уменьшению количества точек, что, в свою очередь, сокращает количество возможных ключей.
- Атаки, такие как метод полного перебора (brute-force) и алгоритм Baby-step Giant-step, становятся более эффективными и быстрыми.
- Такой порядок значительно облегчает задачу факторизации.

Рис. 3. Отклонение порядка группы $E(\mathbb{F}_p)$ от модуля p

Среди выбранных простых модулей $p \leq 500$ наблюдается крайне малое количество модулей, полностью соответствующих критериям безопасности:

- Отклонение порядка группы от модуля удовлетворяет теореме Хассе.
- Все точки имеют ненулевой конечный порядок.
- Порядок всех точек одинаковый.
- Порядок всех точек приближен к порядку группы.

В табл. 1 приведены все модули, удовлетворяющие вышеперечисленным условиям. Среди полученных данные так же можно произвести отбор по величине порядка точки n. Поскольку именно от него зависит надёжность криптографических алгоритмов за счёт слишком долгого перевора приватного ключа.

Таблица 1

Выборка модулей p, удовлетворяющих критериям безопасности

Модуль p	Порядок группы $E(\mathbb{F}_p)$	Отклонение $E(\mathbb{F}_p)$ от p	Порядок точки n (равный для всех точек)
7	6	1	4
37	36	1	13
61	60	1	61
67	78	11	40
79	66	7	67
103	108	5	37
109	126	17	15
127	126	1	8
211	198	13	100
307	324	17	37
397	396	1	45
433	396	37	45
457	486	29	163

В большинстве стандартов, например, secp256k1, намеренно выбираются кривые с группой большого порядка и базовую точку с тем же порядком. Это максимизирует безопасность [4].

Таким образом, исследование малых модулей позволяет изучать свойства эллиптических кривых просто и быстро. Полученные результаты подтверждают, что даже при работе с малыми модулями можно выявить значимые тенденции, аналогичные тем, что проявляются в больших полях, применяемых в реальных блокчейн-системах. Это даёт основание использовать подобный подход в качестве моделирования и предварительной проверки свойств эллиптических кривых. В дальнейшем планируется расширить проведённое исследование и сосредоточиться на выявлении устойчивых закономерностей и формулировке общих правил для выбора «хороших» модулей и точек. Целью является создание набора критериев, позволяющих заранее оценивать криптографическую стойкость кривой и минимизировать риски, связанные с потенциально слабыми параметрами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Маховенко Е.Б. Теоретико-числовые методы криптографии. – М.: Гелиос АРВ, 2006. – 320 с.
2. *Hasse H.* Über die Anzahl der Punkte einer algebraischen Kurve über endlichem Körper // Mathematische Annalen. – 1933. – Bd. 108. – S. 48-68.
3. *Обухов В.А.* Криптография на основе эллиптических кривых (ECC) // Al-Farg'oniy avlodlari. – 2023. – № 4.
4. *Анисимова Э.С.* Использование эллиптических кривых в стандарте цифровой подписи // Актуальные проблемы гуманитарных и естественных наук. – 2015. – № 1-1.

УДК 00. 182

С.И. Макаров

Южный федеральный университет, Россия, г. Таганрог

РЕАГИРОВАНИЕ НА RANSOMWARE-ИНЦИДЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФРАСТРУКТУРЕ КОМПАНИИ

Цель и задачи научно-исследовательской работы проанализировать поведение вирусного программного обеспечения (ВПО) и описать сценарий реагирования на компьютерные инциденты.

Ключевые слова: *реагирование на инциденты, инциденты информационной безопасности, компьютерный вирус, сценарий реагирования*

The purpose and objectives of the research work are to analyze the operation of virus software and describe the scenario of response to computer incidents.

Keywords: *incident response, information security incidents, computer virus, response scenario.*

Введение

С развитием информационных технологий все чаще начали встречаться информационные мошенники. Такие люди хотят обогатиться за счет разработок других людей или компаний. Для этого они создают разного рода вредоносные программы обеспечения (ВПО), которые могут проникать в систему пользователей и блокировать их файлы. Хоть сфера информационной безопасности (ИБ) и развивается очень быстро, но и злоумышленники постоянно придумывают новые схемы обмана, поэтому даже очень хорошо защищенные компании могут быть заражены ВПО. К таким ситуациям нужно быть заранее готовым, своевременно создавать бэкап системы, а также знать, как вести себя при инциденте ИБ, ведь чем раньше будет обнаружен инцидент, тем выше шанс предотвратить критические последствия.

Актуальность

Злоумышленники активно используют вирусы-шифровальщики для заражения информационных систем. Актуальность темы подтверждается статистикой, которую проводят ведущие компании в сфере ИБ.

Например, компания «Солар» за 2024 год проанализировала, что доля атак с финансовой мотивацией (вымогательство с помощью вирусов-шифровальщиков) составила 14% от общих целей атакующих (рис. 1).

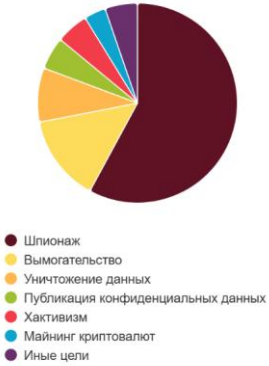


Рис. 1. Статистика о целях атакующих за 2024 год

Также в 2024 году участились случаи инцидентов, когда злоумышленники использовали вирусы-шифровальщики не для вымогательства, а для уничтожения данных. Доля таких целей атакующих составила 8,8%. Большинство атак такого рода на Российский сектор было реализовано группами злоумышленников под названием Shedding Zmiy и Lifting Zmiy, на них пришлось 34,1% и 14,6% всех атак соответственно (рис. 2) [1].

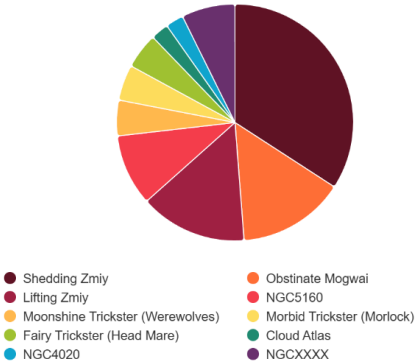


Рис. 2. Активные группы злоумышленников

У таких злоумышленников цель заключается в шпионаже с последующим уничтожением инфраструктуры жертвы. Часто в качестве инструмента злоумышленники использовали вирусы-шифровальщики, которые безвозвратно удаляют данные жертвы. При этом группировки всё активней целятся в ресурсы виртуализации, которые сегодня используют многие организации.

Компания «Positive technologies» в своей статистике за 4 квартал 2024 года пишет, что при атаке против организаций злоумышленники использовали вирусы-шифровальщики в 42% случаев (рис. 3) [2].

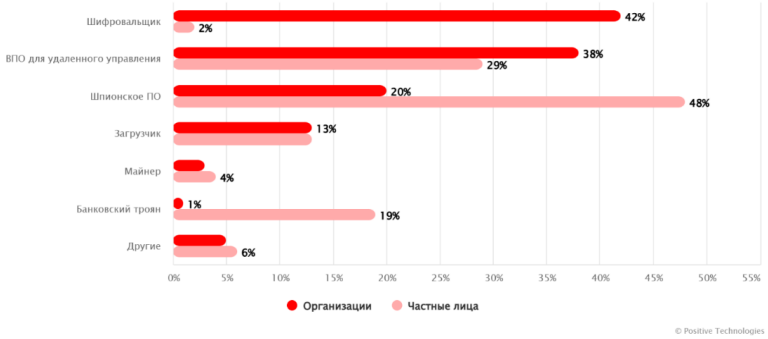


Рис. 3. Доля успешных атак

Также «Positive technologies» упоминает о развитие программ-вымогателей, преступники начинают использовать гибридные инструменты, которые одновременно шифруют и крадут данные. Это делается в случае, если компания не выплатит выкуп за данные, то злоумышленники просто продадут данные, что может нести в себе большие потери компании (денежные и доверие клиентов). Так, в августе 2024 года команда Outpost24 обнаружила последнюю версию инструмента Crystal Rans0m, имеющую такие возможности [3].

В статистике о последствиях атак приводятся данные об утечках конфиденциальной информации (55%) и финансовых потерях (48%) для частных лиц (рис. 4).

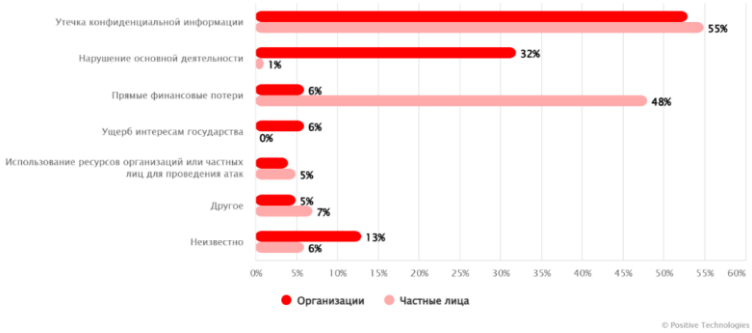


Рис. 4. Последствия атак

Сценарий реагирования на компьютерный инцидент

Одна из самых главных задач ИБ – это защита какой-либо организации от инцидентов ИБ, таких как шифрование файлов ransomware, утечка данных, недоступность веб-сервера в результате DDoS (denial-of-service attack «отказ в обслуживании») или другой кибератаки, эксплуатация уязвимости, хищение носителя с конфиденциальной информацией – лишь несколько очевидных примеров инцидентов ИБ [4].

Понятие инцидента ИБ присутствует в довольно большом количестве нормативно-правовых актов и стандартов, касающихся вопросов обеспечения ИБ. Например, термин раскрывается в таких документах, как ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения» - «Инцидент ИБ – это непредвиденное или нежелательное событие (группа событий) ИБ, которое привело (могут привести) к нарушению функционирования информационного ресурса или возникновению угроз безопасности информации или нарушению требований по защите информации» или ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» – «Инцидент ИБ: Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или ИБ». Хоть в разных документах понятие ИБ трактуется с небольшими отличиями, но главное заключается в том, что под инцидентом ИБ подразумеваются такие события, которые могут привести к нарушению ИБ. А событие ИБ в свою очередь – это зафиксированное состояние информационной (автоматизированной) системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или информационно-телекоммуникационной сети, указывающее на возможное нарушение безопасности информации, сбой средств ЗИ, или ситуацию, которая может быть значимой для безопасности информации, согласно ГОСТ Р 59709-2022.

Также нужно уметь классифицировать инциденты при работе с инцидентами ИБ. Их принято разделять по:

- типам (или видам);
- степени критичности (или степени возможно ущерба) для организации.

При классификации по типам или видам чаще всего используются категории, описанные в нормативных документах и стандартах, или определенные самими организациями.

Для примера рассмотрим стандарт ISO/IEC 27035-1. Он определяет принципы управления инцидентами ИБ, а также содержит примеры типов инцидентов ИБ и типизацию, предлагаемую Национальным координационным центром по компьютерным инцидентам (НКЦКИ) (табл. 1).

Таблица 2

Типы инцидентов

Тип инцидента по ISO/IEC 27035-1	Тип инцидента по НКЦКИ
Отказ в обслуживании (Denial of Service, DoS)	Нарушение или замедление работы контролируемого информационного ресурса
Неавторизованный доступ	Несанкционированный доступ в систему
Заражение вредоносным кодом	Заражение вредоносным программным обеспечением
	Распространение вредоносного программного обеспечения
Нарушение политик ИБ	Нарушение безопасности информации
	Мошенничество с использованием информационных коммуникационных технологий (ИКТ)
	Распространение информации с неприемлемым содержимым
Сбор информации	Сбор сведений с использование ИКТ

Степень критичности инцидентов ИБ обычно определяет сама организация для каждого конкретного случая.

Реагирование на инциденты происходят в несколько этапов [5]:

Локализация инцидента

На этом этапе осуществляется поиск затронутых ресурсов и принимаются меры по ограничению дальнейшего распространения инцидента. Также информируются пользователи, которые работают непосредственно с этими ресурсами, о дальнейших работах сотрудников информационной безопасности.

Выявление и анализ последствий

После того как определили зараженные ресурсы определяют на сколько сильно это затронуло систему и принимают первые шаги, которые могут остановить распространение ВПО в системе.

Ликвидация выявленных последствий

Завершающим шагом является устранение негативных последствий и восстановления затронутых ресурсов. Также всю информацию о затронутых ресурсах и приятых мер фиксируют способом, который каждая компания определяет сама.

Анализ инцидентов ИБ

На завершающем этапе происходит сбор все возможных данных, таких как:

- дампы трафика;
- образцы вредоносного кода;
- снэпшоты машин и др.

Все полученные данные собирают и анализируют специалисты ИБ для установления причин возникновения инцидента ИБ. Также в конце должны быть составлены рекомендации по доработке систем защиты, чтобы в дальнейшем такого не повторялось и повышения эффективности реагирования.

Все инциденты отличаются друг от друга, так в разных случаях злоумышленники преследуют разные цели, будь то кража данных, нарушение работы системы или шпионаж. Отличие ransomware-инцидентов от других заключается в том, что в первую очередь киберпреступники преследуют финансовую выгоду, путем шантажа они вымогают из жертв деньги, также отличительной чертой является, что выполнение ВПО происходит почти сразу, как попадает в систему, в отличие от других атак, которые могут длиться неделями, пока злоумышленники остаются незамеченными в системе [6, 7].

На основании этого были выделены и составлены основные этапы на реагирование инцидента ИБ в рамках данной работы:

1. Отключение зараженной системы от сети, если она к ней подключена.
2. Проверка вредоносной программы антивирусами.
3. Проверка исполняемого файла при помощи специализированного сайта.
4. Анализ трафика при помощи утилиты Wireshark.
5. Просмотр событий Windows.
6. Анализ границ заражения.
7. Восстановление системы при помощи бэкапа.

Практическая работа

Для анализа вируса-шифровальщика была установлена виртуальная машина на базе операционной системы Windows 10 версии 22H2. Также был разработан сценарий попадания вируса в систему и сценарий реагирования на инцидент ИБ специалистов из данной области. Возможный сценарий атаки злоумышленника на компанию: сотруднику приходит на рабочую почту срочное письмо от начальника, в котором содержится неизвестный ему файл и информация о том, что его срочно нужно скачать и открыть (рис. 5).

Рис. 5. Фишинговое письмо

Сотрудник, естественно, не проверяет достоверность данной информации, так как была большая срочность и адрес отправителя совпадал с адресом его начальника. После запуска приложения оно пропало из папки, от куда запустил его сотрудник, а через несколько минут сотрудник обнаружил, что часть файлов на рабочем столе была зашифрована, и их невозможно открыть, также появился файл с названием «_readme.txt», в котором была информация о выкупе (рис. 6). После этого инцидента сотрудник обратился в отдел ИБ, чтобы они осмотрели его компьютер.

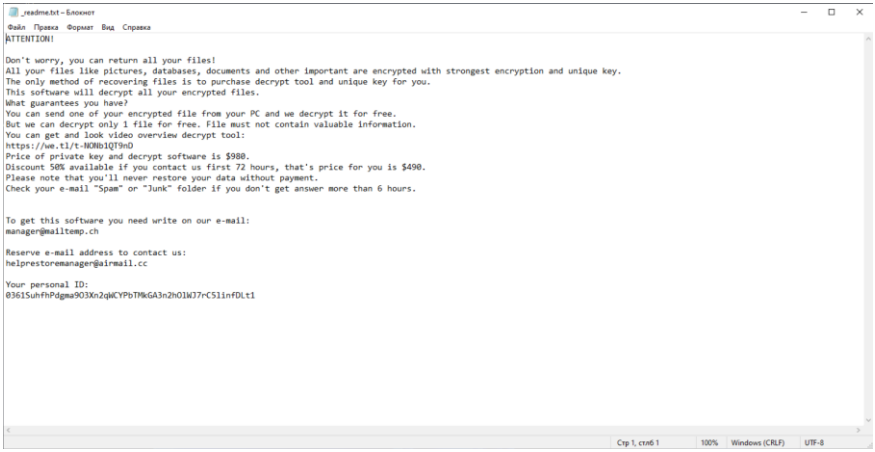


Рис. 6. Информация о выкупе из файла _readme.txt

Далее описание сценария реагирования на инцидент отделом ИБ. При реагировании на ransomware-инцидент первым делом специалист ИБ отключает компьютер от сети, чтобы вирус не распространился на другие устройства.

На втором этапе необходимо проверить запущенные процессы с помощью утилиты «System Informer» можно обнаружить, что запущен нелегитимный процесс под названием «challenge.exe» (рис. 7).

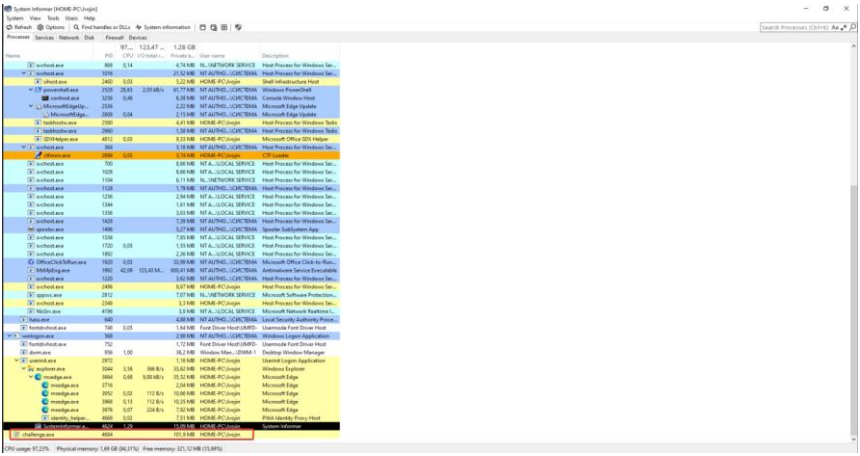


Рис. 7. Нелегитимный процесс challenge.exe

Специалист ИБ открывает свойства процесса, где видит, что данный процесс сильно нагружает жесткий диск, что свидетельствует о его взаимодействии с файлами, а также виден путь, где теперь находится этот файл (рис. 8).

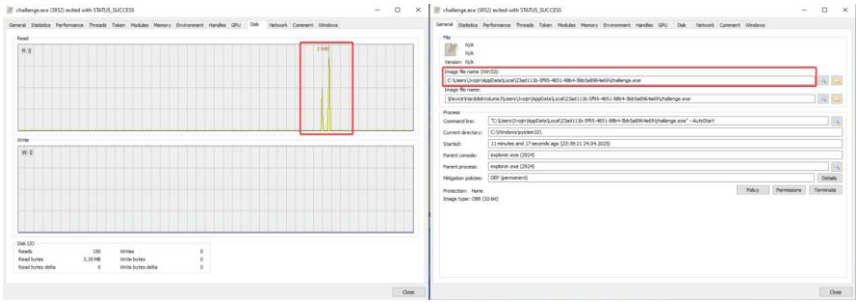


Рис. 8. Информация о процессе

Далее специалист проверяет данную файл с помощью антивирусных программ. Просканировав его с помощью антивируса «Zoner», можно получить информацию о том, что этот процесс не является угрозой для системы (рис. 9).

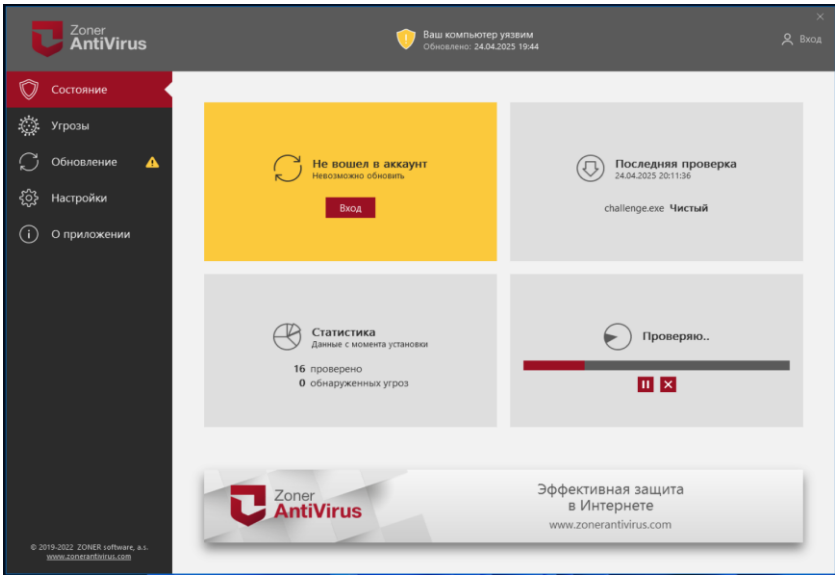


Рис. 9. Проверка с помощью антивируса Zoner

После этого проверив программу с помощью другого антивируса под названием «Dr.Web», можно получить информацию о том, что это троян (рис. 10).

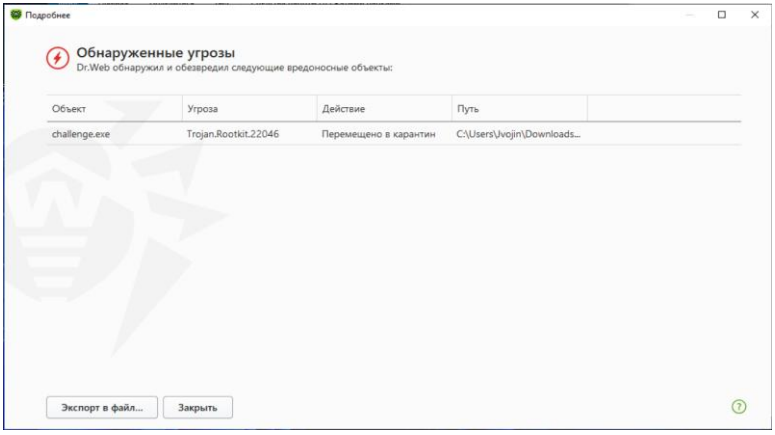


Рис. 10. Проверка с помощью антивируса Dr.Web

Далее можно получить хэш сумму этого файла с помощью встроенной утилиты в Windows под названием «certutil», для этого в командной строке необходимо прописать команду «certutil -hashfile "C:\Users\Jvojin\Downloads\87-Ransomed\challenge.exe"MD5» (рис. 11).

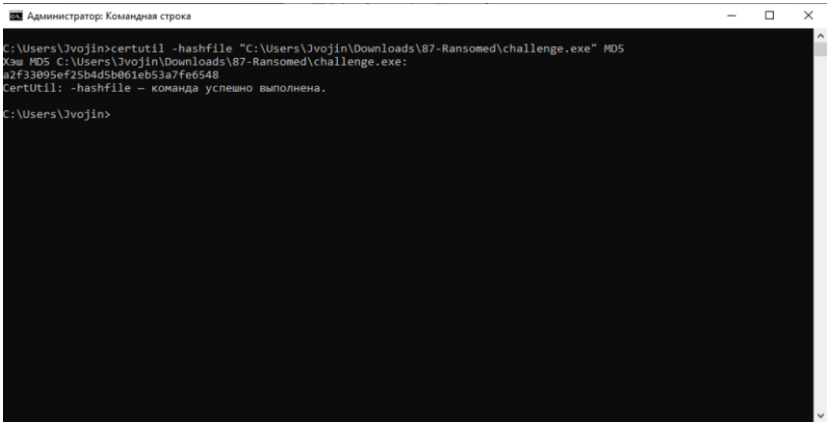


Рис. 11. Хэш сумма

Проверив полученную строку на сайте «VirusTotal», можно обнаружить, что данный файл относится к числу вирусов ransomware (рис. 12).

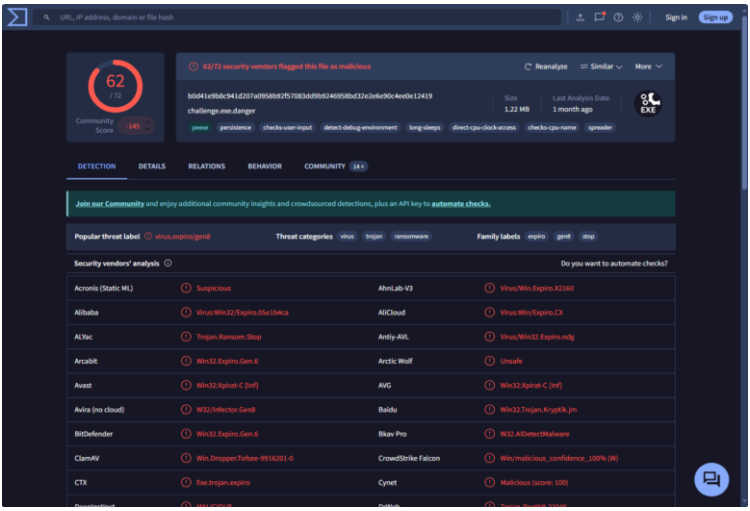


Рис. 12. Проверка файла на сайте VirusTotal

Далее с помощью программы «Wireshark» можно проверить как данное ВПО ведет себя в сети. Проанализировав дамп трафика, можно увидеть, что при запуске данная программа обращается к сторонним сайтам «api.2ip.ua», «kotob.top» и «tzgl.org», где при запросе к доменам в ответ приходят ip-адреса (рис. 13).

Рис. 13. Дамп трафика

Обратившись к журналу событий Windows, можно увидеть, что программа-шифровальщик запускает дочерний процесс «C:\Windows\SysWOW64\icacls.exe» (рис. 14). icacls.exe – это встроенная утилита Windows, которая используется для управления списками контроля доступа (ACL) файлов и папок. Она позволяет просматривать, изменять или устанавливать права доступа для пользователей и групп на уровне файловой системы.

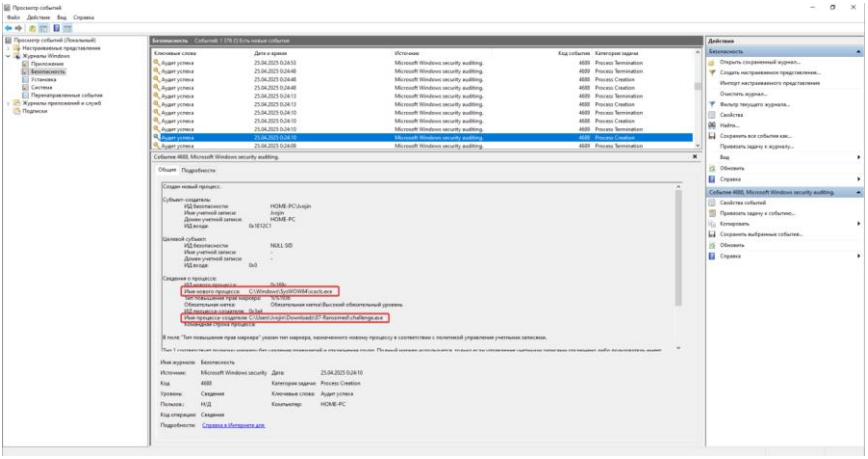


Рис. 14. Журнал событий

Далее необходимо посмотреть границы заражения. Например, данной ситуации можно увидеть, как вирус-шифровальщик не затрагивает системные файлы, заражение которых могло бы нарушить работу всей системы (рис. 15).

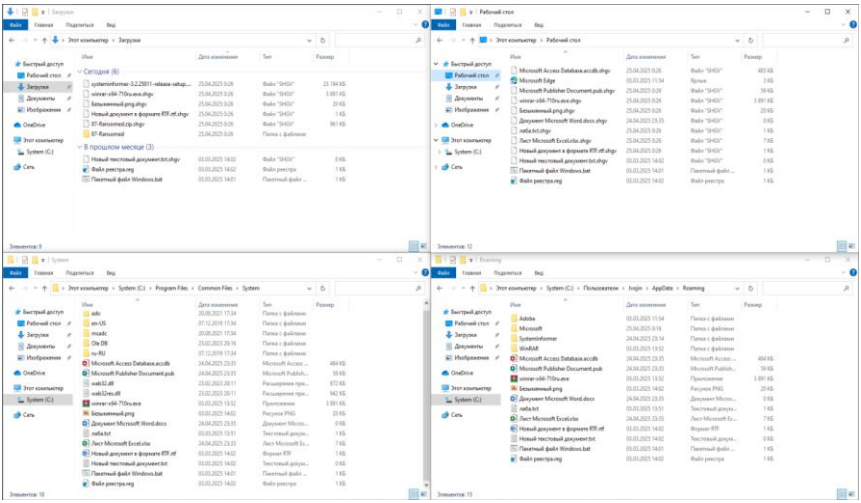


Рис. 15. Границы заражения

Заключительным этапом реагирования на инцидент является восстановления системы в состояние до заражения. Для этого необходим бэкап системы, поэтому после проведения всех работ нужно вернуть систему с помощью последнего бэкапа.

Вывод по практической части: С помощью фишингово письма можно заразить компьютер вирусом-шифровальщиком под названием «Challenge.exe». После запуска исполняемого файла шифровальщик скрывался в системе и запускал дочерний процесс для работы с файловой системой, а также обращался к сторонним ресурсам в интернете. Шифровальщик не трогал системные папки. Утечки данных не было выявлено, целью злоумышленников являлось требование о выкупе зашифрованных файлов. Анализ показал, что не все антивирусы смогли обнаружить данное ВПО. Уязвимостью стал человеческий фактор.

Заключение

В мире существует большое множество различных ВПО начиная от рекламных программ и заканчивая вирусами. В их число входят и ransomware - программы-шифровальщики. Главная задача таких программ – это проникнуть в компьютер пользователя и зашифровать данные, за которые в последствии можно было просить выкуп. Изначально такие программы-шифровальщики предназначались для обычных пользователей и требовали небольшой выкуп для расшифровки данных, но с течением времени злоумышленники начали заражать целые компании и выкуп, соответственно, они просили уже в разы больше.

Если разобрать слово Malware и перевести его с английского языка, то буквальный перевод, malicious – злонамеренный и software – программное обеспечение. То есть malware – это программа, которая была придумана и разработана со злым умыслом и несанкционированно проникает в систему специально для нанесения ущерба как организациям, так и отдельным людям.

По результатам данной работы можно сделать вывод, что злоумышленники активно используют вирусы-шифровальщики для кражи данных компаний и шантажа. Очень важно защищать свои данные, для этого необходимо не попадаться на уловки злоумышленников, своевременно устанавливать обновления для приложений и делать бэкапы своих данных, которые помогут быстро восстановить утерянные данные, в случае если злоумышленник все-таки сможет навредить компании. В ходе работы был проведен анализ актуальности проблемы, были выявлены этапы реагирования на инциденты, а также разработан сценарий атаки, проведен анализ поведения вируса-шифровальщика в системе и разработана пошаговая инструкция с примерами для анализа компьютерного инцидента с помощью программ по анализу ВПО и трафика сети.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Хроники DFIR: как атаковали APT-группировки в 2024 году. – URL: rt-solar.ru/analytics/reports/5354/ (дата обращения: 20.03.2025).
2. Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года. – URL: www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/#id19 (дата обращения: 01.04.2025).
3. PT NGFW URL: ptsecurity.com/ru-ru/products/ngfw/#advantages (дата обращения: 02.04.2025).
4. Интерактивная карта атак шифровальщиков. – URL: cybermap.kaspersky.com/special/ransomware/ru/stats#country=213&type=RMW&period=m (дата обращения: 10.03.2025).
5. Инциденты информационной безопасности: выявление, расследование и реагирование. – URL: selectel.ru/blog/security-incidents/ (дата обращения: 10.03.2025).
6. Кто такой злоумышленник? – URL: keepersecurity.com/blog/ru/2023/08/07/what-is-a-threat-actor/ (дата обращения: 15.03.2025).
7. Как защититься от шифровальщиков-вымогателей: 5 советов. – URL: kaspersky.ru/blog/ransomware-five-tips/31352/ (дата обращения: 01.04.2025).

УДК 004.056.2

Г.Д. Малютин, Е.А. Маро

Южный федеральный университет, Россия, г. Таганрог

ИССЛЕДОВАНИЕ УЯЗВИМОСТИ СКАНЕРОВ ОТПЕЧАТКОВ ПАЛЬЦЕВ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

В данной работе исследуется процесс формирования универсального отпечатка пальца, который может использоваться для прохождения биометрической аутентификации на сканере без предварительной регистрации. Основной задачей исследования является изучение возможностей создания универсального отпечатка, обладающего характеристиками, схожими с реальными биометрическими данными различных пользователей. В ходе анализа были рассмотрены существующие методы синтеза отпечатков пальцев. Универсальный отпечаток создается с использованием нейросетевых алгоритмов, обученных на массиве отпечатков пальцев, доступных из открытых источников. В ходе экспериментов были выполнены работы по созданию копии отпечатка пальца на основе физического пальца с применением различных методов реконструкции. Результаты показали, что предложенный метод обладает высокой степенью универсальности, позволяя успешно имитировать зарегистрированные биометрические данные. Это свидетельствует о потенциальных угрозах для безопасности биометрических систем и подчеркивает необходимость внедрения дополнительных механизмов защиты. В исследовании акцентируется внимание на уязвимостях существующих биометрических технологий и важности разработки новых методов их защиты. Полученные результаты могут быть полезны как для дальнейшего усовершенствования систем аутентификации, так и для оценки рисков, связанных с возможностью генерации универсальных биометрических шаблонов.

Ключевые слова: *универсальный отпечаток пальца, биометрическая аутентификация, нейронные сети, синтетические биометрические данные, безопасность биометрии, уязвимости биометрии, отпечаток пальца.*

This research investigates the process of creating a universal fingerprint that can be utilized for biometric authentication on scanners without prior registration. The primary objective of the research is to explore the feasibility of generating a universal fingerprint that possesses characteristics similar to the actual biometric data of various users. The analysis examines existing methods for synthesizing fingerprints. The universal fingerprint is generated using neural network algorithms trained on a dataset of fingerprints available from open sources. During the experiments, attempts were made to create a replica of a fingerprint based on a physical finger using various reconstruction methods. The results demonstrated that the proposed method exhibits a high degree of universality, successfully mimicking registered biometric data. This finding indicates potential security threats to biometric systems and underscores the necessity for implementing additional protective mechanisms. The research emphasizes the vulnerabilities inherent in current biometric

technologies and the importance of developing new methods for their protection. The findings may be beneficial for further enhancing authentication systems as well as for assessing risks associated with the potential generation of universal biometric templates.

Keywords: *universal fingerprint, biometric authentication, neural networks, synthetic biometric data, biometric security, vulnerabilities in biometrics, fingerprint.*

Введение

В современном мире постоянно растет потребность в идентификации личности, особенно для личной аутентификации. Например, для блокировки смартфона, авторизации банковской операции или снятия денег в банкомате. Биометрические системы распознавания обеспечивают удобный способ выполнения необходимого шага аутентификации без необходимости носить с собой ключи, смарт-карты или запоминать сложные пароли. Таким образом, биометрические системы потенциально могут обеспечить дополнительную безопасность. Согласно ГОСТ Р 54412–2019 – биометрическое распознавание представляет собой автоматическое распознавание индивидов, основанное на их биологических и поведенческих характеристиках [1]. К наиболее часто используемым биологическим признакам относятся: отпечатки пальцев, лицо, радужная оболочка глаза и голос. Для каждого из этих признаков необходимо специальное устройство для захвата образцов конкретного признака, обычно обозначаемое как биометрическое устройство захвата или биометрический сканер. Большинство современных сканеров отпечатков пальцев основаны на оптической или емкостной технологии, и могут иметь площадь около 3 $см^2$, что позволяет интегрировать технологию распознавания отпечатков пальцев в огромное количество различных устройств, от дверных замков до смартфонов. Получение цифровой копии отпечатка пальца – это быстрый и надежный процесс, который демонстрирует высокую востребованность среди потребителей. Технологии распознавания отпечатков пальцев являются преобладающим биометрическим признаком, за счет простоты использования.

При всех преимуществах технология распознавания отпечатков пальцев далека от совершенства. В отличие от паролей, биометрический признак нельзя изменить или аннулировать. Из чего следует, что при компрометации отпечатка пальца, пользователи оказываются в опасной ситуации.

1. Алгоритм работы сканера отпечатка пальца

Биометрическая система распознавания отпечатка пальца состоит из следующих стадий:

- получение образца;
- предварительная обработка;
- извлечение признаков;
- сравнение;
- окончательное решение.

2. Регистрация и верификация в биометрической системе распознавания отпечатка пальца

Функционирование биометрической системы распознавания отпечатка пальца организовано по принципу двухуровневой архитектуры, которая представлена на 0:

- На первом уровне происходит регистрация, где один или несколько образцов каждого субъекта снимаются, предварительно обрабатываются, а извлеченные характеристики сохраняются в базе данных в виде биометрических шаблонов.
- На втором уровне происходит верификация, где снимается новый биометрический образец. Проводится предварительная обработка и извлеченные признаки сравниваются с шаблонами соответствующего субъекта или со всеми шаблонами в базе данных для принятия окончательного решения.

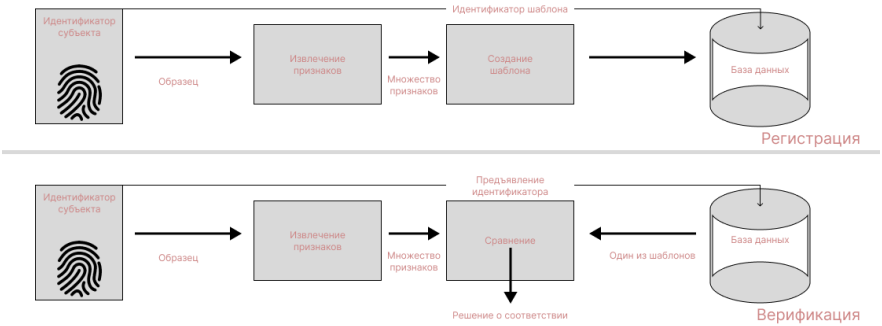


Рис. 1. Алгоритмы регистрации и верификации в биометрической системе

3. Особенности отпечатка пальца

В системах распознавания отпечатков пальцев, как правило, снимается от трех до пяти образцов, чтобы получить снимок пальца, который не зависит от вариаций расположения, деформации и поворота кончика пальца. Кожа на внутренней стороне пальца покрыта папиллярными узорами.

Папиллярный узор – это сложный рельефный рисунок, образованный чередующимися валиками (высотой 0,1–0,4 мм, шириной 0,2-0,7 мм) и долинами – углублениями (шириной 0,1–0,3 мм). Считается, что эти гребни уникальны для каждого человека и относительно стабильны в течение долгого времени [2].

Большинство систем распознавания отпечатков опираются на специфические характеристики рисунка, которые можно разделить на три различных уровня, как представлено на 0:

- детальный уровень: определяются макродетали, такие как рисунок или тип валиков и долин. Валики демонстрируют несколько областей, где они напоминают отчетливую форму, обычно классифицируемую на дельты, петли и витки;
- точечный уровень: определяются макродетали, такие как поток гребня и тип узора, характеристики Гальтона, или миниатюрные точки, такие как раздвоения и окончания;
- глубокий уровень: мелкие детали, например, зарождающиеся валики и потовые поры, могут быть обнаружены, если устройство захвата имеет достаточно высокое разрешение не менее 1000 dpi. Поры можно дополнительно классифицировать на открытые или закрытые, в зависимости от их расположения на гребнях [3].

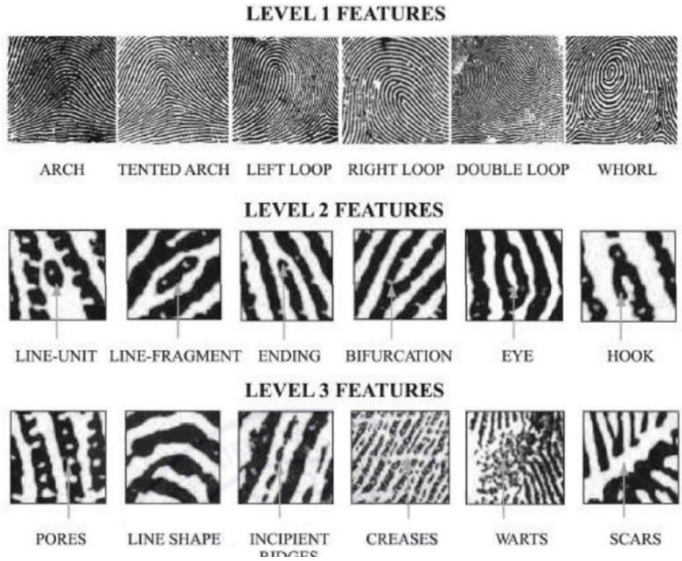


Рис. 2. Особенности отпечатков пальцев на трех уровнях [4]

В настоящее время признаки третьего уровня гораздо труднее подделать, чем признаки первого и второго уровня. Типичный отпечаток содержит около ста точек миниатюр. Область, захватываемая обычными датчиками отпечатков пальцев, содержит около 30-50 dpi. Для положительной идентификации, которая может быть признана судах, в отпечатке должно

быть однозначно идентифицировано не менее 12 dpi, в то время как большинство коммерческих систем распознавания отпечатков способны обеспечить успешное положительное совпадение минимум с 8 dpi.

4. Технологии распознавания отпечатков пальцев

Перед извлечением признаков отпечатка пальца, необходимых для биометрического распознавания, необходимо получить образец отпечатка пальца. Такой образец может быть получен с помощью различных устройств захвата, основанных на оптических свойствах поверхности кожи, электрофизических свойствах кожи, тепловых свойствах валиков и воздушных зазоров в долинах или ультразвуковых свойствах кожи [5]. Первые коммерческие (Commercial Off-The-Shelf, COTS) устройства для снятия отпечатков пальцев появились на рынке в 1980-х годах и были основаны на технологии оптического зондирования.

В настоящее время наблюдается сдвиг в сторону емкостной технологии, с недавних пор и ультразвуковых устройств, особенно в последних моделях смартфонов, поскольку эти датчики достаточно малы, чтобы быть встроенными практически в любое устройство, в то время как оптические устройства по-прежнему преобладают в приложениях повышенной безопасности. Большинство устройств для захвата отпечатков пальцев имеют разрешение не менее 500 dpi.

5. Принцип работы оптического сканера

Палец помещается на стеклянную поверхность, которая является прозрачной призмой. Оптическое устройство для снятия отпечатков содержит источник света для освещения поверхности сегмента, зачатую им является светодиод, и камеру для получения изображения.

В большинстве оптических устройств используется принцип полного внутреннего отражения. Палец помещается непосредственно на стеклянную пластину так, чтобы валики непосредственно касались стеклянной пластины.

Поверхность освещается внутренним источником света через одну сторону призмы. Свет, попадающий на призму, переизлучается в долинах и поглощается в валиках, создавая контраст между ними. Отраженный свет проецируется на камеру через систему линз и фиксируется камерой.

Оптические сканеры больше размерами по сравнению с другими видами, так же свет может одинаково отражаться как от кожи, так и от другого материала. На качество получения снимка зачастую оказывает влияние влажность и загрязненность. В данный момент большая часть сканеров отпечатка пальца встраивается под стеклянную часть экрана телефона. Реализовать такую технологию можно только на AMOLED экранах, в которых источником света служат пиксели экрана.

5.1. Принцип работы емкостного сканера

Емкостные сканеры используют датчики КМОП. Устройства создают электрическое поле между поверхностью датчика и поверхностью пальца. Из-за слоев кожи возникают изменения в электрическом поле валиков и долин, которые затем измеряются и преобразуются в цифровое представление. Датчики имеют металлическую или токопроводящею поверхность, до которой необходимо коснуться, чтобы датчик создал электрическое поле. Емкостные сканеры более уязвимы при использовании поддельных отпечатков пальцев на основе желатина.

5.2. Принцип работы теплового сканера

Тепловые сканеры основаны на комбинации кремния и пироэлектрического материала, который измеряет разницу в температуре и преобразует ее в цифровой сигнал. Когда кончик пальца прикладывается к датчику, валики касаются поверхности датчика, изменяя температуру, в то время как долины изолированы небольшим воздушным зазором между кожей и поверхностью датчика, за счет этого температура остается постоянной там, где расположены долины. Это создает необходимую разницу в температурах между валиками и долинами, которую можно измерить. Недостатком является то, что через некоторое время изображение исчезает, так как датчик достигает теплового равновесия, то есть по всей поверхности датчика сохраняется постоянная температура. Тепловые устройства считаются менее удобными для пользователя из-за необходимости совершать движение пролистывания. Тепловые датчики используются редко.

5.3. Принцип работы ультразвукового сканера

Ультразвуковые сканеры используют разницу в акустическом сопротивлении между кожей валиков и воздухом в долинах, валики непосредственно касаются поверхности датчика. Ультразвуковой сканер является акустическим излучателем, который передает акустический сигнал на поверхность кончика пальца и улавливает принятый сигнал. Диапазон частот этих устройств составляет от 20 кГц до нескольких ГГц. Высокие частоты соответствуют более высокому разрешению получаемых изображений. Ультразвуковые устройства были более дорогими, чем другие устройства для снятия отпечатков пальцев, но с появлением новых технологий производства и экранных сенсорных решений для смартфонов эти устройства стали более популярными. Главным преимуществом является безопасность. Это связано с тем, что датчик сканирует трехмерную модель пальца, так же ультразвуковая волна проходит сквозь палец.

6. Уязвимости сканеров отпечатков пальцев

Благодаря высокой точности и низкой стоимости сканеры отпечатков пальцев являются наиболее часто устанавливаемыми биометрическими устройствами в смартфонах в настоящее время для облегчения аутентификации или авторизации в мобильных приложениях. Операционные системы мобильных устройств, являются связующим звеном между аппаратным и программным обеспечением, которое должно обеспечивать приложениям, работающим на смартфонах, удобный доступ к сканеру отпечатков пальцев. Android, как наиболее распространенная операционная система для смартфонов, предоставляет набор функций Application programming interface (API), предназначенных для использования приложениями сканеров отпечатков пальцев. Благодаря поддерживаемому API для сканеров отпечатков пальцев разработчикам не нужно беспокоиться о различиях в аппаратном обеспечении, даже если сканеры отпечатков пальцев от разных производителей или имеют разное расположение в смартфоне.

Несмотря на удобство, безопасность аутентификации по отпечаткам пальцев также очень важна. Помимо обеспечения безопасности самого сканера, во всех смартфонах используется подход по изолированию критически важных для безопасности устройства операций в выделенный сегмент – Trusted execution environment (TEE).

6.1. DeepMasterPrints

В 2018 году исследователи из Нью-Йоркского университета и Университета Мичигана представили технологию DeepMasterPrints [6]. Инструмент, построенный на базе Generative adversarial network (GAN), способен создавать искусственные отпечатки пальцев, которые обладают высокой вероятностью совпадения с реальными отпечатками в биометрических системах. Разработка открыла возможность для реализации атак по словарю на системы защиты. Алгоритм работы DeepMasterPrints представлен на 0.

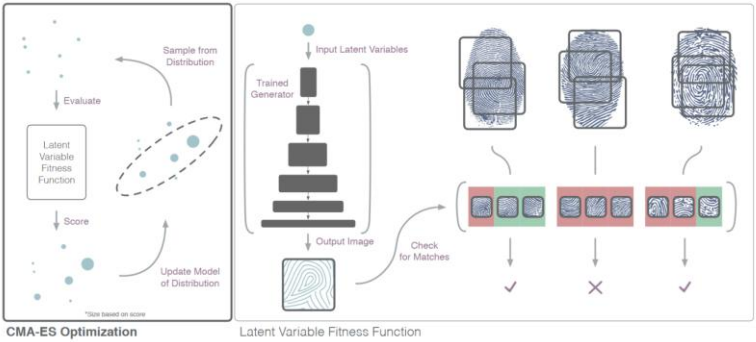
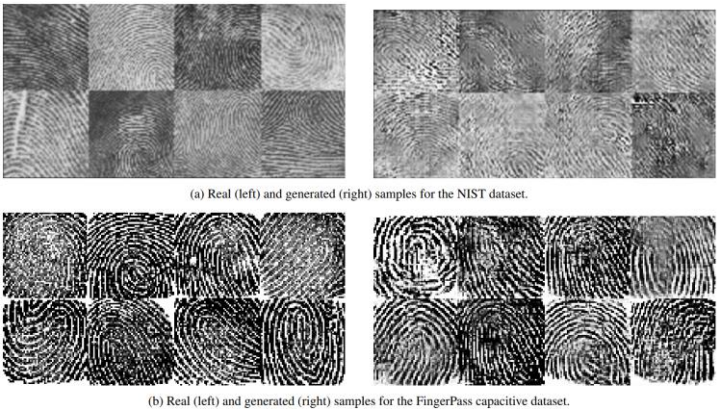


Рис. 3. Алгоритм работы DeepMasterPrints

Большинство современных сканеров, встроенных в смартфоны и ноутбуки, имеют ограниченную площадь считывания и распознают только часть отпечатка. Поскольку некоторые участки отпечатков разных людей имеют сходные черты, исследователи пришли к выводу, что можно создать отпечаток, объединяющий общие элементы различных образцов. Это повышает вероятность того, что созданный отпечаток совпадет с несколькими реальными отпечатками в базе данных.

DeepMasterPrints стала логическим продолжением проекта MasterPrints, представленного ранее в работе [7]. В отличие от предшественника, который лишь модифицировал существующие отпечатки, новая технология способна генерировать уникальные образы на основе базы из 6000 реальных отпечатков пальца.

Эксперименты проводились на двух наборах данных, которые представлены на 0: классическом наборе данных NIST с отпечатками, снятыми при помощи чернил, и наборе данных, полученными с использованием современных цифровых сенсоров. Технология показала лучшие результаты при работе с цифровыми отпечатками.



(a) Real (left) and generated (right) samples for the NIST dataset.

(b) Real (left) and generated (right) samples for the FingerPass capacitive dataset.

Рис. 4. Сравнение цифровых отпечатков пальцев с отпечатками, снятыми при помощи чернил

В зависимости от уровня безопасности системы результаты оказались следующими:

- низкий уровень защиты (1% ложных совпадений) – успешность обхода достигла 77%;
- средний уровень защиты (0,1% ложных совпадений) – вероятность успешного совпадения составила 23%;
- высокий уровень защиты (0,01% ложных совпадений) – обход системы удался в 1,2% случаев.

Несмотря на впечатляющие результаты при низком уровне защиты, на практике большинство современных биометрических сенсоров имеют более строгие параметры безопасности. Успешность атак на среднем уровне показывает, что технология DeepMasterPrints может представлять потенциальную угрозу для систем аутентификации, особенно в случае использования цифровых сенсоров.

6.2. Атака на сканер

Исследователи обнаружили несколько различных уязвимостей биометрических систем распознавания и систем отпечатков пальцев. Уязвимости можно разделить на восемь различных атак [8]:

- атака представления;
- копирование биометрического сигнала;
- модификация признаков;
- замена признаков;
- переопределение устройства сопоставления;
- замена шаблонов;
- модификация данных через канал;
- изменение решения.

За исключением первой атаки (атаки представления) остальные семь атак относятся к изменению цифровых сигналов или информации, хранящейся в цифровом виде. Первая атака относится к физической или атаке на уровне сенсора (устройство биометрического захвата) путем представления поддельного представления, которое является воспроизведением подлинного биометрического признака. Остальные семь атак можно предотвратить, используя шифрование и аутентификацию устройств на каналах передачи данных, а также защиту шаблонов для базы данных. Однако атака представления является прямой физической атакой на сенсор, и одной из наиболее важных возможностей третьей и четвертой атаки, поскольку объект атаки доступен и атаку легко реализовать без дополнительных знаний о внутреннем устройстве биометрической системы распознавания. Системы распознавания отпечатков считаются очень надежными и часто используются для защиты конфиденциальной информации. Разработано и описано несколько различных методов создания поддельных отпечатков пальцев, в большинстве из которых используются такие материалы, как: желатин, воск, древесный клей, клей ПВА, пластик, глина, паста для снятия слепков зубов и силикон. В связи с высоким риском, возникающим в результате успешных презентационных атак (presentation attack), исследователи и промышленные предприятия внедрили способы обнаружения и предотвращения презентационных атак для обеспечения безопасности своих биометрических систем, которые могут быть реализованы либо в аппаратном, либо в программном обеспечении, и называются системами обнаружения презентационных атак (Presentation Attack Detection, PAD).

6.3. Создание копии отпечатка пальца

Процесс создания копии отпечатка пальца можно разделить на два основных класса, в зависимости от имеющихся исходных данных у исследователя.

Первый класс прямых атак – лабораторная проверка на основе физического использования самого пальца зарегистрированного пользователя. В данном случае получение копии отпечатка можно реализовать следующими способами:

- палец помещается в быстроотвердевающее вещество, например в воск. После отвердевания материала получится форма пальца. Далее форма заполняется веществом на который реагирует сканер, например желатин;
- пальцем нажимает на мягкое вещество, например пластилин. После это остается объемный след отпечатка. Далее форма заполняется веществом, на который реагирует сканер, например желатин;
- используется 3D изображение пальца, которое можно получить с помощью смартфона с LIDAR сканером. После получения модели пальца она загружается в программное обеспечение для 3D моделирования, с помощью которой создается 3D копия пальца. Остается только распечатать образец на 3D принтере.

Второй класс прямых атак – атаки без физического вовлечения зарегистрированного пользователя в создание копии отпечатка. С помощью различны способов снятия следов отпечатка пальца с предметов, фотографирования в высоком разрешении и так далее. Сначала с гладкой поверхности с помощью дактилоскопического порошка проявляется отпечаток, после чего высококачественной камерой фотографируется проявленный след или с использованием дактилопленки снимается отпечаток пальца и помещается на белую поверхность. Проявленный отпечаток сканируется в высоком разрешении. На основе изображения отпечатка пальца копию можно сделать двумя способами:

- след отпечатка пальца загружается в программное обеспечение для 3D моделирования, с помощью которой делается 3D копия отпечатка, и создается прототип пальца на 3D принтере;
- след отпечатка пальца загружается в графический редактор для повышения контраста. Далее понадобиться лазерный принтер и ацетатная бумага. При печати получается текстурное изображение следа. На последнем этапе на полученное изображение наносится вещество с помощью, которого можно аутентифицироваться на устройстве, например ПВА клей. После отвердевания состава будет получена копия отпечатка вероятно пригодная для проведения атаки на сканеры.

6.4. Исследование прямых атак на сканеры отпечатков пальца

В ходе проведения экспериментов использовался первый класс прямых атак, в результате проведения которых можно сделать следующий вывод – наиболее безопасным к прямым атакам является сканер в устройстве Samsung S10, что связанно с ультразвуковой технологией, формирующей 3D копию отпечатка пальца, за счет чего подделать отпечаток становится сложнее.

Результаты проведенных экспериментов представлены в табл. 1.

Таблица 1

Результаты презентационных атак для различных мобильных устройств

Устройство	Технология сканера	Используемый материал для копии	Количество попыток аутентификации	Количество успешных попыток аутентификации
Apple 7	Оптический	Желатин	10	6
		Клей ПВА с ПАП-2	10	9
Xiaomi redmi 4x	Емкостный	Желатин	10	6
		Клей ПВА с ПАП-2	10	8
Xiaomi mi 11 lite	Емкостный	Желатин	10	4
		Клей ПВА с ПАП-2	10	6
Samsung A51	Оптический	Клей ПВА с ПАП-2	10	9
Apple MacBook Pro	Емкостный	Клей ПВА с ПАП-2	10	8
Samsung S10	Ультразвуковой	Клей ПВА с ПАП-2	10	5

Заключение

Проведенное исследование позволило изучить возможность формирования универсального отпечатка пальца с применением нейросетевых алгоритмов, обученных на массиве биометрических данных из открытых источников. В ходе работы проведены эксперименты по физической реконструк-

ции отпечатка пальца, что позволило глубже оценить границы применимости данного метода.

Анализ характеристик показывает потенциальную возможность компрометации биометрической аутентификации. Это свидетельствует о необходимости дальнейшего изучения механизмов защиты, направленных на предотвращение атак с использованием синтетических биометрических шаблонов. Учитывая возрастающую роль биометрических технологий в современных системах безопасности, актуальной задачей становится разработка методов детекции подобных угроз и совершенствование алгоритмов, обеспечивающих надежную идентификацию пользователей.

Результаты данного исследования могут быть полезны как в контексте практического применения биометрических систем, так и для дальнейших научных исследований в области кибербезопасности. Дальнейшие направления исследования могут быть сосредоточены на разработке новых методов криптографической защиты биометрических данных, анализе устойчивости различных систем аутентификации к атакам на основе универсальных отпечатков, а также на оценке этических и правовых аспектов, связанных с использованием синтетических биометрических данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Всероссийский научно-исследовательский институт сертификации и Русское общество содействия развитию биометрических технологий, систем и коммуникаций. Биометрия. – URL: https://docs.cntd.ru/document/1200169607 (дата обращения: 10.01.2025).
2. Основы дактилоскопии. – URL: https://studwood.net/657983/pravo/osnovy_daktiloskopii_chast (дата обращения: 10.01.2025).
3. *Jain A., Chen Y., Demirkus M.* Department of Computer Science and Engineering. – URL: http://biometrics.cse.msu.edu/Publications/Fingerprint/JainChenDemirkus_FpLevel3_ICPR2006.pdf (дата обращения: 10.01.2025).
4. *Abhishek K., Yogi A.* A Minutiae Count Based Method for Fake Fingerprint Detection. – URL: https://www.sciencedirect.com/science/article/pii/S1877050915021729 (дата обращения: 10.01.2025).
5. *Maltoni D., Maio D., Jain A. Prabhakar S.* Handbook of Fingerprint Recognition. – URL: https://download.e-bookshelf.de/download/0000/0079/95/L-G-0000007995-0002341237 (дата обращения: 10.01.2025).
6. *Bontrager P., Roy A., Togelius J.* DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution. – URL: https://arxiv.org/pdf/1705.07386 (дата обращения: 10.01.2025).
7. *Roy A., Memon N., Ross A.* MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems. – URL: https://ieeexplore.ieee.org/document/7893784 (дата обращения: 10.01.2025).
8. *Ratha N., Connell J., Bolle R.* Enhancing security and privacy in biometrics-based authentication systems. – URL: https://cedar.buffalo.edu/~govind/CSE717/papers/CancelableBiometrics.pdf (дата обращения: 10.01.2025).

УДК 004.056

М.В. Мартыненко, В.Д. Михайлова

Южный федеральный университет, Россия, г. Таганрог

СИСТЕМА ОБНАРУЖЕНИЯ АТАК НА УРОВНЕ УЗЛА УМНОГО ПРОИЗВОДСТВА

Статья посвящена системе обнаружения атак на уровне узла умного производства, ориентированной на выявление кибератак в режиме реального времени. Актуальность исследования обусловлена ростом атак на промышленные системы, использующие уязвимые протоколы, такие как ModBus TCP, и необходимостью защиты критической инфраструктуры от новых угроз, включая вредоносное программное обеспечение типа FrostyGoop. Предлагаемая система решает проблемы традиционных методов, основанных на сигнатурном анализе и требующих предварительного обучения модели, за счет комбинированного анализа сетевого трафика и физических параметров устройств (загрузка, температура центрального процессорного устройства и др.). Методология системы включает нормализацию данных с использованием распределений Пуассона (для дискретных параметров) и Гаусса (для непрерывных параметров), а также оценку аномалий через меру Кульбака-Лейблера, которая количественно определяет расхождения между временными рядами. Тестирование системы, проведенное на стенде с одноплатными компьютерами Raspberry Pi и микроконтроллерами STM32, имитирующими конвейерное производство, подтвердило эффективность системы. Атаки, такие как сканирование Nmap и перебор паролей, были обнаружены на ранних этапах за счет анализа аномальных всплесков сетевой активности. Результаты демонстрируют, что система способна минимизировать риски, обеспечивая адаптивное обнаружение атак на промышленные узлы без глубокого и длительного анализа статистических данных.

Ключевые слова: *система обнаружения атак, умное производство, ModBus TCP, обнаружение аномалий, кибербезопасность промышленных сетей*

The article is devoted to an attack detection system at the smart manufacturing node level, focused on detecting cyber attacks in real time. The relevance of the study is due to the growing attacks on industrial systems using vulnerable protocols such as ModBus TCP and the need to protect critical infrastructure from new threats, including malicious software such as FrostyGoop. The proposed system solves the problems of traditional methods based on signature analysis and requiring prior model training by combining network traffic analysis and physical device parameters (load, CPU temperature, etc.). The methodology of the system includes data normalization using Poisson (for discrete parameters) and Gaussian (for continuous parameters) distributions, as well as anomaly estimation using the Kullback-Leibler measure, which quantifies discrepancies between time series. Testing of the system, conducted at a stand with Raspberry Pi single-board computers and

STM32 microcontrollers that simulate conveyor production, confirmed the effectiveness of the system. Attacks such as Nmap scanning and password cracking were detected in the early stages by analyzing abnormal bursts of network activity. The results demonstrate that the system is capable of minimizing risks by providing adaptive detection of attacks on industrial nodes without deep and lengthy analysis of statistical data.

***Keywords**: attack detection system, smart manufacturing, ModBus TCP, anomaly detection, industrial network cyber security.*

Введение

Развитие умного производства, характеризующееся интеграцией Интернета вещей (IoT-устройств), промышленных контроллеров и облачных платформ, привело к росту угроз кибербезопасности. Основная уязвимость заключается в использовании устаревших протоколов передачи данных, таких как ModBus TCP, которые изначально разрабатывались без учета современных требований к защите информации. ModBus, будучи одним из старейших и наиболее распространенных протоколов в промышленной автоматизации, обеспечивает простоту интеграции и совместимость устройств, что делает его популярным в секторах энергетики, нефтегазовой промышленности и логистики. Однако его ключевая особенность – отсутствие встроенных механизмов шифрования и аутентификации – превращает его в уязвимое звено инфраструктуры [1].

Актуальность проблемы подтверждается случаями кибератак, с использованием вредоносного программного обеспечения (ПО) FrostyGoop, которые эксплуатируют уязвимости ModBus для нарушения работы промышленных систем [2].

Подобные атаки демонстрируют, что традиционные методы защиты, основанные на сигнатурном анализе, неэффективны против новых угроз, требующих детектирования аномалий в реальном времени. В статье предлагается система обнаружения атак, которая основывается на анализе сетевого трафика и физических параметров узлов умного производства для выявления киберугроз без предварительного обучения на эталонных данных.

Обзор существующих систем обнаружения атак

Современные системы обнаружения вторжений (IDS) в промышленных сетях преимущественно используют сигнатурный подход, предполагающий сравнение сетевых пакетов с базой известных угроз. Однако данный метод не способен идентифицировать новые типы атак, такие как уязвимость нулевого дня или целевые эксплойты, что снижает его эффективность в условиях совершенствующихся киберугроз.

Сигнатурные системы обнаружения вторжений (IDS) требуют постоянного обновления баз данных угроз, что в динамичных промышленных средах, где устройства часто работают без простоя, становится технически и органи-

зационно сложной задачей. Например, атаки, эксплуатирующие уязвимости нулевого дня, остаются незамеченными до тех пор, пока сигнатура угрозы не будет добавлена в реестр, что создает критическое окно уязвимости.

Дополнительным ограничением является неспособность таких систем распознавать атаки, модифицированные под конкретную инфраструктуру, – например, полиморфные вредоносные программы, изменяющие свой код для обхода детектирования [3].

Это особенно критично для промышленных протоколов вроде ModBus TCP, где отсутствие встроенной защиты делает системы уязвимыми к целевым атакам, таким как манипуляция командами для управления оборудованием [4].

Альтернативой являются системы, основанные на анализе аномалий, которые строят модель «нормального» поведения системы и фиксируют отклонения от нее [5]. Однако большинство таких решений сталкиваются с рядом принципиальных ограничений, снижающих их применимость в промышленных условиях.

Во-первых, для создания достоверной модели требуется длительный этап обучения, в течение которого система собирает и анализирует данные в условиях, когда сеть гарантированно не подвергается атакам. В реальных промышленных средах, где оборудование работает непрерывно, такой этап затруднителен или невозможен [6]. Например, внезапные изменения в режиме работы конвейерной линии или обновление прошивки контроллера, во время обучения модели, могут исказить модель «нормального» поведения, приводя к ложным срабатываниям [7].

Во-вторых, существующие системы анализа аномалий фокусируются преимущественно на сетевом трафике, игнорируя физические параметры устройств, такие как загрузка центрального процессора (CPU), температура компонентов или уровень потребления энергии. Это создает «слепые зоны»: атаки, вызывающие перегрузку процессора через вредоносные скрипты или манипуляцию промышленными контроллерами, остаются незамеченными до тех пор, пока не произойдет критический сбой.

Дополнительной проблемой является неспособность таких систем учитывать контекст эксплуатации оборудования. Например, рост числа ModBus-запросов в ночное время может быть расценен как аномалия, хотя на самом деле это часть планового технического обслуживания.

Несмотря на указанные недостатки, обнаружение аномалий на основе сетевого трафика признается организациями эффективным инструментом противодействия угрозам [8].

Таким образом, традиционные системы обнаружения вторжений, основанные на статических сигнатурах, демонстрируют низкую эффективность в защите промышленных сетей от изощренных киберугроз, таких как атаки нулевого дня или полиморфные вредоносные программы, оставляя

критическую инфраструктуру уязвимой [9]. В то же время, несмотря на растущую популярность методов анализа аномалий, их потенциал в промышленных условиях ограничен из-за игнорирования физических параметров устройств и неспособности адаптироваться к динамике производственных процессов.

Это создает парадоксальную ситуацию: системы, призванные противостоять новым угрозам, сами становятся «узким местом» безопасности из-за технических ограничений и высокого уровня ложных срабатываний. Следовательно, для повышения устойчивости умного производства требуется разработка гибридных решений, сочетающих анализ сетевого трафика с мониторингом физических показателей и учитывающих контекст эксплуатации оборудования.

Методологическая основа системы обнаружения атак на уровне узла умного производства

Предлагаемая система обнаружения атак решает указанные проблемы за счет комбинированного анализа сетевых и физических данных в реальном времени, что позволяет выявлять угрозы на ранних этапах их проявления. Ее ключевая особенность — отсутствие необходимости в предварительном обучении модели на исторических данных, что критически важно для промышленных сред, где оборудование функционирует непрерывно, а простои для сбора «нормальных» данных недопустимы.

Кроме того, система интегрирует функцию отслеживания и учета текущих технологических процессов, позволяя пользователю дополнительно задавать параметры каждого процесса, для более точного анализа.

Система обнаружения атак функционирует на основе динамического сравнения временных рядов данных, что позволяет идентифицировать аномалии без предварительного обучения на эталонных наборах «нормальной» активности.

Ключевой принцип системы заключается в количественной оценке расхождений между вероятностными распределениями параметров за текущий и предшествующий временные интервалы. Такой подход исключает зависимость от статических моделей поведения и обеспечивает адаптивность к изменяющимся условиям промышленной среды.

Система обрабатывает три категории данных:

1. Сетевые параметры:
    - Количество пакетов по протоколам (TCP, UDP, ModBus TCP и др.).
    - Частота и структура ModBus-запросов, включая анализ Function Code, что критически важно для выявления несанкционированных операций.

2. Физические параметры:
   - Загрузка центрального процессора, использование оперативной памяти, температура компонентов. Эти метрики позволяют обнаруживать атаки, вызывающие аппаратную перегрузку (криптомайнинг или DDoS-атаки).
3. Технологические процессы :
   - Временные характеристики выполнения операций (длительность цикла конвейера).
   - Количество управляющих пакетов, ассоциированных с текущими процессами (задается оператором в качестве метаданных для каждого узла).

Для унификации анализа разнородных данных применяется метод нормализации, основанный на теоретико-вероятностных моделях:

- Распределение Пуассона используется для дискретных параметров, описывая вероятность возникновения событий за фиксированный интервал времени. Используемая формула для распределения Пуассона (1)

$$P(k) = \frac{\lambda^k e^{-\lambda}}{k!}. \quad (1)$$

- Нормальное распределение применяется к непрерывным параметрам, аппроксимируя их статистические характеристики (математическое ожидание и дисперсию). Используемая формула для распределения Гаусса (2)

$$f(y) = \frac{1}{\sigma_s\sqrt{2\pi}} e^{-\frac{(y-M_y)^2}{2{\sigma_s}^2}}. \quad (2)$$

Нормализация преобразует исходные данные в вероятностные распределения, что позволяет количественно оценить динамику изменений через меру Кульбака-Лейблера (KL-дивергенцию). Используемая формула для вычисления KL-дивергенции (3)

$$D_{KL}(P||Q) = \sum_i P(i) \log \frac{P(i)}{Q(i)}. \quad (3)$$

Высокие значения KL-дивергенции между текущим и предыдущим временными интервалами указывают на статистически значимые отклонения, что служит индикатором потенциальной атаки.

Важно отметить, что концепция энтропии уже давно показывает свою эффективность при анализе сетевого трафика. Например, методы, основанные на оценке информационной энтропии, успешно используются для выявления DDoS-атак [10].

Архитектура системы

Системы обнаружения атак представляет собой приложение для операционной системы Linux, написанное на языке программирования C++. Приложение построено по модульному принципу, что обеспечивает гибкость и масштабируемость, и включает следующие модули:

- Модуль сбора данных – агрегирует информацию из сетевого трафика и датчиков устройств. Для захвата и анализа сетевых пакетов в реальном времени используется библиотека libpcap. Данные физических параметров считываются через файловую систему proc.
- Модуль анализа данных – выполняет нормализацию параметров и рассчитывает энтропию. Для повышения точности и скорости вычислений используется библиотека Boost.
- Модуль принятия решений – классифицирует аномалии на основе пороговых значений KL-дивергенции, формирует отчеты для оператора и сохраняет результаты в локальной базе данных SQLite для последующего анализа.
- Модуль отслеживания технологических процессов – отслеживает последовательность и длительность операций, используя метаданные технологических процессов. Это позволяет учитывать контекст при анализе данных: так, всплеск сетевой активности в фазе «ожидания» будет классифицирован как аномалия.
- Модуль выявления аномалий технологических процессов – анализирует отклонения в динамике управляющих команд на каждом этапе производственного цикла.

Модульная структура и выбор технологий (C++, libpcap, SQLite, Linux) позволяют развернуть систему на устройствах с ограниченными ресурсами как например, на одноплатных компьютерах Raspberry Pi, что особенно актуально для умного производства. Схема взаимодействия модулей представлена на рис. 1.

Практическая реализация и тестирование

Для проверки системы обнаружения атак был разработан и развернут тестовый стенд, моделирующий умное производство. Архитектура стенда включает следующие компоненты:

1. Физическая основа:
   - Конвейерная лента с прессовочным механизмом, имитирующая процесс обработки грузов.

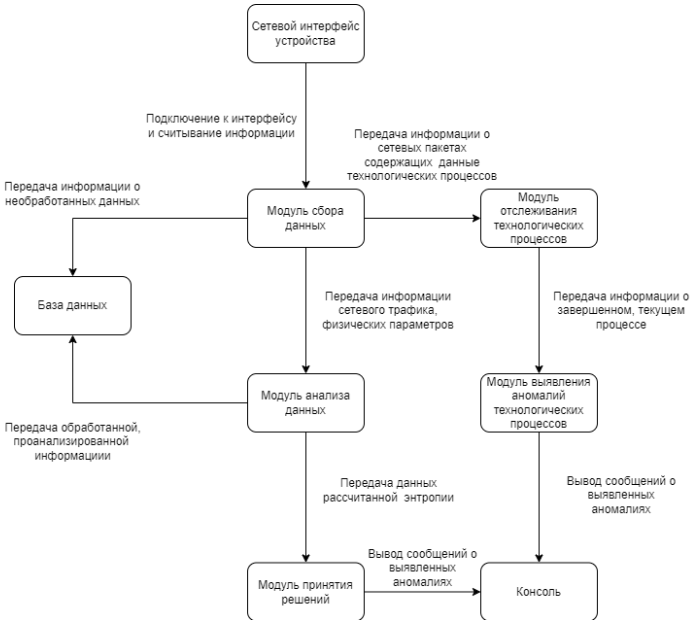


Рис. 1. Схема взаимодействия модулей системы обнаружения

2. Вычислительные узлы:
   - Три одноплатных компьютера Raspberry Pi , выполняющих роль:
     - PLC (программно-логический контроллер) для управления оборудованием;
     - HMI (человеко-машинный интерфейс) для визуализации данных;
     - SCADA-сервер (система диспетчерского управления и сбора данных).
3. Управляющие модули:
   - Два микроконтроллера STM32, отвечающих за привод конвейерной ленты и сбор данных с датчиков положения груза.

Все компоненты интегрированы в единую сеть на основе протокола ModBus TCP, что обеспечивает взаимодействие между PLC, HMI, SCADA и исполнительными устройствами. Стенд воспроизводит типовой сценарий промышленного процесса: PLC, получая задания от HMI, управляет скоростью конвейера и прессов через STM32, а SCADA-система агрегирует данные для мониторинга. Такая конфигурация позволяет имитировать реальные условия эксплуатации, включая сетевые взаимодействия и обработку физических параметров.

Для оценки эффективности разработанной системы были протестированы распространенные сетевые атаки, которые может применить атакующий.

В качестве первичной разведки атакующий может использовать утилиту Nmap, для сканирования сети и идентификации активных узлов [11]. Данное действие вызывает аномальный всплеск TCP/UDP-трафика, что приводит к увеличению энтропии. На рис. 2 представлен график значений энтропии, рассчитанных для временных интервалов (длительность интервала 10 секунд) под воздействием атаки - сканирование.

Рис. 2. График значений энтропии для TCP пакетов при проведении сканирования использованием Nmap

Для получения несанкционированного доступа к устройству, атакующий может воспользоваться атакой подбор пароля, [12] применение которой вызывает увеличение количества TCP запросов к целевой системе. Система также фиксирует подобные изменения как аномалию. На рис. 3 представлен график значений энтропии, рассчитанных для временных интервалов (длительность интервала 10 секунд) под воздействием атаки – подбор пароля.

Рис. 3. График значений энтропии для TCP пакетов при проведении атаки подбор пароля

Также атакующий может воспользоваться различными DDoS-атаками, для дестабилизации работы системы. Подобные атаки не только вызывают серьезные возмущения в сетевом трафике, но также оказывают сильное влияние на загрузку CPU. Система улавливает повышение загруженности CPU, относительно нормальной работы. На рис. 4 представлен график значений энтропии, рассчитанных для временных интервалов (длительность интервала 10 секунд) под воздействием атаки – отказ в обслуживании.

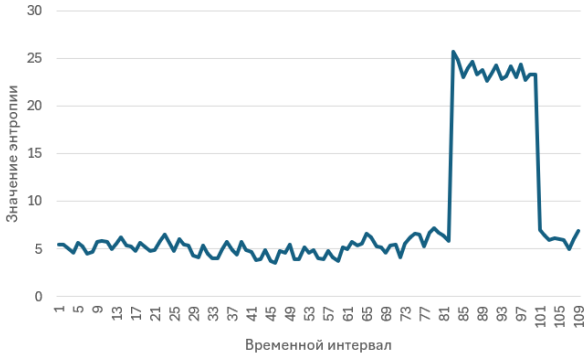


Рис. 4. График значений энтропии для загруженности CPU при проведении DDoS атаки

Для интеграции контекста технологических процессов в модель обнаружения атак была проведена детальная оценка управляющих команд, передаваемых по протоколу ModBus TCP на тестовом стенде. В рамках полного цикла перемещения груза выделены четыре ключевых этапа – технологических процесса:

1. Ожидание (состояние покоя конвейера).
2. Движение вперед (активация привода ленты).
3. Прессовка (срабатывание штамповочного механизма).
4. Обратное движение (возврат ленты в исходное положение).

Для каждого этапа идентифицированы соответствующие функциональные коды ModBus и зафиксирована статистика передачи пакетов. На основе этих данных система осуществляет детектирование аномалий, анализируя отклонения в количестве и последовательности управляющих команд. На рис. 5 представлен график количества пакетов технологических процессов, для циклов производства при нормальной работе.

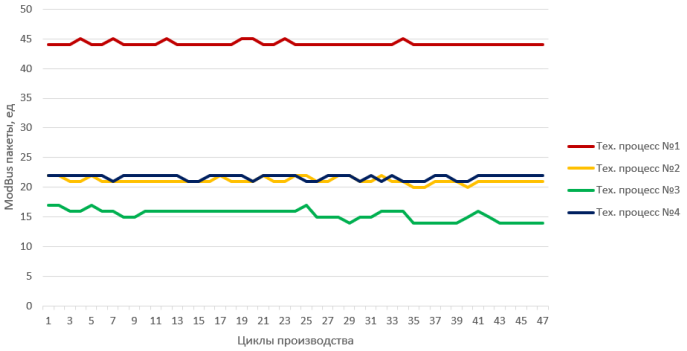


Рис. 5. График количества сетевых пакетов технологических процессов при нормальной работе

При моделировании атаки, направленной на несанкционированный перехват и модификацию управляющих команд ModBus, наблюдается значительное отклонение графиков технологических процессов от эталонных значений. Система обнаружения атак идентифицирует подобные отклонения как аномалию. На рис. 6 представлен график количества пакетов технологических процессов, для циклов производства под воздействием атаки - перехват и модификация пакетов.

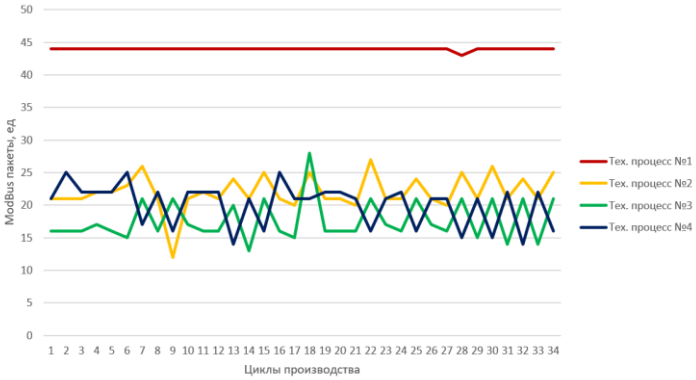


Рис. 6. График количества сетевых пакетов технологических процессов, при перехвате и модификации пакетов

Выводы

Разработанная система обнаружения атак демонстрирует высокую эффективность в защите узлов умного производства от современных киберугроз. Ключевым преимуществом системы является её способность выявлять аномалии в реальном времени без предварительного обучения на исторических данных с использованием KL-дивергенции.

Тестирование на стенде, включающем Raspberry Pi и STM32, подтвердило способность системы обнаруживать атаки на ранних этапах. Результаты исследования подтверждают, что предложенный подход значительно повышает уровень кибербезопасности критической инфраструктуры, обеспечивая баланс между точностью детектирования и оперативностью реагирования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Конев А.А., Репкин В.С., Цимбалов К.И.* Сценарий атаки на автоматизированную систему управления технологическим процессом с учетом уязвимости протокола Modbus TCP [Электронный ресурс]. – 2024. – URL: https://swsys.ru/index.php?page=article&id=5125 (дата обращения: 20.03.2025).
2. *Graham M., Ahlers C., O'Meara K.* DRAGOS, INC. Impact of FrostyGoop ICS Malware on Connected OT Systems [Электронный ресурс]. – 2024. – URL: https://regmedia.co.uk/2024/07/23/dragos_frostygoop-report.pdf.
3. SafAaeon inc, Understanding polymorphic viruses and their impact on Cybersecurity [Электронный ресурс]. – 2023. – UPL: https://www.safeaeon.com/security-blog/polymorphic-virus/ (дата обращения: 07.03.2025).
4. *Alsabbagh W., Amogbonjaye S., Urrego D., Langendoerfer P*. A Stealthy False Command Injection Attack on Modbus based SCADA Systems – 2022. – URL: https://www.researchgate.net/publication/365366081_A_Stealthy_False_Command_Injection_Attack_on_Modbus_based_SCADA_Systems (дата обращения: 12.03.2025).
5. *Awaad A., Alheeti K.M., Najem A.K.* Anomaly-Based IDS (Intrusion Detection System) for Cyber-Physical Systems. – 2024. – URL: https://www.researchgate.net/publication/387181846_Anomaly-Based_IDS_Intrusion_Detection_System_for_Cyber-Physical_Systems (дата обращения: 22.03.2025).
6. *Umer M.A., Junejo K.N., Jilani M.T., Mathur A.* Machine Learning for Intrusion Detection in Industrial Control Systems: Applications, Challenges, and Recommendations. – 2022. – URL: https://www.researchgate.net/publication/358846616_Machine_Learning_for_Intrusion_Detection_in_Industrial_Control_Systems_Applications_Challenges_and_Recommendations (дата обращения: 17.03.2025).
7. Securitylab, Сетевые аномалии. Что это и как их определить? [Электронный ресурс] – 2023. – URL: https://www.securitylab.ru/analytics/535530.php (дата обращения: 05.04.2025).
8. *Грибанов С.* NDR – следующий уровень развития сетевой безопасности [Электронный ресурс]. – 2025. – URL: https://garda.ai/blog/news/ndr-sleduyushchiy-uroven-razvitiya-setevoy-bezopasnosti (дата обращения: 10.03.2025).

9. Information Security Asia. What Is An Intrusion Detection System [Электронный ресурс]. – 2025. – URL: https://informationsecurityasia.com/what-is-an-intrusion-detection-system/#Can_an_IDS_detect_zero-day_exploits (дата обращения: 10.04.2025).
10. *Yu H., Yang W., Cui B., Sui R., Wu*. Renyi entropy-driven network traffic anomaly detection with dynamic threshold [Электронный ресурс]. – 2024. – URL: https://cybersecurity.springeropen.com/articles/10.1186/s42400-024-00249-1 (дата обращения: 25.02.2025).
11. Бальдер Нагвальевич, Как использовать Nmap для сканирования уязвимостей [Электронный ресурс]. – 2024. – URL: https://android-robot.com/kak-ispolzovat-nmap-dlya-skanirovaniya-uyazvimostej/ (дата обращения: 14.04.2025).
12. Selectel, Brute force-атаки [Электронный ресурс]. – 2025. – URL: https://selectel.ru/blog/what-is-brute-force/ (дата обращения: 02.03.2025).

УДК 004.056

Е.И. Мижутина

Ярославский государственный университет им. П.Г. Демидова,
Россия, г. Ярославль

СРАВНИТЕЛЬНЫЙ АНАЛИЗ НУЛЕВЫХ ВОДЯНЫХ ЗНАКОВ ЦИФРОВЫХ КАРТ, ОСНОВАННЫХ НА СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИКАХ

В работе рассматриваются современные подходы к защите цифровых карт, в том числе с использованием технологии нулевого водяного знака (zero-watermarking). Цель исследования – сравнение эффективности различных алгоритмов создания нулевых водяных знаков для векторных карт, основанных на статистических характеристиках и частотном анализе. В качестве задач исследования выделены: анализ существующих методов защиты данных, реализация и тестирование алгоритмов, а также оценка их устойчивости к атакам. Проведенные эксперименты показали, что оба алгоритма устойчивы к атакам. Однако матричный дескриптор обладает более высокой точностью. Основной вывод исследования заключается в том, что выбор метода защиты пространственных данных должен учитывать требования к точности, сложности реализации и типу данных. Результаты работы могут быть использованы для разработки более совершенных алгоритмов защиты векторных карт.

Ключевые слова: *пространственные данные, нулевой водяной знак, защита данных, частотный анализ, дескриптор.*

The paper explores modern approaches to digital map protection using zero-watermarking technology. The aim of the study is to compare the effectiveness of different algorithms for creating zero-watermarks for vector maps based on frequency analysis. The objectives of the study include analyzing existing data protection methods, implementing and testing algorithms, and evaluating their resilience to object addition/deletion attacks. The experiments show that both algorithms are resistant to attacks. However, the matrix approach demonstrates higher accuracy. The main conclusion of the study is that the choice of vector data protection method should consider the requirements for accuracy, implementation complexity, and data type. The results of the work can be used to develop more advanced algorithms for protecting vector maps.

Keywords: *vector data, zero-watermark, data protection, frequency analysis, descriptor.*

В современном мире пространственные данные стали критически важным ресурсом, лежащим в основе множества решений – от градостроительства и сельского хозяйства до навигационных систем и экологического мониторинга. Их обработка, как правило, осуществляется с помощью геоинформационных

систем (ГИС). Пространственные данные – это цифровое представление географических объектов, где каждый объект описывается с помощью координат и атрибутов. В ГИС объекты хранятся по слоям, каждый слой содержит объекты одной природы (например, слой рек, слой автомобильных дорог, слой населенных пунктов) и одной геометрии, здесь под геометрией понимается содержится ли в слое набор ломаных линий (линейный слой, например, слой дорог), многоугольников или полигонов (полигональный слой, например, слой водоемов или административных границ) или набор точек (точечный слой, например слой мелких населенных пунктов). Набор согласованных векторных слоев представляет собой цифровую карту.

Процесс формирования качественных пространственных данных связан с рядом сложностей: необходимостью применения дорогостоящего оборудования, привлечения квалифицированных специалистов, согласованности разнородных источников информации, также требуются значительные ресурсы для поддержания актуальности цифровой карты. Карты являются объектом авторского права, что следует из Гражданского кодекса РФ, статья 1259. Отсюда возникает задача защиты авторских прав на цифровые карты.

Одним из ключевых подходов к защите пространственных данных является применение цифровых водяных знаков (ЦВЗ) [1–3]. Водяные знаки представляют собой невидимые или слабозаметные маркеры, которые встраиваются в данные для определения их происхождения или собственности. ЦВЗ могут быть как видимыми, так и невидимыми, но в случае пространственных данных чаще используются невидимые методы, чтобы не нарушать целостность и точность информации. Как правило, ЦВЗ встраиваются в координаты точек [4]. Заметим, что защита цифровых карт должна вестись по двум направлениям: во-первых, защита пространственных данных от незаконного копирования и распространения, во-вторых, защита от внесения изменений или искажения набора пространственных данных.

В соответствии с первым направлением ЦВЗ должен быть стойким к различным видам атак:

- геометрическим: эти атаки включают изменение геометрических характеристик данных, таких как масштабирование, поворот, сдвиг или искажение;
- добавления/удаления объектов, в том числе и атака генерализацией;
- на атрибутивную информацию, то есть изменение атрибутов объектов, таких как названия, типы или другие метаданные;
- смены проекции, т.е. перевод данных в другую картографическую проекцию;
- скремблирования или изменения порядка хранения данных [1–5].

Для оповещения о несанкционированных изменениях ЦВЗ должен быть «хрупким», то есть разрушаться при любых преобразованиях [6].

Инновационный подход к созданию водяных знаков описан в исследовании [7], где используется машинное обучение для создания адаптивных водяных знаков. В этом методе алгоритм автоматически подстраивается под характеристики данных, что позволяет повысить устойчивость водяного знака к различным видам атак.

Для защиты пространственных данных также применяется технология zero-watermarking (нулевого водяного знака). В отличие от традиционных методов, этот подход не вносит изменений в исходные данные, а формирует уникальный дескриптор на основе их внутренних характеристик. Это позволяет сохранить исходное качество и точность пространственной информации, обеспечивая надежную защиту авторских прав. При проверке дескриптор вычисляется заново, после чего сформированный ЦВЗ посредством запроса к базе данных сравнивается с исходным, и на этом основании делается вывод об авторстве.

В работе [8] предложен метод, формирующий нулевой водяной знак на основе геометрических характеристик объектов, таких как углы и расстояния между вершинами полигонов. Этот подход позволяет создавать устойчивые к искажениям водяные знаки, которые сохраняют свою целостность даже при изменении масштаба или повороте карты.

Ученые из Китая и, независимо от них, исследователи из Ярославля предложили использовать для формирования дескриптора статистические характеристики цифровой карты [9,10]. Каждый фрагмент цифровой карты содержит определенное количество точек (вершин), при этом в другом участке такой же площади с довольно высокой вероятностью количество точек будет иным. Отсюда частоты распределения точек карты кажутся уникальной характеристикой каждой цифровой карты. Кроме того, дескриптор, основанный на частотном анализе, будет стоек к атакам скремблирования, так же, как и к геометрическим атакам, и позволит установить авторство цифровой карты.

Целью настоящего исследования было сравнение двух различных алгоритмов создания нулевого водяного знака для векторных карт, основанных на статистических характеристиках исходных данных.

В статье [9], был представлен алгоритм создания дескриптора, основная идея которого состоит в следующем: вычисляется средняя точка (AvePoint), согласно формуле 1, где ($\overline{X}$, $\overline{Y}$) координата средней точки:

$$\overline{X} = \sum_{i=1}^{m} x_i$$
$$\overline{Y} = \sum_{i=1}^{m} y_i \quad (1)$$

Карта делится на кольца, разделяемые концентрическими окружностями, с центром в точке (AvePoint), и расстоянием (Step), как показано на рис. 1.

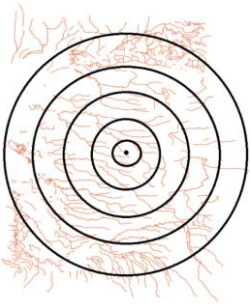


Рис. 1. Деление карты концентрическими окружностями

Благодаря разделению концентрическими окружностями, данный алгоритм устойчив к атакам вращения.

Затем подсчитывается количество вершин в каждом кольце и заносится в массив(M). Вычисляется среднее количество точек в кольце (AveNums) и строится двоичный вектор(M*), согласно правилу (2):

$$M_i^* = \vdash_{1,\, M_i \geq AveNums}^{0,\, M_i < AveNums} \quad (2)$$

Выполняется операция XOR над вектором M* и битами информации об авторе для генерации водяного знака, и водяной знак регистрируется в хранилище прав интеллектуальной собственности. Нулевой водяной знак может быть извлечен аналогично и будет сравнен с зарегистрированным водяным знаком, и, таким образом, авторские права могут быть подтверждены.

Данный алгоритм по вычислению дескриптора был реализован. Была проведена серия экспериментов для определения его стойкости. Дескриптор исходной цифровой карты сравнивался с дескриптором той же карты, подвергнутой какой-либо атаке. При этом использовался следующий алгоритм проверки подлинности карты: вычислялся дескриптор для эталонной карты и для проверяемой карты с одним и тем же параметром Step, задающим расстояние между концентрическими окружностями; производилось поэлементное сравнение вычисленного вектора M* с эталонным и определялся процент соответствия дескриптора проверяемой карты исходному.

Следует отметить, что по построению дескрипторы на основе статистических характеристик, являются стойкими к геометрическим атакам, атакам скремблирования и смены проекции.

Перечень атак, применявшихся к цифровым картам:

1. Увеличение числа точек, то есть добавление новых объектов на карту, на 25%, 33%, 50% и 75%
2. Сокращение числа точек путем геометрического упрощения на 25%, 33%, 50% и 75%.

В качестве исходных данных рассматривались фрагменты цифровых карт севера Краснодарского края масштаба 1:1000000. Параметр Step подбирался таким образом, чтобы расстояние между концентрическими окружностями было равно 1, 2, 5, 10 мм в масштабе карты.

Для атаки добавлением объектов к исходному набору данных, представляющему собой реки и каналы, добавлялись дополнительные слои. Слои подбирались таким образом, чтобы обеспечить увеличение исходного количества точек на 25%, 33%, 50% и 75%.

Для проведения атаки геометрического упрощения использовался алгоритм Дугласа – Пейкера [11] с сокращением количества точек на 25, 33, 50 и 75% от исходного набора данных. Результаты экспериментов представлены в табл. 1, 2.

Таблица 1

Результаты стойкости дескриптора после атаки добавления

Добавление количества точек в %	Расстояние между концентрическими окружностями для вычисления дескриптора (в мм в масштабе карты)			
	1	2	5	10
25	82%	84%	83%	81%
33	74%	73%	74%	77%
50	74%	75%	74%	77%
75	68%	70%	69%	68%

Таблица 2

Результаты стойкости дескриптора после атаки упрощения

Сокращение количества точек в %	Расстояние между концентрическими окружностями для вычисления дескриптора (в мм в масштабе карты)			
	1	2	5	10
25	85%	89%	97%	100%
33	94%	98%	96%	100%
50	81%	84%	87%	97%
75	75%	82%	87%	90%

Для проверки уникальности дескриптора было проведено сравнение с картой иной местности того же масштаба, но содержащую примерно такое же количество точек. Результаты представлены в табл. 3.

Таблица 3

Результаты сравнения дескрипторов различных фрагментов карт

Расстояние между концентрическими окружностями для вычисления дескриптора (в мм в масштабе карты)			
1	2	5	10
79%	69%	81%	75%

В работе [10] было предложено два подхода к созданию дескриптора, основанного на статистических характеристиках карты: линейный и матричный.

Линейный вариант. Векторная карта разбивается на k частей вертикальными параллельными линиями, как показано на рис. 2,а.

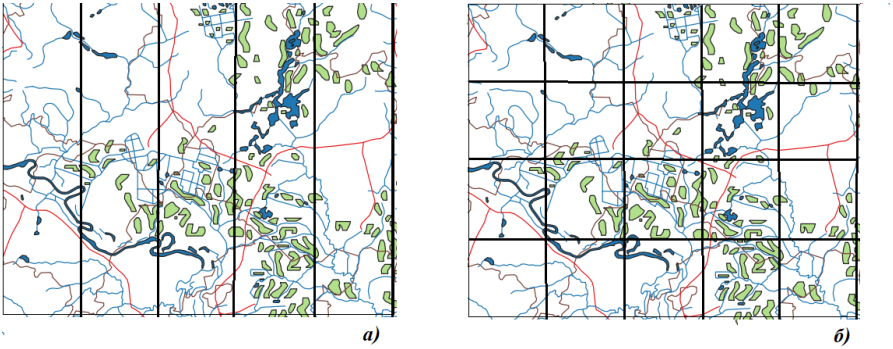


Рис. 2. Разбиение цифровой карты при k=5: а) линейного дескриптора, б) матричного

Для каждой из k частей подсчитываются принадлежащие ей точки векторной карты и формируется вектор Watermark размера k. После этого вектор нормируется. Находим min и max – минимальное и максимальное значение в массиве Watermark и вычисляем его элементы по формуле 3:

$$Watermark[i] = \frac{Watermark[i]-min}{max-min}, \text{ где } i = \overline{0, k-1}. \quad (3)$$

Получаем линейный дескриптор Watermark в виде вектора, каждый элемент которого находится в промежутке от 0 до 1.

Матричный вариант. На исходную векторную карту набрасывается прямоугольная сетка k×k (рис. 2,б). Для каждой ячейки сетки подсчитывается количество принадлежащей ей точек карты. Значения вычисляются и нормируются аналогично линейному подходу. На выходе получаем дескриптор в матричном виде.

Были проведены те же самые атаки, что и в случае выше. Из-за того, что элементом дескриптора является действительное число, считалось, что элементы совпадают, если их разность по модулю меньше установленной ошибки – 5%. Результаты экспериментов надёжности дескриптора против атак добавления и удаления объектов, а также уникальности дескриптора представлены в табл. 4-6 [10].

Таблица 4

Результаты стойкости дескрипторов после добавления объектов

Дескриптор	Добавление количества точек в %	Сторона ячейки для вычисления дескриптора (в мм в масштабе карты)			
		1	2	5	10
Линейный	25	65%	31%	31%	68%
	33	63%	31%	27%	48%
	50	59%	34%	20%	51%
	75	45%	42%	50%	20%
Матричный	25	93%	93%	92%	85%
	33	92%	92%	90%	80%
	50	90%	90%	84%	69%
	75	89%	89%	80%	69%

После сравнения результатов противостояния дескрипторов из статей атакам добавления, можно сделать следующие выводы: алгоритм, основанный на концентрических окружностях, показывает более высокие проценты совпадения, нежели линейный алгоритм, где дескриптор представляет собой массив значений в отрезке [0,1]. Однако дескриптор на основе концентриче-

ских окружностей на различных фрагментах карты дает очень схожий результат, что вызывает сомнения в его применимости на практике. Можно предположить причину подобного поведения: этот дескриптор представляет собой бинарный вектор, элемент которого равен нулю, если количество точек в соответствующем кольце меньше среднего значения, и единице в противном случае. И в другой местности могут быть участки с подобным поведением.

Таблица 5

Результаты стойкости дескрипторов после атаки упрощения

Дескриптор	Сокращение числа точек на %	Сторона ячейки для вычисления дескриптора (в мм в масштабе карты)			
		1	2	5	10
Линейный	25	82%	94%	100%	100%
	33	85%	88%	98%	100%
	50	65%	73%	50%	89%
	75	26%	30%	31%	41%
Матричный	25	96%	96%	98%	99%
	33	94%	94%	96%	96%
	50	92%	91%	93%	86%
	75	91%	86%	80%	68%

Таблица 6

Результаты сравнения дескрипторов различных фрагментов карт

Дескриптор	Сторона ячейки для вычисления дескриптора (в мм в масштабе карты)			
	2	5	10	15
Линейный	14%	12%	10%	11%
Матричный	45%	32%	26%	24%

Наилучшие результаты во всех экспериментах показал матричный дескриптор, предложенный ярославскими исследователями. Это можно объяснить тем, что: отсутствует зависимость от центральной точки, области разбиения имеют одинаковую площадь и форму, благодаря этому покрытие карты более равномерное, а результаты точнее. Следует отметить, что оптимальным выбором параметров Step и k является 5-10 мм в масштабе карты.

Перспективы дальнейших исследований включают разработку универсальных алгоритмов, сочетающих преимущества различных подходов к созданию водяного знака.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Peng Y., Lan H., Yue M. et al.* Multipurpose watermarking for vector map protection and authentication // Multimedia Tools and Applications. – 2018. – Vol. 77. – P. 7239-7259. – DOI: 10.1007/s11042-017-4631-z.
2. *Выборнова Ю.Д., Сергеев В.В*. Метод защиты векторных карт с использованием изображения ЦВЗ как вторичного контейнера // Компьютерная оптика. – 2019. – Т. 43, № 3. – С. 474-483. – DOI: 10.18287/2412-6179-2019-43-3-474-483.
3. *Zhu C.Q.* Research progresses in digital watermarking and encryption control for geographical data // Acta Geodaetica et Cartographica Sinica. – 2017. – Vol. 46. – P. 1609-1619. - DOI:10.11947/j.AGCS.2017.20170301
4. *Li Y., Zhang L., Wang X., Zhang X., Zhang Q.* A Novel Invariant Based Commutative Encryption and Watermarking Algorithm for Vector Maps // ISPRS International Journal of Geo-Information. – 2021. – Vol. 10. – P. 718. – DOI: 10.3390/ijgi10110718.
5. *Wang Y., Yang C., Ding K.* Multiple Watermarking Algorithms for Vector Geographic Data Based on Multiple Quantization Index Modulation // Applied Sciences. – 2023. – Vol. 13. – P. 12390. – DOI: 10.3390/app132212390.
6. *Wang N., Kankanhalli M.* 2D Vector Map Fragile Watermarking with Region Location // ACM Transactions on Spatial Algorithms and Systems. – 2018. – Vol. 4, No. 4. – Article 12. – 25 p. – DOI: 10.1145/3239163.
7. *Zhou X., Cao C., Ma J., Wang L.* Adaptive Digital Watermarking Scheme Based on Support Vector Machines and Optimized Genetic Algorithm // Mathematical Problems in Engineering. – 2018. – Vol. 2018. – № 6. – P. 1–9. – DOI: 10.1155/2018/2685739.
8. *Wang S., Zhang L.-M., Zhang Q.-H., Li Y.* A Zero-watermarking Algorithm for Vector Geographic Data Based on Feature Invariants // Research Square. – 2022. – September. – DOI: 10.21203/rs.3.rs-2030350/v1.
9. *Wang X., Huang D., Zhang Z.* A Robust Zero-Watermarking Algorithm for Vector Digital Maps Based on Statistical Characteristics // Journal of Software. – 2012. – Vol. 7, No. 10. – P. 2349-2356. – DOI: 10.4304/jsw.7.10.2349-2356.
10. *Якимова О.П., Горшков В.Г.* Новый дескриптор на основе частотного анализа для защиты векторных карт // Материалы 34-й Международной конференции по компьютерной графике и машинному зрению GRAPHICON 2024. – Омск: Омский государственный технический университет, 2024. – С. 708-714. – DOI: 10.25206/978-5-8149-3873-2-2024-708-714.
11. *Douglas D.H., Peucker T.K.* Algorithms for the reduction of the number of points required to represent a digitized line or its caricature // Cartographica: The International Journal for Geographic Information and Geovisualization. – 1973. – Vol. 10, No. 2. – P. 112-122.

УДК 004.056

В.А. Овсянникова

Южный федеральный университет, Россия, г. Таганрог

СЕРВИС ОЦЕНКИ УГРОЗ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

В данной статье описаны этапы разработки сервиса оценки угроз киберфизических систем, который предназначен для оценки угроз на основе анализа уязвимостей, атак и структурно-функциональных характеристик компонентов. Сервис реализует подход к моделированию угроз и подбору потенциальных уязвимостей на основе актуальных баз данных, включающих сведения об известных типах атак, угрозах, уязвимостях и структурно-функциональных характеристиках. Пользователь может как загрузить СФХ автоматически, так и выбрать параметры из базы. Все результаты анализа и отображаются в личном кабинете, структурированы по сервисам. В ходе исследования был проведен анализ аналогов и выбран функционал веб-сервиса. Также описан функционал и разработан макет дизайна сервиса оценки угроз киберфизических систем.

Ключевые слова: *База данных уязвимостей, база данных угроз, база данных атак, вектор атаки, структурно-функциональные характеристики.*

This article describes the development stages of a cyber-physical system threat assessment service designed to assess threats based on an analysis of vulnerabilities, attacks, and the structural and functional characteristics of components. The service implements an approach to threat modeling and identifying potential vulnerabilities based on up-to-date databases containing information on known attack types, threats, vulnerabilities, and structural and functional characteristics. Users can either automatically upload cyber-physical system threat assessments (SPSAs) or select parameters from the database. All analysis results are displayed in the user account, structured by service. During the study, an analysis of analogs was conducted and the functionality of the web service was selected. The functionality was also described and a design mockup for the cyber-physical system threat assessment service was developed.

Keywords: *Vulnerability database, threat database, attack database, attack vector, structural and functional characteristics.*

Введение

В условиях стремительного роста количества и сложности кибератак, защита киберфизических систем требует применения более интеллектуальных и интегрированных подходов. Традиционные средства анализа безопасности зачастую не обеспечивают комплексной обработки информации об угрозах, уязвимостях и векторах атак с учётом структурно-функциональных характеристик (СФХ) защищаемой системы. Это существенно снижает точность оценки рисков и ограничивает возможности принятия превентивных мер.

В частности, в статье «Моделирование информационной безопасности» отмечается, что существующие подходы к моделированию информационной безопасности организации сталкиваются с рядом ограничений и трудностей при практической реализации, что требует компромиссов между уровнем защищенности информационных активов и экономическими соображениями [1].

Для решения такой проблемы в рамках исследования разрабатывается клиентская часть веб-платформы. Ее основу составляют модули, обеспечивающие доступ к базам данных атак, уязвимостей, угроз и СФХ, а также сервисы: генератор векторов атак, модуль моделирования угроз и системы автоматического подбора уязвимостей. Одним из ключевых элементов является скрипт, собирающий СФХ с устройства пользователя, на основе результатов работы которого производится аналитика.

Кроме того, в документе ФСТЭК России «Методика оценки угроз безопасности информации» подчеркивается необходимость учета архитектурных особенностей систем и сетей при определении актуальных угроз безопасности информации, что свидетельствует о важности интеграции структурно-функциональных характеристик в процесс оценки угроз [2].

Целью работы является создание клиентской части веб-сервиса, ориентированной на практическое применение в области анализа угроз киберфизических систем. Разработка данного решения способствует формированию современной инфраструктуры для поддержки анализа киберугроз с учётом индивидуальных характеристик систем, что представляет интерес как для научного сообщества, так и для прикладных задач в области информационной безопасности.

Обзор аналогов

В настоящее время инструменты для моделирования угроз активно применяются. Например, Threat Dragon [3]. Данный продукт был создан для работы с моделями угроз в браузере, он позволяет строить схемы, классифицировать угрозы и описывать сценарии. Однако, как и большинство инструментов OWASP, Threat Dragon не интегрирован с реальными данными системы пользователя и не предназначен для анализа на основе СФХ.

Таблица 1

Преимущества и недостатки Threat Dragon (OWASP)

Преимущества	Недостатки
Поддержка методологии STRIDE	Не взаимодействует с реальными данными системы
Удобный интерфейс	Не проводит анализ уязвимостей
Подходит для обучения	Нет подбора атак и уязвимостей

Также стоит обратить внимание на CISA Known Exploited Vulnerabilities Catalog. Это каталог эксплуатируемых уязвимостей, публекуемый Агенством по кибербезопасности и защите инфраструктуры США представляет собой реестр, включающий исключительно те уязвимости, для которых зафиксирована фактическая эксплуатация в дикой среде. Этот каталог носит практико-ориентированный характер.

Таблица 2

Преимущества и недостатки сайта CISA Known Exploited Vulnerabilities Catalog

Преимущества	Недостатки
Гарантированная актуальность	Неудобный интерфейс
Поддержка в формате JSON и CSV	Нет механизма сопоставления с архитектурой системы
Используется в госсекторе	Не предоставляет механизма формирования моделей угроз

Матрица MITRE ATTACK представляет собой базу знаний о техниках противника и основывается на реальных наблюдениях. Однако сама по себе матрица не предоставляет механизмов визуального моделирования или интеграции с данными конкретной системы.

Таблица 3

Преимущества и недостатки MITRE ATT&CK

Преимущества	Недостатки
Регулярно обновляется на основе данных от ведущих аналитиков и компаний	Требует дополнительного сопоставления с архитектурой конкретной системы
Используется многими организациями в сфере кибербезопасности	Не учитывает индивидуальные особенности конкретной ИТ-инфраструктуры
Основана на реальных сценариях атак	Отсутствует связь с уязвимостями

Модель угроз по методическим материалам ФСТЭК России применяется при аттестации объектов информатизации. Она ориентирована на выполнение требований безопасности в рамках нормативно-правового поля РФ. Несмотря на свою регламентированность, модель требует ручного заполнения и обладает ограниченной гибкостью при работе с нестандартными архитектурами.

Таблица 4

Модели угроз ФСТЭК

Преимущества	Недостатки
Соответствует требованиям национального законодательства	Ограничение применением на территории РФ
Обеспечивает единый подход к классификации угроз	Низкая интеграция с международными базами данных
Включает учет нарушителей различного уровня	Требует участия сертифицированных специалистов

Принцип работы сервиса оценки угроз

Сервис оценки угроз киберфизических систем предназначен для анализа угроз, уязвимостей и возможных сценариев атак на киберфизические системы. Этот сервис ориентирован на специалистов в области информационной безопасности, а также может использоваться в образовательных целях для подготовки студентов технических направлений.

Ключевая особенность архитектуры клиентской части сервиса заключается в разделении на независимые сервисы. В состав входят следующие модули баз данных: структурно-функциональных характеристик, угроз, атак, уязвимостей.

Сервис сбора СФХ представляет собой вспомогательный модуль, работа которого начинается с загрузки специального скрипта, который нужно скачать на устройство пользователя. На сайте представлена инструкция по работе со скриптом и описание предназначения сервиса. После запуска скрипт начинает собирать основные структурно-функциональные характеристики среды. Скрипт содержит Python-код, который представляет собой набор системных команд Linux, сохранённых в виде строковых констант. В нем импортируется путь к JSON-файлу, куда будет сохраняться системная информация после выполнения команды. Потом описаны сетевые команды для получения списка IPv4-адресов и интерфейсов (без IPv6), текущего IP-адреса хоста, сканирования устройства в локальной сети по заданному интерфейсу. Далее присутствуют команды для получения информации о системе: имени хоста, информации о дистрибутиве, подробностей о ядре и архитектуре операционной системы. Также присутствуют команды для получения информации о программном обеспечении и службах: статуса службы systemd, списка всех установленных пакетов с версиями, списка графических приложений. Кроме того, производится сканирование TCP и UDP портов и сетевых протоколов и сохранение их в XML. Скрипт формирует файл, который нужно загрузить на сервер. Данные далее будут представлены в личном кабинете пользователя в разделе мои СФХ. Их можно использовать в остальных сервисах для детальной аналитики. Если не загружать файл с результатами работы скрипта, это не повлияет на аналитическую работу других сервисов, поскольку можно выбрать структурно-функциональные характеристики из общего списка.

Сервис формирования перечня уязвимостей содержит описание предназначения сервиса и возможность выбрать СФХ как из личного кабинета, так и из базы данных СФХ. Для удобства пользователя можно их комбинировать. В результате можно скачать файл с таблицей. С интерфейсом сервиса можно ознакомиться на рис. 1.

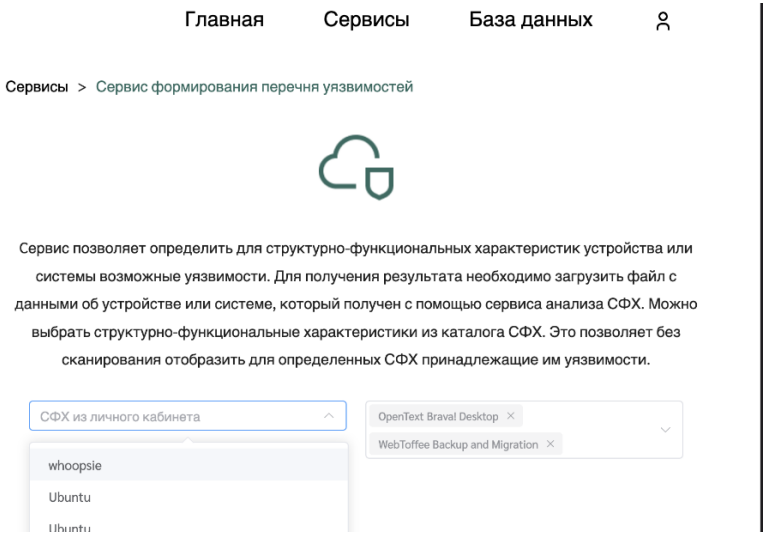


Рис. 1. Интерфейс сервиса формирования перечня уязвимостей

Сервис формирования модели угроз уязвимостей содержит описание предназначения сервиса. В форме для отправки запроса на сервер присутствуют поля: название, СФХ из личного кабинета, СФХ из базы данных, домен, характеристики. Отчет после отправки запроса сформируется и будет представлен в личном кабинете пользователя, где можно скачать файл с результатом и присутствует дата его формирования. С интерфейсом сервиса можно ознакомиться на рис. 2.

Сервис формирования вектора атаки содержит автоматический расчет вектора атаки по выбранным СФХ, вектор строится из трех этапов – точка входа, вектор атаки и нарушение функции безопасности. Есть возможность вручную выбрать этапы атаки для каждой СФХ и поддержка множественного выбора и редактирования. В результате генерируется итоговый отчет на основе введенных параметров, он сохраняется в личном кабинете пользователя. Для пользователя появляются уведомления об ошибках и успехах. С интерфейсом сервиса формирования вектора атаки можно ознакомиться на рис. 3.

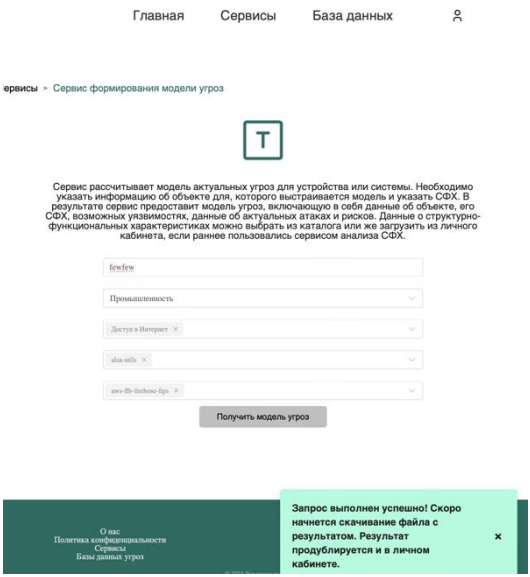


Рис. 2. Интерфейс сервиса формирования модели угроз

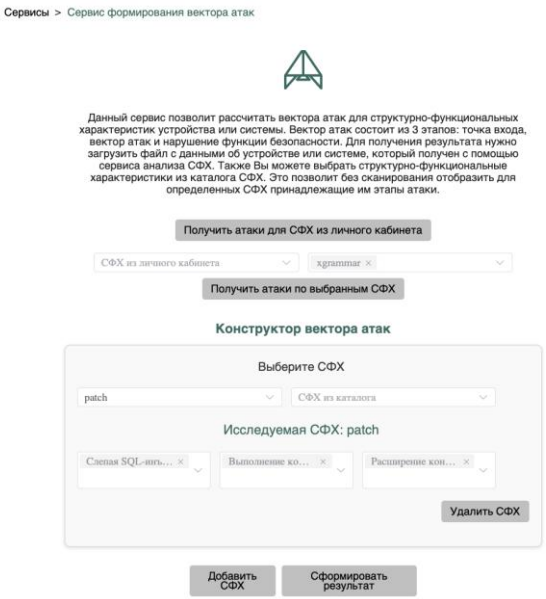


Рис. 3. Интерфейс сервиса формирования вектора атаки

Заключение

В результате проделанной работы была разработана клиентская часть веб-сервиса оценки угроз киберфизических систем, включающая в себя интерфейс взаимодействия с базами данных атак, угроз, уязвимостей и структурно-функциональных характеристик. Реализованы ключевые модули, обеспечивающие формирование вектора атаки, построение модели угроз и подбор уязвимостей. В отличие от таких решений, как OWASP Threat Dragon, сфокусированных на ручном построении моделей без привязки к архитектуре конкретной системы, созданный сервис обеспечивает практико-ориентированный подход, позволяющий проводить анализ на основе реальных данных пользователя. Также по сравнению с каталогом CISA Known Exploited Vulnerabilities, сервис предоставляет не только справочную информацию, но и применим в автоматизированной оценке угроз с учётом контекста защищаемого объекта. Пользовательский интерфейс обеспечивает интуитивное взаимодействие и отображение результатов в личном кабинете. С интерфейсом личного кабинета можно ознакомиться на рис. 4.

СФХ: aptdaemon

Атака	Этап
Обход пути	Вектор
Использование косой черты и кодирования URL в сочетании с обходом логики проверки	Вектор
Управление веб-вводом для вызовов файловой системы	Вектор
Использование обратных косых черт в альтернативном кодировании	Точка входа
Использование косой черты в альтернативном кодировании	Вектор

СФХ: Caribou

Атака	Этап
Обход пути	Вектор
Использование косой черты и кодирования URL в сочетании с обходом логики проверки	Вектор
Управление веб-вводом для вызовов файловой системы	Вектор
Использование обратных косых черт в альтернативном кодировании	Точка входа
Использование косой черты в альтернативном кодировании	Вектор

Рис. 4. Интерфейс личного кабинета

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Моделирование информационной безопасности [Электронный ресурс] // Труды Нижегородского государственного технического университета им. Р.Е. Алексеева. – 2022. – № 4. – С. 28-36. – Режим доступа: https://www.nntu.ru/frontend/web/ngtu/files/nauka/izdaniya/trudy/2022/04/028-036.pdf (дата обращения: 11.04.2025).
2. Методика оценки угроз безопасности информации [Электронный ресурс] / ФСТЭК России. – 2021. – 49 с. – Режим доступа: https://187.ussc.ru/upload/iblock/b16/b167e833baa088e23c6255f2c2767aa3.pdf (дата обращения: 11.04.2025).
3. OWASP Threat Dragon [Электронный ресурс] // Open Web Application Security Project. – Режим доступа: https://www.threatdragon.com/#/ (дата обращения: 11.04.2025).
4. *Басыня Е.А.* Системное администрирование и информационная безопасность: учебное пособие – Новосибирск: Новосибирский государственный технический университет, 2018. – 79 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book_red&id=575325 (дата обращения: 04.03.2025).
5. *Скрыпников А.В., Денисенко В.В., Арапов Д.В., Герасимова Т.Д.* Защита Web-приложений – Воронеж: Воронежский государственный университет инженерных технологий, 2020. – 77 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book_red&id=612405 (дата обращения: 04.03.2025).
6. *Белоус А.И., Солодуха В.А.* Основы кибербезопасности: стандарты, концепции, методы и средства обеспечения: научно-популярное издание. – М.: Техносфера, 2021. – 482 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book_red&id=617523 (дата обращения: 04.03.2025).
7. *Хаулет Т.* Защитные средства с открытыми исходными текстами: Практическое руководство по защитным приложениям: учебное пособие – М.: Интернет-Университет Информационных Технооологий (ИНТУИТ), 2007. – 608 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book_red&id=233306 (дата обращения: 04.03.2025).
8. *Вострецова Е.В.* Основы информационной безопасности: учебное пособие – Екатеринбург: Изд-во Уральского Университета, 2019. – 207 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book_red&id=697636 (дата обращения: 04.03.2025).

УДК 004.056.55

Д.А. Панченко, Е.А. Ищукова

Южный федеральный университет, Россия, г. Таганрог

ИССЛЕДОВАНИЕ ПРОТОКОЛА BULLETPROOFS И АУДИТА БЕЗОПАСНОСТИ, ВЫПОЛНЕННОГО КОМПАНИЕЙ QUARKSLAB

Все большее распространение получают электронные платежи, которые используются во многих сферах деятельности. И на ровне с ними большую популярность получили криптовалюты. На начальном этапе создания криптовалюты задумывались как средство, представляющее анонимность платежей. Но с их большим распространением стало ясно, что это не совсем так. В связи с чем стали появляться анонимные криптовалюты, которые использую доказательство с нулевым разглашением (ZKP). Так как с помощью данного протокола можно обеспечить полную анонимность платежей. Таким образом возросла популярность протоколов и систем доказательства, использующих технологию доказательство с нулевым разглашением. Поэтому стало появляться все больше систем доказательства таких как Groth16, Plonk и другие. При этом возникает проблема безопасности реализации данных систем и протоколов. В этой области ведутся активные исследования и регулярно публикуются статьи о найденных уязвимостях. Так как данные протоколы использую сложные криптографические механизмы, то задача их верификации очень сложно. Поэтому при использовании формальных средств верификации таких как Tamarin Prover или Scyther не всегда можно найти уязвимости и слабости протокола. Именно поэтому верификации исходного кода конкретной реализации может помочь при проверке протокола. Так как с помощью этого можно найти больше уязвимостей и слабых мест. В данный работе будут представлен пример такого исследования. На пример прокола Bulletproofs. Компанией Quarkslab был проведен аудит безопасности данного протокола, в котором было обнаружено несколько уязвимостей. Таким образом на данном примере видно на сколько важна верификация исходного кода реализации протокола.

Ключевые слова: *криптовалюта, доказательство с нулевым разглашением, ZKP, Bulletproofs, zkSNARK, zkSTARK, Monero, Quarkslab.*

Electronic payments are becoming more and more widespread and are used in many areas of activity. And cryptocurrencies have also become very popular. At the initial stage of their creation, cryptocurrencies were conceived as a means of representing the anonymity of payments. But with their widespread use, it became clear that this is not entirely true. In connection with this, anonymous cryptocurrencies began to appear that use zero-knowledge proof (ZKP). Since this protocol can ensure complete anonymity of payments. Thus, the popularity of protocols and proof systems using zero-knowledge proof technology has increased. Therefore, more and more proof systems such as Groth16, Plonk and

others began to appear. At the same time, the problem of security of the implementation of these systems and protocols arises. Active research is being conducted in this area and articles on the vulnerabilities found are regularly published. Since these protocols use complex cryptographic mechanisms, the task of their verification is very difficult. Therefore, when using formal verification tools such as Tamarin Prover or Scyther, it is not always possible to find vulnerabilities and weaknesses of the protocol. That is why verification of the source code of a specific implementation can help when checking the protocol. Since with this you can find more vulnerabilities and weaknesses. This paper will present an example of such a study. For example, the Bulletproofs puncture. Quarkslab conducted a security audit of this protocol, in which several vulnerabilities were found. Thus, this example shows how important it is to verify the source code of the protocol implementation.

Keywords: *cryptocurrency, zero-knowledge proof, ZKP, Bulletproofs, zkSNARK, zkSTARK, Monero, Quarkslab.*

Введение

С течением времени всё большее развитие получает информационные технологии. И тем больше людей пользуются ими в различных сферах. На текущий момент система электронных платежей, которая часто используется в повседневной жизни, является одним из перспективных направлений развития информационных технологий. Поэтому для неё требуется надежная информационная безопасность [1].

Криптовалюты обрели популярность на ровне с системой электронных платежей. Поэтому также требуют надежной защиты. В связи с чем возросла популярность протоколов доказательства с нулевым разглашением [2], так как они активно использовались в криптовалютах, например Zcash, для обеспечения анонимности. Так же данные протоколы можно использовать и для аутентификации в веб-приложениях [3]. Это говорит о том, что данные протоколы являются перспективным направлением развития криптографии [4].

В связи с чем всё острее становится проблема безопасности реализации систем доказательства, которые использую протоколы доказательства с нулевым разглашением. Так как данные протоколы использую различные криптографические механизмы, то поиск уязвимостей в них не является простой задачей. А проблема верификации данных протоколов остаются актуальной.

Так как большинство средств верификации производят анализ протоколов в абстрактном виде, то это не позволяет проверить протокол полностью. А также при его реализации возникают дополнительные уязвимости, связанные с конкретным языком программирования. Таким образом верификация прокола по исходного коду является более актуальной чем с помощью средств формальной верификации [5].

Таким образом проблема верификации протоколов доказательства с нулевым разглашением является актуальной на данный момент. И в данной работе будет рассмотрен протокол Bulletproofs и его аудит безопасности,

выполненный Quarkslab, в котором был исследован исходный код протокола. На примере, которого становится ясно что верификация исходного кода протокола, может быть полезна и даёт полный список уязвимостей и недочетов, которые могут быть допущены в реализации протокола.

Описание протокола Bulletproofs

В декабре 2017 года группой прикладной криптографии Стэнфорда был предложен новый протокол Bulletproofs, который может убедить проверяющего, что секрет находится в указанном диапазоне [6]. На рис. 1 показано математическое представление протокола Bulletproofs.

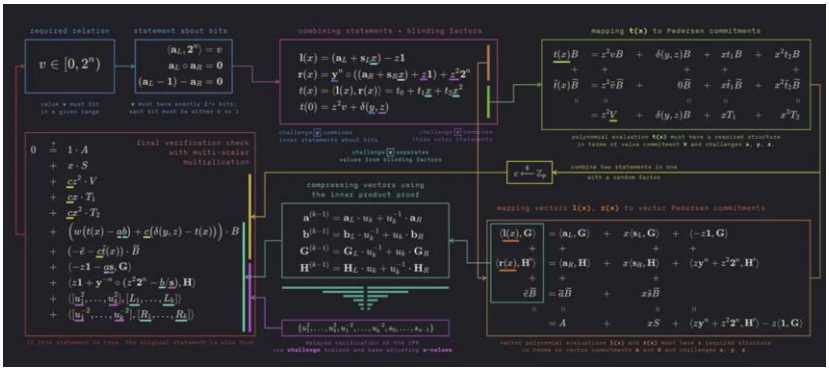


Рис. 1. Математическое представление протокола Bulletproofs [7]

Bulletproofs – это короткие, неинтерактивные доказательства с нулевым разглашением, которые не требуют доверенной настройки. По своей сути это доказательство диапазона, который использует методы доказательства с нулевым разглашением. Он схож с zkSNARK и zkSTARK. Но в отличии от zkSNARK:

- Не использует доверенную настройку, так как использует математические принципы для сокрытия входных данных.
- Не использует пары и работает с любой эллиптической кривой с достаточно большим размером подгруппы.
- Поддерживает самые быстрые эллиптические кривые, такие как Ristretto.
- Использует собственный формат для вычислений, который легко преобразуется в R1CS и обратно с помощью линейной алгебры; [8]

В отличии от zkSTARK он имеет меньший вес доказательства, что позволяет объединять несколько доказательство в одно без большого роста веса самого доказательства. Но Bulletproofs требуют больше времени для проверки, чем доказательство zkSNARK и zkSTARK. Подробное сравнение этих протоколов показано на рис. 2.

	SNARKs	STARKs	Bulletproofs
Algorithmic complexity: prover	O(N * log(N))	O(N * poly-log(N))	O(N * log(N))
Algorithmic complexity: verifier	~O(1)	O(poly-log(N))	O(N)
Communication complexity (proof size)	~O(1)	O(poly-log(N))	O(log(N))
- size estimate for 1 TX	Tx: 200 bytes, Key: 50 MB	45 kB	1.5 kb
- size estimate for 10.000 TX	Tx: 200 bytes, Key: 500 GB	135 kb	2.5 kb
Ethereum/EVM verification gas cost	~600k (Groth16)	~2.5M (estimate, no impl.)	N/A
Trusted setup required?	YES 😒	NO 😄	NO 😄
Post-quantum secure	NO 😒	YES 😄	NO 😒
Crypto assumptions	DLP + secure bilinear pairing 😒	Collision resistant hashes 😄	Discrete log 😉

Рис. 2. Сравнение zk протоколов [9]

Bulletproofs являются как безопасными, так и неинтерактивными, и достигается этого с помощью проблемы дискретного логарифмирования и эвристики Фиата-Шамира.

Одним из примером использования Bulletproofs, является криптовалюта Monero. Первоначально в ней использовались подписи Шнорра и кольцевые подписи Борромео. После перехода на Bulletproofs размеры транзакций и комиссии были сокращены на 80% [10].

Верификация протокола Quarkslab

Quarkslab – это французская компания, специализирующаяся на кибербезопасности и разработке инновационных технологий для обеспечения информационной безопасности. Она была основана в 2011 году и с тех пор стала довольно известной благодаря своим продуктам и услугам в области киберзащиты. Основная область деятельности Quarkslab включает в себя анализ уязвимостей, исследование безопасности программного обеспечения, а также разработку инструментов и решений для обеспечения безопасности информационных систем [11].

В январе 2018 года Monero Research Lab через Open Source Technology Improvement Fund запросила у Quarkslab описание работы, в котором подробно описывались бы шаги оценки безопасности. Основной целью в криптовалюте с открытым исходным кодом Monero (XMR) была реализация нового криптографического доказательства: Bulletproof.

Их мотивацией для перехода от доказательств Борромео к доказательствам «пуленепробиваемости» является размер доказательства, поскольку это значительно сократит размер транзакций, тем самым снизив комиссии за транзакции на платформе примерно на 70–80%.

В ходе оценки безопасности реализации Bulletproof были обнаружены несколько уязвимостей. Четыре основные уязвимости могут быть вызваны ненадежными входными данными для функции проверки доказательств. Помимо возможности создания неверных выходных значений, они могут быть первыми шагами к тому, чтобы заставить верификатор принять ложное доказательство:

- Арифметическое переполнение в функции двойного скалярного умножения, которая используется либо для вычисления доказательства, либо для проверки доказательства с входными данными, находящимися под прямым контролем доказывающей стороны.
- Две алгоритмические ошибки в одной версии функции мультиэкспонентации (Bos-Coster и Pippenger), которая используется при проверке доказательства, позволяя либо ошибочно выводить точку идентичности, либо молча отбрасывать элемент в вычислении. Входные данные для этих функций напрямую выводятся из входных данных злоумышленника, хотя и не прямолинейным образом.
- Отсутствие надлежащих проверок безопасности на входах основной функции проверки доказательств, хотя все эти входы контролируются потенциальным злоумышленником. Это отсутствие проверок делает три предыдущие уязвимости еще более критическими, поскольку они напрямую подвержены некорректным входам (неприведенные скаляры, точки либо не на кривой, либо не в основной подгруппе кривой).

Также были обнаружены три уязвимости среднего уровня в процедурах десериализации (включая неправильную проверку размера). Поскольку десериализация происходит на ненадежных входных данных под контролем злоумышленника, ошибки могут привести как минимум к исключениям и потенциальным отказам в обслуживании.

Также сообщалось о двух ошибках, которые соответствуют крайне маловероятным событиям, вызванным внутренними вычислениями некоторых криптографических функций. Хотя эти события вряд ли произойдут случайно, никто не может предсказать все будущие приложения и контексты использования этих фрагментов кода, и что эти значения не могут быть обработаны точнее, чем случайно в некоторых случаях использования. Добавление соответствующих проверок для реализации предполагаемой семантики и достижения большей надежности кода определенно рекомендуется.

Значения хешируются до нуля для создания проблем в протоколе: проблемы с нулевым значением подрывают безопасность протокола, кроме того, их нельзя инвертировать, так как для некоторых из них это требуется протоколом.

Нулевое случайное значение, заданное в качестве входных данных для подписи Шнорра, приводит к компрометации закрытого ключа. Если значение хэша равно нулю, то подпись не зависит от закрытого ключа.

За время оценки ни одна из обнаруженных уязвимостей не привела к практическому использованию, позволяющему либо создать ложное доказательство, принятое проверяющим, либо раскрыть информацию о доказательстве [12].

Заключение

Хоть найденные уязвимости и не привели к практическому использованию, это не означает, что это невозможно. Так как найденные слабые стороны, могут превратиться в уязвимости во время эволюции кода. Таким образом верификации исходного кода протокола показывает те уязвимости, которые присущи конкретной реализации. Это позволяет найти даже самые мелкие уязвимости. Исходя из этого можно сделать вывод, что для нахождения всех уязвимостей необходимо выполнять верификацию исходного кода протокола.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Калмыков И.А., Саркисов А.Б., Макарова А.В., Калмыков М.И.* Расширение методов защиты систем электронной коммерции на основе модулярных алгебраических схем // Известия ЮФУ. Технические науки. – 2014. – № 2 (151). – С. 218-225.
2. *Юрцев А.Н.* Доказательства с нулевым разглашением // Международный журнал гуманитарных и естественных наук. – 2023. – № 4-4 (79). – С. 138-141
3. *Сиганов И.Д.* Доказательство с нулевым разглашением как метод аутентификации в веб-приложениях // Математические структуры и моделирование. – 2016. – № 4 (40). – С. 143-150ю
4. *Мурзагалиев А.Р.* Перспективные направления развития криптографии // Скиф. Вопросы студенческой науки. – 2022. – № 5 (69). – С. 302-306.
5. *Бабенко Л.К., Писарев И.А.* Верификация безопасности криптографических протоколов по исходным кодам системы электронного голосования с применением множественного бросания бюллетеней // Известия ЮФУ. Технические науки. – 2019. – № 5 (207). – С. 46-57.
6. Bulletproofs: Short Proofs for Confidential Transactions and More. – URL: https://eprint.iacr.org/2017/1066 (дата обращения: 10.11.2024).
7. Building on Bulletproofs. – URL: https://cathieyun.medium.com/building-on-bulletproofs-2faa58af0ba8?ref=blog.pantherprotocol.io (дата обращения: 21.02.2025).

8. Bulletproofs. – URL: https://sikoba.com/docs/SKOR_DK_Bulletproofs_201905.pdf (дата обращения: 15.11.2024).
9. Awesome zero knowledge proofs (zkp). – URL: https://github.com/matter-labs/awesome-zero-knowledge-proofs?ref=blog.pantherprotocol.io (дата обращения: 22.02.2025).
10. Bulletproofs In Crypto – An introduction to a Non-Interactive ZKP. – URL: https://blog.pantherprotocol.io/bulletproofs-in-crypto-an-introduction-to-a-non-interactive-zk-proof/ (дата обращения: 20.02.2025).
11. Quarkslab. – URL: https://www.securitylab.ru/glossary/quarkslab/ (дата обращения: 15.02.2025).
12. Security Audit of Monero Bulletproofs. – URL: https://blog.quarkslab.com/security-audit-of-monero-bulletproofs.html (дата обращения: 12.02.2025).

УДК 00.1082

В.А. Реброва

Южный федеральный университет, Россия, г. Таганрог

КОМПЛЕКС МЕР ПО ПРОТИВОДЕЙСТВИЮ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В КОМПАНИЯХ

Работа посвящена актуальной проблеме – противодействию социальной инженерии в компаниях. Информация – один из наиболее ценных ресурсов любой организации. Уязвимым звеном в её потере является человек, которым можно управлять и манипулировать. В данной статье рассматриваются основные методы и приёмы социальной инженерии, анализируются причины её успешности и предлагаются эффективные меры по предотвращению атак. Реализация предложенных мер поможет значительно снизить риски, связанные с социальной инженерией, и повысить уровень защищённости информации в компаниях.

Ключевые слова: *социальная инженерия, злоумышленник, киберпреступление, атака, человеческий фактор.*

The work is devoted to an urgent problem – countering social engineering in companies. Information is one of the most valuable resources of any organization. A vulnerable link in her loss is a person who can be controlled and manipulated. This article discusses the main methods and techniques of social engineering, analyzes the reasons for its success, and suggests effective measures to prevent attacks. The implementation of the proposed measures will help significantly reduce the risks associated with social engineering and increase the level of information security in companies.

Keywords: *social engineering, attacker, cybercrime, attack, human factor.*

Введение

В эпоху цифровых технологий информация стала одним из наиболее ценных ресурсов для любого предприятия. Она служит фундаментом для принятия обоснованных решений и даёт организации преимущество перед конкурентами. Тем не менее информация уязвима перед лицом угроз, которые могут привести к её утрате, искажению или неправомерному использованию.

Одной из таких угроз является социальная инженерия – метод психологического воздействия на человека с целью получения конфиденциальных данных или побуждения его к нежелательным действиям. В наше время специалисты по кибербезопасности непрерывно работают над созданием современных и надёжных систем защиты данных. Однако, несмотря на все усилия, полностью обезопасить систему невозможно, поскольку любая система уязвима. Технологии имеют свои ограничения, и чаще всего злоумышленник выигрывает именно за счёт человеческого фактора [1].

Проведение атаки с использованием социального инжиниринга

Компьютерная система не существует сама по себе. Многие забывают, что главный инструмент взлома любой системы – это сам человек. Социальная инженерия использует человеческую психологию для доступа к информации или системам.

Цель социальной инженерии – получение конфиденциальных данных, личных сведений и паролей для доступа к системе. Киберпреступников также интересуют коммерческая тайна и информация о банковских операциях. С помощью социальной инженерии злоумышленники могут длительное время манипулировать жертвой и использовать её в своих целях. Жертвой может стать любой человек, независимо от его социального статуса и места работы.

Способы социальной инженерии разнообразны и представляют собой заранее подготовленные действия, нацеленные на конкретных людей и имеющие определённые цели. Это может привести к разнообразным негативным последствиям:

1. Компрометации информации: если конфиденциальные сведения попадут в руки третьей стороны, компанию ждут высокие финансовые и репутационные риски. Могут быть раскрыты коммерческая тайна и внутренние разработки.

2. Нарушении доступности и целостности информации: преступники могут уничтожить или модифицировать данные, находящиеся в базах, что сделает их непригодными для использования владельцем.

3. Нецелевое использование информации: полученная конфиденциальная информация может быть использована для осуществления мошеннических схем, которые приведут к финансовым и репутационным потерям компании. Основная цель социальных инженеров – это получение доступа к защищенным системам с целью кражи конфиденциальной информации, таких как, пароли, данные о кредитных картах, личные данные пользователя.

Атака социального инженера разделяется на три стадии подготовки:

1. Четкое определение цели (устанавливается, какая именно информация необходима, где она находится и каким способом её можно получить).
2. Сбор данных об объекте (изучается жертва с целью выявления уязвимостей. Источниками информации могут быть различные данные, включая анализ трафика, переписки и другие сведения).
3. Планирование действий и психологическая подготовка (разрабатывается сценарий совершения преступления и проводится моральная настройка).

Все атаки хакеров данной области формируются в несколько этапов:

Первым этапом является формирование цели воздействия на тот или иной объект (жертву). Затем собирается информация об объекте, с целью обнаружения уязвимых мест, которые можно использовать при атаке. Злоумышленник создаёт нужные условия для воздействия на объект. После того, как достигнута аттракция, жертва сама совершает нужные действия [3].

В производстве человек может столкнуться с двумя видами инжиниринга: краткосрочным и долговременным. Под «краткосрочным» понимается совершение воздействия на жертву за короткий промежуток времени. Однако этому есть противопоставление – злоумышленник не может выполнить значительные действия на человека, требующие больше времени, как, например, это показано в следующем примере. При «долговременном» влиянии требуется больше временных ресурсов, чтобы подчинить жертву. Плюсом такого воздействия является совершение более значительных действий человеком.

Киберпреступники используют различные психологические инструменты воздействия на человека, это могут выступать страх, жадность, надежда и другие эмоции для повышения эффективности своих атак. Поэтому хакеры, например, при рассылке фишинговых писем в теме для письма используют специальные фразы, по типу «список сотрудников на увольнение», «выплаты премий за год» и т. п. При получении таких сообщений люди часто начинают поддаваться эмоциям, теряться и забывают об элементарных правилах безопасности [4].

Рассмотрим основные мотивы совершения преступления в сфере компьютерной информации посредством социального инжиниринга:

1. Финансовая выгода.
2. Манипуляции и контроль.
3. Получение доступа к коде конфиденциальным данным.
4. Преследование корыстных целей.

Проблема социальной инженерии является серьезной на сегодняшний день. Каждый человек подвержен манипуляции и воздействию, поэтому в ближайшее время главную угрозу для безопасности будет представлять социальный инжиниринг по сравнению с использованием других методов атак.

Рассмотрим основные виды атак, применяемые хакерами при воздействии на человека.

Распространенная цель социальной инженерии – перехват учетных данных пользователя в процессе так называемого фишинга. **Фишинг** – рассылка электронных писем или сообщений с поддельными ссылками на сайты, внешне похожие на официальные, чтобы обманом заставить пользователя ввести свои данные, такие как логины и пароли. Фишинговые сообщения электронной почты или веб-сайты пытаются обмануть пользователя и заставить его указать свои реальные учетные данные для авторизации, ими-

тируя легитимный веб-сайт или администратора-отправителя, с которым конечный пользователь знаком. Наиболее распространенная фишинговая атака – это электронное письмо якобы от администратора сайта, утверждающего, что учетные данные пользователя должны быть проверены, иначе доступ к сайту будет прекращен [5].

Целевой фишинг – это тип фишинга, который нацелен против конкретного человека или группы людей с применением непубличной информации, которой владеет цель атаки. Например, отправка сотрудникам документа по электронной почте якобы от участника проекта: при его открытии файл выполняет вредоносные команды.

Другой распространенный метод социальной инженерии – «Троянский конь». Он направлен на то, чтобы обманным путем заставить пользователя запустить вредоносную программу. Такой код может распространяться через электронную почту в виде вложений или ссылок для скачивания. Кроме того, вредоносные файлы нередко размещаются на веб-сайтах.

Злоумышленники могут взломать легитимные ресурсы, чтобы под видом важных обновлений, антивирусных программ или необходимых плагинов побудить пользователя загрузить и запустить вредоносное ПО. В некоторых случаях компрометации подвергается не сам сайт, а его отдельные элементы, например, рекламные баннеры. Пользователи, которые доверяют ресурсу и посещают его на протяжении многих лет, зачастую не подозревают о возможной угрозе. Однако использование электронной почты далеко не единственный инструмент социальной инженерии [6].

Мошенники также звонят пользователям, которым может понадобиться техническая поддержка, от имени популярного разработчика, из государственного учреждения или компании. **Вишинг** (телефонный фишинг) – мошенники звонят по телефону, представляясь другим лицом, чтобы обманом получить конфиденциальную информацию или вымогать деньги. Кроме того, сюда можно отнести и **смишинг** (SMS-фишинг) – мошеннические SMS-сообщения, в которых содержатся фальшивые ссылки или просьбы о переводе денег.

Одна из самых популярных афер по телефону – когда мошенник звонит якобы от лица техподдержки, утверждая, что на компьютере пользователя была обнаружена вредоносная программа. Затем он просит загрузить «антивирусную» программу, которая, что неудивительно, обнаруживает множество вредоносных объектов. Мошенник побуждает загрузить и выполнить программу удаленного доступа, которую затем использует для авторизации на компьютере жертвы, чтобы внедрить другое вредоносное ПО [7].

Претекстинг – атака, при которой злоумышленник выдумывает историю (претекст), чтобы завоевать доверие жертвы и заставить её раскрыть информацию. Например, он может представиться коллегой, сотрудником компании или даже другом жертвы. Бейтинг – использование заманчивых

"ловушек", чтобы вызвать интерес и заставить человека совершить действие. Например, сотрудник компании находит флешку с наклейкой «Конфиденциальные данные» или «Зарплатная ведомость». Из любопытства он подключает ее к рабочему компьютеру, чтобы узнать, что на ней находится. В этот момент на его устройство устанавливается вредоносное ПО, которое дает злоумышленнику доступ к корпоративной сети.

Пользователей следует научить никогда не устанавливать какое-либо программное обеспечение непосредственно с сайта, который они посещают, если это не сайт легитимного разработчика ПО. Если веб-сайт сообщает, что вам нужно установить какое-то программное обеспечение, чтобы продолжить просмотр ресурса, и вы думаете, что это законный запрос, покиньте его и перейдите на сайт разработчика стороннего программного обеспечения, чтобы наверняка установить корректное приложение. Не стоит устанавливать ПО с чужого веб-сайта, а не с сайта непосредственного разработчика.

В 2022 г. киберпреступники стали активно использовать модель, которая в том числе включает в себя обход многофакторной аутентификации – управление доступом, который требует от пользователей подтверждения их данных посредством использования двух различных факторов проверки. При совершении большого количества попыток войти в аккаунт при помощи полученных злоумышленником данных, это вызывает бесконечный поток уведомлений у пользователя. Дабы остановить рассылку некоторые пользователи подтверждают вход, тем самым дав зелёный свет преступнику.

Одним из самых ярких и дерзких ограблений с использованием социальной инженерии считается ограбление банка в Бангладеш в феврале 2016 года. С помощью инсайдеров хакеры произвели рассылку фишинговых электронных писем, содержащие зараженные вредоносным ПО файлы. Когда жертвы открывали эти вложения, они предоставили хакерам доступ к сети и системам банка.

Оказавшись внутри, злоумышленники воспользовались внутренними процессами и механизмами контроля, чтобы манипулировать банковской системой SWIFT — сетью обмена сообщениями, которую финансовые учреждения используют для безопасного отправления и получения платежей. Хакеры попытались перевести почти 1 млрд. долларов из Банка Бангладеш на свои счета. Однако некоторые транзакции не сработали, и хакерам удалось перевести лишь часть украденных денег.

Меры защиты от социальной инженерии

Обучение противостоянию социальной инженерии – одно из лучших, наиболее важных средств защиты. Обучение должно включать примеры наиболее распространенных видов социальной инженерии. Однако в некоторых компаниях заведомо проводятся фишинговые атаки, в ходе которых работникам отправляются поддельные электронные письма. Сотрудники, попавшиеся на данные уловки, проходят дополнительное обучение.

К некоторым мерам защиты можно отнести:

Тестирование на возможные атаки. Специалистам IT-отделов компаний или организаций зачастую рекомендуется проводить проверку на возможные атаки с использованием социальной инженерии [8]. Суть теста заключается в искусственно созданной атаке на компьютерную систему или пользователей для проверки на наличие возможных уязвимостей. Кроме того, это позволяет определить степень возможного ущерба. Тест на проникновение — это искусственно смоделированная кибератака на компьютерную систему или определённых пользователей для проверки наличия уязвимостей. Такие периодические тесты полезны тем, что позволяют определить готовность пользователей, и оценить возможные масштабы утечки данных. Проводить имитацию фишинговых тестов можно с использованием специальных программ. В ходе тестов сотрудникам рассылают фишинговые электронные письма и выясняют, кто попадается на тактики социальной инженерии. Затем эти сотрудники могут пройти переподготовку.

Многофакторная аутентификация. Такой метод включает в себя два различные виды подтверждения личности: например, пароль, код на телефон или использования токена. Это один из наиболее эффективных методов противодействия атакам по технологиям социальной инженерии.

Использование защиты от вредоносных программ. Такая защита должна быть комплексной и включать антивирусное ПО для веб-сёрфинга, почтовый антивирус и антишпионское ПО. Некоторые компании предоставляют пакетную защиту, но можно использовать и несколько хороших приложений от разных разработчиков. Одной из наиболее важных задач такой защиты является предотвращение опасностей при нажатии пользователем на ссылки из писем и в мессенджерах. Таким образом, если пользователь нажимает на ссылку (в браузере, электронной почте или мессенджере) и, если веб-страница является подозрительной с точки зрения сетевых угроз, защита должна предотвращать загрузку страницы с вредоносным контентом и блокировать её.

Регулярные обновления операционной системы. Операционные системы на всех компьютерах организации должны оперативно обновляться, поскольку разработчики часто выпускают фиксы для устранения замеченных уязвимостей.

Правильный подбор и периодическая смена пароля. В качестве эффективной превентивной меры организациям следует применять строгие политики управления паролями. Сотрудники должны быть обязаны периодически менять свои пароли и, что не менее важно, правильно составлять их. Лучший вариант здесь: случайно сгенерированные сложные пароли, подобрать которые практически невозможно. Разумеется, нужно обучить сотрудников и правильному хранению таких паролей.

Использование брандмауэра. Хороший сетевой файрволл (WAF) блокирует вредоносные запросы, которые также могут включать и атаки с использованием социальной инженерии. Таким образом, прежде чем посетители попадают на ваш сайт, они фильтруются WAF, который определяет, является ли подключение безопасным, и блокирует подключение, если оно похоже на мошенническую атаку.

Социальная инженерия – одна из главных опасностей для информационной безопасности. Чтобы эффективно защититься от неё, нужно применять разнообразные меры защиты, быть бдительным и постоянно обновлять свои знания в области кибербезопасности. Важно осознавать, что основная цель социальной инженерии – получение доступа к конфиденциальной информации.

Применение нейросетевых технологий в борьбе с атаками социальной инженерии

В современных условиях нейросетевые технологии становятся важным инструментом в противодействии таким угрозам. Рассмотрим основные методы использования современных ИИ-систем на примере по борьбе с социальной инженерией.

Распознавание фишинговых атак с помощью NLP

Нейросети, основанные на **Natural Language Processing (NLP),** могут анализировать тексты электронных писем, SMS и сообщений в мессенджерах. Они выявляют признаки фишинга, такие как аномальные грамматические конструкции или призывы к срочным действиям.

Кроме того, нейросети могут проверять доменные имена отправителей на соответствие известным угрозам, например, использование похожих символов, определение подозрительного IP-адреса отправителя и сравнение его с базами данных угроз.

Алгоритмы **Computer Vision** анализируют страницы сайтов и сравнивают их с оригинальными ресурсами. Нейросети выявляют визуальные несовпадения, например отличия в логотипах, цветах, шрифтах [9]**.**

Киберзащита и анализ поведения пользователей

Системы поведенческого анализа **(User Behavior Analytics)** отслеживают привычки пользователей и выявляют аномальное поведение. Например, если сотрудник внезапно начал загружать большие объемы данных в нерабочее время, система может запустить дополнительную проверку. Нейросети способны распознавать манеру набора текста или движения мыши для определения аномалий.

Еще одним не мало важным способом в борьбе с социальной инженерией является применение чат-ботов и обучающих систем для сотрудников компании**.** Они могут обучать пользователей распознавать атаки социаль-

ной инженерии, проводя тестирования и симуляции. В организациях такие боты могут оперативно предупреждать сотрудников о возможных атаках. Нейросети могут анализировать уровень осведомленности каждого пользователя и адаптировать программу обучения. Это повышает эффективность защиты от атак социальной инженерии, так как учитываются индивидуальные слабые места.

Нейросетевые технологии значительно повышают уровень защиты от социальной инженерии, автоматизируя выявление мошеннических схем, анализируя поведение пользователей и повышая осведомленность людей о возможных угрозах. Однако развитие методов атак также не стоит на месте, поэтому требуется постоянное совершенствование ИИ-систем кибербезопасности.

Заключение

В ходе проведенного анализа причин возникновения социальной инженерии, было выявлено, что данная проблема представляет собой серьезную угрозу для безопасности компаний, поскольку используется человеческий фактор. Технические методы не могут обеспечить полную защиту от таких атак. Для эффективного противодействия этой угрозе необходим комплексный подход, который включает как технические, так и организационные меры. Обучение сотрудников, внедрение системы многоуровневой аутентификации, фильтрация фишинговых сообщений, ограничение доступа и другие меры помогают существенно снизить риски от атак социальной инженерии и защитить данные компании от утечек.

При обеспечении информационной безопасности компьютеров и других устройств, часто упускается из виду угроза, исходящие от людей. Социальный инжиниринг не заменяет защиту от хакерских атак, но она помогает бороться с действиями злоумышленников, использующих обман и злоупотребление доверием людей для достижения своих целей. Однако, сотрудники организации, предприятия, а также обычные граждане должны быть осведомлены о методах социального инжиниринга и уметь распознавать и предотвращать соответствующие атаки.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Роджер Граймс.* Как противостоять хакерским атакам? Уроки экспертов по информационной безопасности: пер. с англ. М.А. Райтман. – М.: Эксмо, 2023. –368 с.
2. *Созаев С.С., Кунашев Д.А.* Социальная инженерия, ее техники и методы ее противодействия [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-ee-tehniki-i-metody-ee-protivodeystviya/viewer.

3. *Гаврилов А.* Социальный инжиниринг в действии // Безопасность. – 2012. – № 3. – С. 118-122.
4. *Никитин Е.В.* Проблемы противодействия технологиям социальной инженерии как элементу преступной деятельности [Электронный ресурс]. – URL: https://cyberleninka.ru/article/n/problemy-protivodeystviya-tehnologiyam-sotsialnoy-inzhenerii-kak-elementu-prestupnoy-deyatelnosti/viewer.
5. *Хлестова Д.Р., Байрушин Ф.Т.* Социальная инженерия – одна из наиболее опасных угроз ИБ предприятий [Электронный ресурс]. – URL: https://cyberleninka.ru/ article/n/sotsialnaya-inzheneriya-odna-iz-naibolee-opasnyh-ugroz-ib-predpriyatiy/viewer.
6. *Прокофьев И.В.* Введение в теоретические основы компьютерной безопасности: учебное пособие. – М.: МИФИ, 2008. – 287 с.
7. *Кузнецов М.В., Симдянов М.В.* Социальные инженеры и социальные хакеры. – СПб.: БХВ-Петербург, 2007. – 368 с.
8. *Касперски К.* Секретное оружие социальной инженерии // Журнал сетевых решений. – 2012. – № 9. – С. 12-15.
9. *Петровичев Е.И.* Нейросетевая технология в системах искусственного интеллекта // Текст научной статьи по специальности «Компьютерные и информационные науки». – 2008. – С. 134-145.

УДК 004.056

Р.А. Рузин

Южный федеральный университет, Россия, г. Таганрог

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СВЯЗИ И ПЕРЕДАЧИ ДАННЫХ БАС

Цель работы – провести анализ существующих методов защиты беспроводных каналов связи беспилотных авиационных систем (БАС), выявить их уязвимости и рассмотреть подходов к повышению устойчивости систем передачи данных к потенциальным угрозам, таким как перехват сигналов, глушение (jamming), атакам типа Man-in-the-Middle и эксплуатации уязвимостей беспроводных протоколов. В работе проведён сравнительный анализ методов обеспечения безопасности связи, включая шифрование данных, резервирование каналов и применение адаптивных протоколов связи. Особое внимание уделено использованию инструментов тестирования защищённости беспроводных систем, таких как HackRF, GNU Radio и SDRangel. Рассмотрены их возможности для анализа устойчивости каналов связи, моделирования атак и выявления уязвимостей. Проведённое исследование показало, что комплексный подход, включающий сочетание современных криптографических технологий, динамического управления частотным спектром и мониторинга угроз, позволяет значительно повысить надёжность каналов связи БАС. Использование специализированных инструментов для тестирования безопасности является эффективным методом выявления потенциальных уязвимостей и разработки мер по их устранению, что способствует повышению общей устойчивости систем связи беспилотных авиационных комплексов.

Ключевые слова: *беспилотные авиационные системы, безопасность связи, защита данных, шифрование, глушение сигнала, атаки Man-in-the-Middle, SDR, HackRF, GNU Radio, SDRangel, киберугрозы, радиочастотная защита.*

The objective of this study is to analyze existing methods for protecting wireless communication channels in unmanned aerial systems (UAS), identify their vulnerabilities, and examine approaches to enhancing the resilience of data transmission systems against potential threats such as signal interception, jamming, Man-in-the-Middle attacks, and the exploitation of wireless protocol vulnerabilities.The study provides a comparative analysis of security measures, including data encryption, channel redundancy, and the use of adaptive communication protocols. Special attention is given to security testing tools such as HackRF, GNU Radio, and SDRangel. Their capabilities in analyzing communication channel resilience, simulating attacks, and identifying vulnerabilities are examined. The research findings indicate that a comprehensive approach combining modern cryptographic technologies, dynamic frequency spectrum management, and threat monitoring significantly enhances the reliability of UAS communication channels. The use of special-

ized security testing tools proves to be an effective method for identifying potential vulnerabilities and developing mitigation measures, thereby improving the overall resilience of UAS communication systems.

Keywords: *unmanned aerial systems, communication security, data protection, encryption, signal jamming, Man-in-the-Middle attacks, SDR, HackRF, GNU Radio, SDRangel, cyber threats, radio frequency protection.*

Введение

Безопасность связи и передачи данных в беспилотных авиационных системах является одной из ключевых задач, обеспечивающих их эффективное функционирование. Надежность каналов связи критически важно для устойчивого управления, своевременного обмена информацией и защиты от несанкционированного доступа. В современных условиях БАС сталкиваются с различными угрозами, включая кибератаки, радиопомехи и уязвимости в системах передачи данных. В связи с этим особую актуальность приобретает применение современных методов и технологий защиты информации, направленных на минимизацию возможных рисков и повышение общей надежности функционирования беспилотных систем.

Угрозы безопасности связи в БАС

Одной из ключевых проблем безопасности связи в беспилотных авиационных системах является угроза перехвата и подмены сигналов. Злоумышленники могут попытаться получить несанкционированный доступ к управляющим командам, что способно привести к утрате контроля над БАС и их неправильному функционированию. Кроме того, существует риск глушения (jamming) и подавления связи, при котором намеренно создаются мощные радиопомехи, блокирующие передачу данных между оператором и беспилотной системой. Такой вид атаки может не только препятствовать выполнению поставленных задач, но и полностью вывести аппарат из строя.

Еще одной серьезной угрозой являются атаки типа «человек посередине» (Man-in-the-Middle, MitM), при которых злоумышленник перехватывает обмен данными между оператором и БАС, изменяя или подменяя передаваемую информацию. Это может привести к искажению телеметрических данных, ложным командам или утечке конфиденциальной информации. Также необходимо учитывать уязвимости беспроводных протоколов, используемых для связи, поскольку многие из них подвержены атакам на уровне шифрования или аутентификации. Недостаточная защита каналов передачи данных может сделать БАС уязвимыми к взлому, что ставит под угрозу их безопасную эксплуатацию [1].

Протоколы и технологии защиты связи в БАС

Одним из основных методов обеспечения безопасности связи в беспилотных авиационных системах является использование защищённых каналов передачи данных. Для предотвращения несанкционированного доступа широко применяются криптографические алгоритмы, такие как AES-256, обеспечивающие высокий уровень защиты информации. Шифрование данных позволяет минимизировать риск перехвата и подмены передаваемых команд и телеметрической информации. Дополнительно для повышения безопасности могут использоваться виртуальные частные сети (VPN), создающие зашифрованные туннели передачи данных. Важную роль также играют специализированные протоколы, такие как DTLS (Datagram Transport Layer Security), обеспечивающие аутентификацию и целостность данных при их передаче.

Для повышения надёжности связи в БАС целесообразно использовать резервирование каналов передачи данных. Одновременное применение радиочастотного соединения и мобильных сетей (LTE/5G) позволяет системе автоматически переключаться на резервный канал в случае возникновения помех или разрыва основного соединения. Такой подход способствует обеспечению стабильного управления и непрерывной передачи данных, что особенно важно при эксплуатации беспилотных систем в удалённых районах. Кроме того, для снижения влияния радиопомех могут применяться узкополосные или когнитивные радиосистемы, способные адаптивно выбирать наименее загруженные частотные диапазоны. Использование антенн с высоким коэффициентом усиления также способствует улучшению качества сигнала, обеспечивая устойчивую связь даже на значительных расстояниях.

При управлении беспилотными авиационными системами в реальном времени критически важна минимальная задержка передачи данных, так как она напрямую влияет на оперативность получения управляющих команд и телеметрической информации. Для обеспечения высокой скорости передачи даже в условиях возможных радиопомех применяются современные технологии, такие как ортогональное частотное разделение (OFDM – Orthogonal Frequency Division Multiplexing), позволяющее значительно повысить устойчивость связи и эффективность использования доступного спектра частот.

Оборудование, используемое для передачи данных, включая трансмиттеры, антенны и приемники, должно обладать высокой надежностью и быть адаптировано к различным условиям эксплуатации. Важное значение имеют материалы, устойчивые к внешним воздействиям, таким как температурные перепады, влага, коррозия и механические нагрузки. Это позволяет гарантировать стабильную работу системы связи на протяжении длительного времени.

Для повышения уровня защиты и предотвращения кибератак целесообразно внедрение систем мониторинга и обнаружения атак (IDS – Intrusion Detection Systems). Такие системы анализируют трафик в каналах связи и позволяют своевременно выявлять подозрительную активность, включая попытки несанкционированного доступа или перехвата данных. При обнаружении угрозы могут автоматически активироваться дополнительные защитные механизмы, например, усиленное шифрование, смена канала связи или переход на резервные системы.

Комплексный подход к обеспечению безопасности связи позволяет создать надежную и защищённую инфраструктуру для передачи данных в беспилотных авиационных системах, обеспечивая их эффективное функционирование в различных условиях эксплуатации [2].

Анализ уязвимостей и тестирование безопасности беспроводных протоколов с использованием HackRF

Для оценки эффективности используемых методов защиты связи необходимо проведение тестирования на устойчивость к возможным угрозам. Одним из программных инструментов, позволяющих выявлять уязвимости беспроводных каналов передачи данных, является HackRF. Его функциональные возможности позволяют моделировать различные виды атак и анализировать безопасность беспилотных авиационных систем в реальных условиях.

HackRF является одним из популярных программных инструментов для тестирования безопасности беспроводных систем, включая каналы связи БАС. Это программное обеспечение для программно-определяемого радио (SDR – Software Defined Radio), которое позволяет анализировать, передавать и принимать радиосигналы в широком диапазоне частот от 1 МГц до 6 ГГц. Благодаря этим возможностям HackRF может использоваться для исследования уязвимостей связи БАС, а также для тестирования устойчивости систем передачи данных к потенциальным угрозам.

Одним из ключевых направлений использования HackRF в области безопасности связи является анализ устойчивости каналов управления БАС к перехвату и глушению сигналов. С его помощью можно проводить тестирование на возможность атак типа jamming, при которых создаются помехи, нарушающие стабильность связи. Кроме того, HackRF позволяет моделировать атаки типа Man-in-the-Middle, при которых злоумышленник перехватывает и модифицирует сигналы между оператором и БАС. Это даёт возможность выявить уязвимости в используемых протоколах связи и разработать более надёжные методы их защиты.

Еще одним важным аспектом является тестирование безопасности беспроводных протоколов, применяемых в БАС. Многие беспилотные системы используют Wi-Fi, Bluetooth, Zigbee или специализированные радиопротоколы для передачи данных, и HackRF позволяет исследовать их за-

щитные механизмы, выявлять возможные уязвимости в шифровании и аутентификации. Это особенно важно в условиях растущих киберугроз, когда злоумышленники могут использовать уязвимости беспроводных стандартов для получения несанкционированного доступа к управлению БАС или к передаваемым данным.

Таким образом, применение HackRF в тестировании безопасности связи беспилотных авиационных систем позволяет не только выявлять потенциальные угрозы, но и разрабатывать меры по их предотвращению, что способствует повышению надёжности и защищённости беспроводных каналов передачи данных [3].

Использование GNU Radio для анализа безопасности и защиты каналов связи в беспилотных авиационных системах

Одним из перспективных инструментов для обеспечения безопасности связи и передачи данных в беспилотных авиационных системах является программная платформа GNU Radio. Это гибкий фреймворк с открытым исходным кодом, предназначенный для обработки радиосигналов и моделирования беспроводных систем. Благодаря широкому функционалу GNU Radio активно используется для анализа устойчивости каналов связи, тестирования защищённых протоколов передачи данных и выявления потенциальных уязвимостей в радиочастотных системах управления БАС.

Применение GNU Radio позволяет изучать влияние различных факторов на надёжность каналов связи, включая радиопомехи, атаки на беспроводные протоколы и попытки несанкционированного доступа. Используя этот инструмент, можно моделировать и анализировать атаки типа jamming, в ходе которых создаются помехи, способные нарушить передачу команд между оператором и БАС. Кроме того, с помощью GNU Radio можно тестировать системы на устойчивость к атакам типа Man-in-the-Middle, позволяющим злоумышленнику перехватывать и модифицировать передаваемые сигналы. Это особенно важно для повышения уровня защищённости систем связи, поскольку даёт возможность заранее выявлять и устранять уязвимости.

Дополнительным преимуществом GNU Radio является возможность работы с различными беспроводными стандартами, такими как Wi-Fi, Bluetooth, ZigBee, а также специализированными авиационными протоколами. Это позволяет исследовать их механизмы шифрования, аутентификации и защиты данных, а также разрабатывать новые методы повышения безопасности связи в БАС. Программная среда GNU Radio активно используется в научных исследованиях и практических экспериментах, направленных на совершенствование защищённых систем передачи данных.

Применение GNU Radio в беспилотных авиационных системах может быть полезно как на этапе проектирования, так и в ходе эксплуатации. На стадии разработки его можно использовать для моделирования защищённых каналов связи и тестирования алгоритмов шифрования. В процессе

эксплуатации платформа позволяет проводить мониторинг радиочастотного спектра, выявлять подозрительные сигналы и анализировать инциденты, связанные с нарушением работы каналов связи. Возможность гибкого конфигурирования системы даёт операторам БАС инструменты для повышения устойчивости связи и оперативного реагирования на потенциальные угрозы.

Таким образом, использование GNU Radio позволяет не только анализировать безопасность каналов связи, но и разрабатывать эффективные методы защиты от различных атак. Это делает платформу ценным инструментом для тестирования и совершенствования систем передачи данных в БАС, способствуя повышению их надёжности и устойчивости в условиях сложной радиочастотной обстановки [4].

Анализ и обеспечение безопасности беспроводных каналов связи в БАС с использованием SDRangel

Ещё одним мощным инструментов для анализа и обеспечения безопасности беспроводных каналов связи в беспилотных авиационных системах является программная платформа SDRangel. Это современное программное обеспечение для работы с программно-определяемыми радиосистемами, позволяющее принимать, передавать и анализировать радиосигналы в реальном времени. Благодаря поддержке широкого спектра SDR-устройств, таких как HackRF, BladeRF, USRP и RTL-SDR, SDRangel используется для изучения уязвимостей беспроводных систем связи, тестирования устойчивости каналов передачи данных и моделирования возможных атак.

Применение SDRangel в области безопасности БАС позволяет анализировать работу беспроводных протоколов, выявлять потенциальные угрозы и тестировать системы на устойчивость к различным видам атак. Одной из важных возможностей платформы является детальный спектральный анализ сигналов, позволяющий исследовать стабильность каналов связи и выявлять помехи. Это особенно полезно для обнаружения атак на связь, таких как глушение, при котором создаются сильные радиопомехи, приводящие к потере управления БАС. Кроме того, SDRangel даёт возможность моделировать атаки перехвата и подмены сигналов, позволяя исследовать методы защиты передаваемых данных.

Дополнительное преимущество SDRangel заключается в поддержке различных беспроводных стандартов, включая Wi-Fi, Bluetooth, GSM, LoRa и специализированные авиационные протоколы. Это даёт возможность тестировать их устойчивость к попыткам несанкционированного доступа, проверять эффективность механизмов шифрования и выявлять уязвимости в аутентификации устройств. Функции передачи данных, встроенные в SDRangel, позволяют не только анализировать радиосигналы, но и проверять системы связи на устойчивость к атакам типа Man-in-the-Middle, что делает платформу ценным инструментом для тестирования защищённых каналов управления БАС.

Программное обеспечение SDRangel может применяться как на этапе разработки беспилотных авиационных систем, так и в процессе их эксплуатации. На этапе проектирования оно используется для моделирования работы защищённых каналов связи, тестирования новых методов кодирования и шифрования данных. В ходе эксплуатации SDRangel позволяет проводить мониторинг радиочастотного спектра в режиме реального времени, выявлять аномалии в сигналах и анализировать возможные угрозы. Это делает его важным инструментом для операторов БАС, обеспечивающим дополнительный уровень контроля над беспроводными системами.

Таким образом, SDRangel является универсальным инструментом для анализа и тестирования безопасности связи беспилотных авиационных систем. Благодаря широкому набору функций, поддержке различных SDR-устройств и возможности работы с множеством радиопротоколов, эта платформа позволяет исследовать устойчивость каналов связи, выявлять уязвимости и разрабатывать эффективные методы защиты передаваемых данных. Это делает SDRangel незаменимым инструментом в сфере кибербезопасности БАС, способствующим повышению их надёжности в условиях реальной эксплуатации [5].

Заключение

Обеспечение безопасности связи и передачи данных в беспилотных авиационных системах требует комплексного подхода, включающего использование современных криптографических методов, резервирование каналов, а также мониторинг и анализ потенциальных угроз. Применение инструментов для тестирования защищённости беспроводных протоколов, таких как HackRF, GNU Radio и SDRangel, позволяет выявлять уязвимости и разрабатывать эффективные меры защиты от атак. Внедрение данных решений способствует повышению надежности и устойчивости систем связи БАС, обеспечивая их стабильное функционирование даже в условиях сложной радиочастотной обстановки и возможных киберугроз.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Иванов П.С., Смирнов А.В.* Методы защиты данных в беспроводных сетях: учеб. пособие. – М.: Техносфера, 2018. – 412 с.
2. Андреев М.Ю., Кузнецов Д.П. Безопасность беспроводных сетей и защита данных. – М.: Бином, 2021. – 290 с.
3. HackRF. (n.d.). HackRF – Great Scott Gadgets. – URL: https://greatscottgadgets.com/hackrf/ (дата обращения: 28.02.2025).
4. GNU Radio. (n.d.). GNU Radio – The Free & Open-Source Radio Ecosystem. – URL: https://www.gnuradio.org/ (дата обращения: 28.02.2025).
5. SDRangel. (n.d.). SDRangel – Open Source Qt5 / OpenGL 3.0+ SDR and Signal Analyzer. – URL: https://www.sdrangel.org/ (дата обращения: 28.02.2025).

УДК 004.94

П.С. Соколова

Волгоградский государственный университет, Россия, г. Волгоград

МОДЕЛЬ ОПРЕДЕЛЕНИЯ СОСТАВА СИСТЕМЫ ЗАЩИТЫ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

Цель работы – снижение рисков информационной безопасности электронных платежных систем (ЭПС) с помощью разработанной программной модели определения их состава системы защиты. Для этого рассмотрена статистика атак в сфере электронных платежей. Проанализирована структура ЭПС, в результате которой выявлены наиболее уязвимые места. Рассмотрены угрозы информационной безопасности ЭПС. Представлены функциональная модель и архитектура модели определения состава системы защиты ЭПС. Рассмотрен интерфейс и порядок работы с программным комплексом определения наиболее рациональных средств защиты электронных платежных систем. Приведены результаты экспериментальных исследований с помощью разработанной модели, показывающие достижение цели.

Ключевые слова: *система электронных платежей, оценка рисков, определение состава системы защиты.*

The aim of the work is to reduce the information security risks of electronic payment systems (EPS) using the developed software model for determining their composition of the protection system. For this purpose, the statistics of attacks in the field of electronic payments are considered. The EPS structure is analyzed, as a result of which the most vulnerable places are identified. Threats to the EPS information security are considered. The functional model and architecture of the model for determining the composition of the electronic payment system protection system are presented. A software package for determining the most rational means of protecting electronic payment systems is described. The results of experimental studies using the developed model are presented, showing the achievement of the goal.

Keywords*: electronic payment system, determination of the composition of the protection system, risk assessment, protection tools.*

Введение

В мировой экономике непрерывно функционируют ЭПС. Покупки в сети Интернет, обмен валют, денежные переводы – все это за счет минимальной комиссии и быстрого доступа все больше вытесняет оборот обычных денег. В электронных платежных системах курсирует конфиденциаль-

ная информация, которая требует тщательной защиты от просмотра и модификации. Поэтому актуальна разработка новых способов, инструментов и видов защиты электронных платежей, что и объясняет актуальность данного исследования [3].

Целью разработки модели определения состава системы защиты ЭПС является снижение рисков ИБ ЭПС.

Электронная платежная система – это технология, состоящая из совокупности методов, договоренностей и подтехнологий, которая позволяет производить расчеты между контрагентами по сетям передачи данных. Под защищенностью ЭПС понимается совокупность технических и клиентских средств защиты, обеспечивающих требуемый уровень безопасности [1].

Рассмотрим структуру ЭПС (рис. 1).

1. Регистрация пользователя: Пользователь регистрирует аккаунт в платежной системе, предоставляя свои персональные данные и создавая учетную запись.

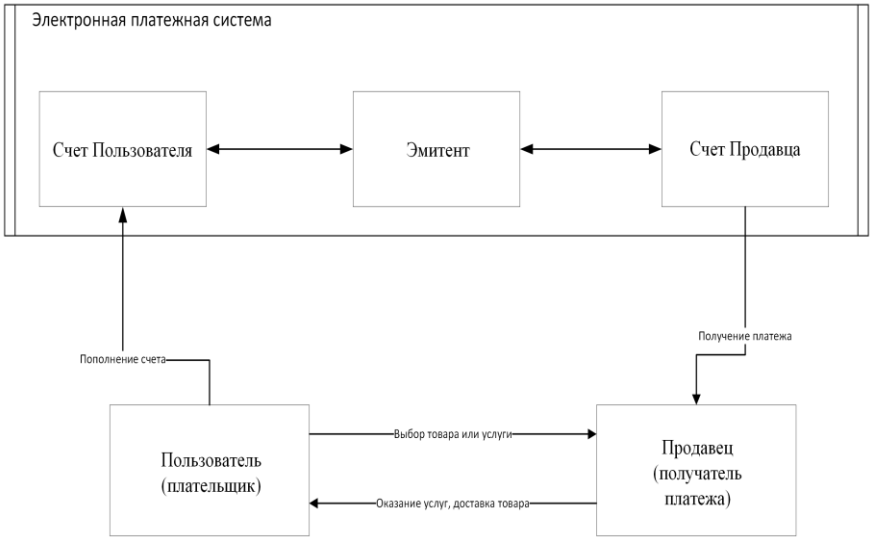


Рис. 1. Схема работы ЭПС

2. Аутентификация: Платежная система проверяет подлинность учетных данных пользователя и аутентифицирует его, используя различные методы, такие как пароль, двухфакторная аутентификация и т.д.

3. Пополнение счета: Пользователь может пополнить свой электронный счет, используя различные способы, такие как банковский перевод, карточные платежи или электронные платежи.

4. Совершение платежа: Пользователь может осуществить платеж, указав информацию о получателе (номер счета или электронный адрес) и сумму платежа.

5. Подтверждение платежа: Платежная система проверяет достаточность средств на счете пользователя и выполняет платеж, если все условия выполняются. Пользователь получает подтверждение о совершенном платеже.

6. Уведомление получателя: Платежная система уведомляет получателя о полученных средствах и предоставляет информацию о платеже.

7. Списание средств: Средства со счета пользователя списываются после осуществления платежа.

Из данной схемы можем выделить уязвимые места ЭПС:

1) доступ клиентов к средствам, аккумулированным на счетах;
2) обработка информации внутри организаций отправителя и получателя сообщений;
3) пересылка сообщений между банками, между банком и банкоматом, между банком и клиентом [7].

Активы ЭПС, наиболее подвергнутые угрозам:

- система обработки платежей (программное обеспечение, аппаратное обеспечение) подвергаются утечке данных из-за недостаточной аутентификации и авторизации пользователей;
- система хранения данных(базы данных) подвергается риску утечки данных из-за ненадлежащей защиты или атак хакеров;
- мобильные приложения подвергаются риску перехвата и подделки транзакций или кражи данных;
- веб-сайты подвергаются риску потери или кражи данных через вредоносные ПО и незащищенные формы;
- коммуникационные каналы подвергаются риску перехвата или подделки сообщений во время транзакций;
- физические устройства (банкоматы, POS–терминалы) подвергаются риску стримминга, взлома или манипулирования устройствами.

Анализ угроз электронным платёжным системам

По данным ЦБ РФ, отмечается постоянный рост похищенных средств. Рассмотрим статистику методов атак (рис. 2) в финансовом секторе за 1–3 кварталы 2023 года по данным PositiveTechnologies [10]:

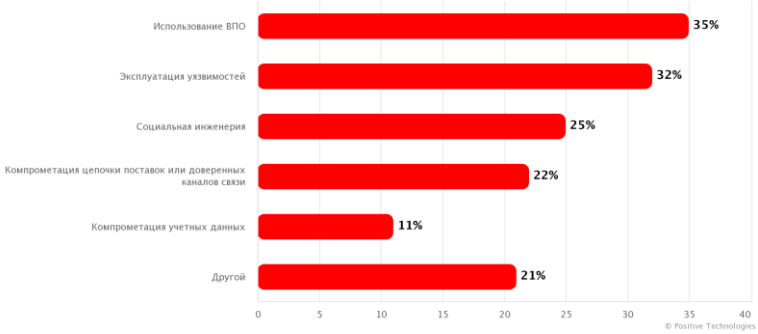


Рис. 2. Статистика методов атак финансовых организаций

Для решения проблемы нарушения конфиденциальности, целостности, и доступности информации средства защиты информации должны выполнять требования, установленные НПА [1, 2]:

- обеспечение защиты информации при управлении доступом;
- обеспечение защиты вычислительных сетей;
- контроль целостности и защищенности информационной инфраструктуры;
- защита от вредоносного кода;
- предотвращение утечек информации;
- управление инцидентами защиты информации;
- защита среды виртуализации;
- защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств.

Обеспечение защиты информации при осуществлении переводов денежных средств осуществляется с помощью средств криптографической защиты информации. САВЗ и способы защиты от вредоносного кода позволяют обеспечить защиту систем баз данных и серверов. СЗИ, используемые для защиты среды виртуализации от НСД, позволяют исключать НСД к информации, обрабатываемой в виртуальной инфраструктуре, контролировать информационный обмен, регистрировать события безопасности. Системы обнаружения вторжений позволяют выявить уязвимости в системе и вовремя реагировать на инциденты.

Разработка функциональной модели определения состава системы защиты электронных платежных систем

Функциональная модель формализации и описания процесса определения состава системы защиты электронных платежных систем выполнена в соответствии с методологией IDEF0. Диаграмма процесса представлена на рис. 3.

Рис. 3. Контекстная IDEF0-диаграмма процесса определения состава системы защиты ЭПС

Представим диаграмму процесса более подробно (рис. 4).

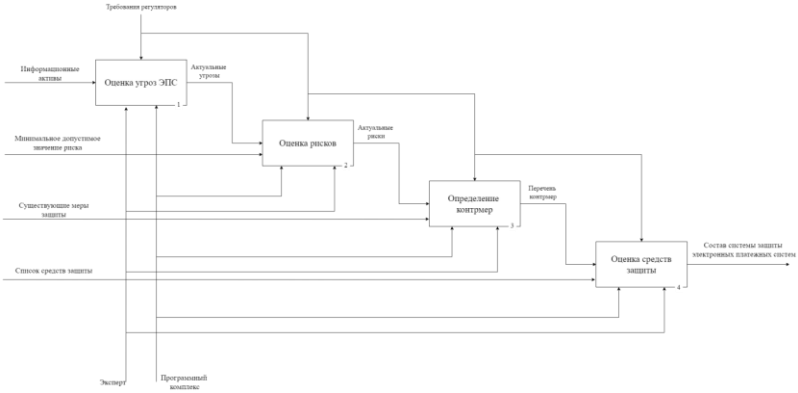


Рис. 4. Диаграмма процесса определения состава системы защиты электронных платежных систем.

Разработка архитектуры модели

Архитектура программного комплекса определения состава системы защиты электронных платежных систем разделена на 3 блока: блок оценки угроз ЭПС, блок определения контрмер, блок оценки средств защиты. Состав каждого блока представлен на рис. 5:

Рис. 5. Архитектура программного комплекса

В блоке оценки угроз эксперт выставляет оценку активам ЭПС, вероятности возникновения угрозы и степени уязвимости актива относительно угрозы. Блок определения контрмер служит для выявления необходимых контрмер на основе полученной оценки рисков. В блоке оценки средств защиты эксперт вводит данные для оценки средств защиты, далее программный комплекс производит расчет с помощью формулы расстояния Евклида и выбирает наиболее рационального средства защиты электронных платежных систем.

Экспериментальные исследования

Рассмотрим этапы работы эксперта с программным комплексом.

Эксперимент 1 – Описание системы, которой необходима защита ЭПС.

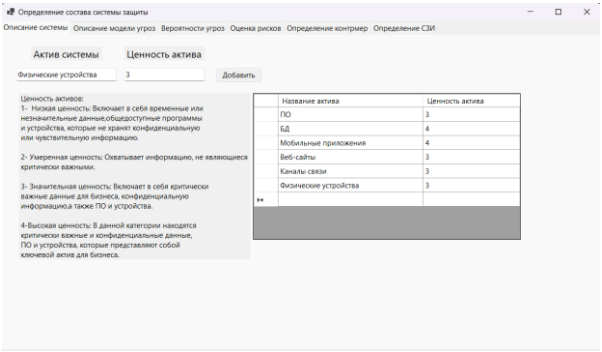


Рис. 6. Описание ЭПС (экранная копия)

На первом этапе пользователь вводит активы ЭПС и определяет ценность для каждого актива системы по шкале от 1 до 4 (рис. 6).

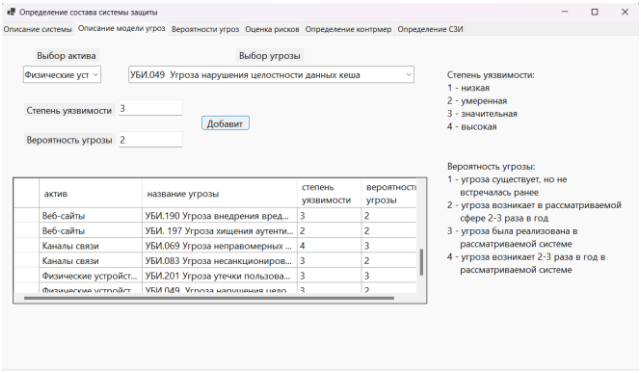


Рис. 7. Оценка ценности активов (экранная копия)

Далее для каждого из активов определяется степень уязвимости (от 1 до 4) и вероятность реализации угроз (от 1 до 4) (рис. 7).

Эксперимент 2 – Оценка рисков системы, которой необходима защита ЭПС.

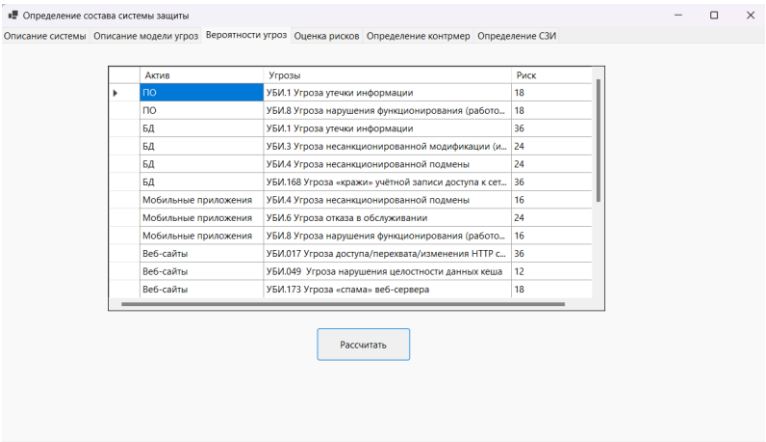


Рис. 8. Уровень риска активов ЭПС (экранная копия)

На вкладке «Вероятности угроз» производится расчет уровня риска для угроз информационной безопасности для активов системы (рис. 8).

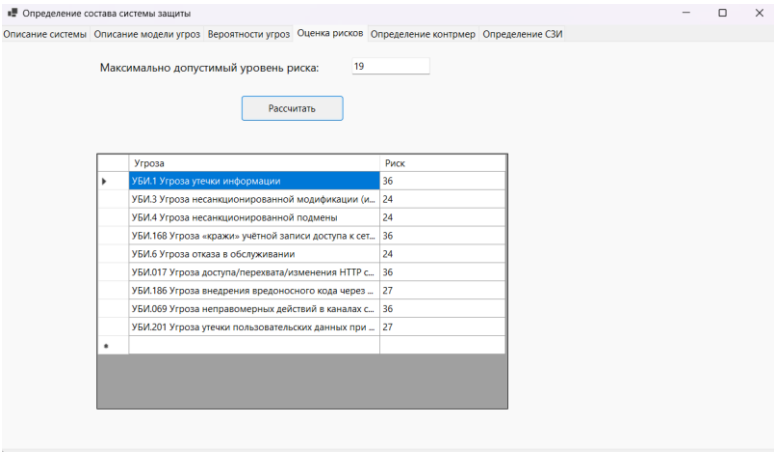


Рис. 9. Уровень риска угроз (экранная копия)

Пользователь определяет максимально допустимый уровень риска для своей системы и, исходя из этих данных, вычисляются угрозы, превышающие данный уровень (рис. 9).

Эксперимент 3 – Определение контрмер системы, которые необходимы для защиты ЭПС.

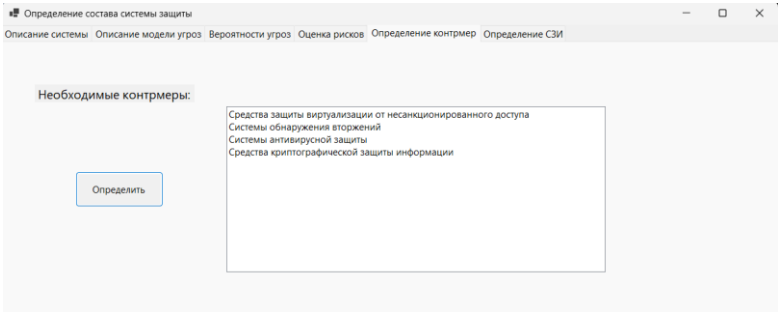


Рис. 10. Определение контрмер (экранная копия)

Исходя из списка выявленных угроз, формируется список необходимых контрмер для снижения рисков реализации угроз (рис. 10).

Эксперимент 4 позволил определить средства защиты, необходимые для защиты электронных платежных систем.

Эксперимент 5 Оценка рисков системы после внедрения системы защиты.

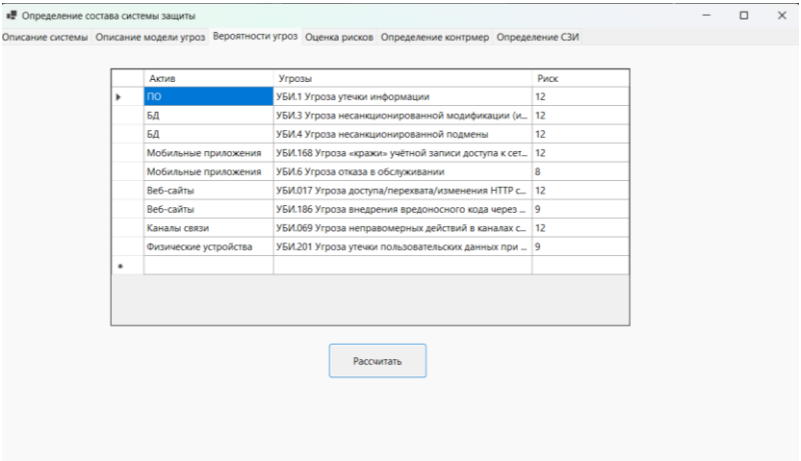


Рис. 11. Уровень риска после реализации контрмер (экранная копия)

Применение модели показало снижение рисков ИБ для ЭПС (рис. 11).

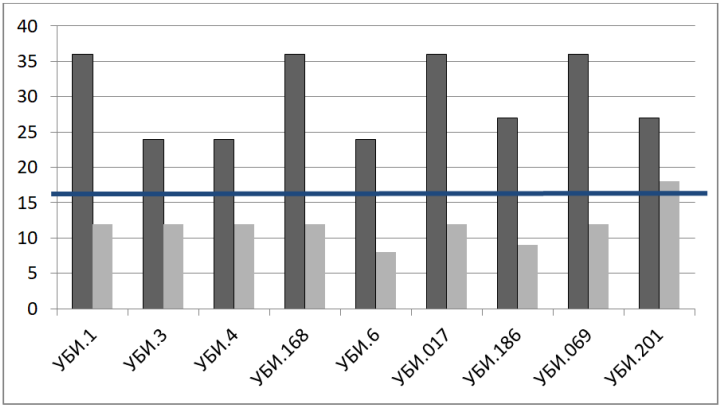


Диаграмма 1. Результаты оценки ИБ активов системы до и после внедрения предлагаемых СЗИ. уровень приемлемого риска. По оси X – номера угроз, по оси Y – уровень риска

После внедрения выбранной системы безопасности уровни риска для активов системы были значительно снижены, что подтверждает эффективность разработанной системы.

Заключение

Разработанный программный комплекс позволяет определить состав системы защиты электронных платежных систем, учитывая ценность активов ЭПС, их угрозы и степень реализации, вероятность возникновения угроз. Предложенная модель может использоваться в системах финансовых организаций, которые используют в своей работе электронные платежные системы для снижения рисков информационной безопасности до приемлемого уровня.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161–ФЗ // Собрание законодательства РФ. 04.07.2011. № 27. ст. 3872.
2. Положение Банка России от 4 июня 2020 г. № 719–П "О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств" [Электронный ресурс]. – URL: https://www.garant.ru/products/ipo/prime/doc/74609682/?ysclid=lrlzk6d9ms539919089 (Дата обращения: 10.11.2023).
3. *Ермаков Н.С., Галкина Е.А.* Мировой подход к защите электронных денег и диверсификация рисков // Экономика: вчера, сегодня, завтра. – 2020. – Т. 10. № 1А. – С. 443-451.
4. Безопасность электронных платежных систем Безопасность электронных платежных систем [Электронный ресурс] // studfile.net: [сайт]. – URL: https://studfile.net/preview/9453195/page:35/(Дата обращения: 20.11.2023).
5. *Мусалаева С.А., Краснякова Н.Н.* Электронные деньги и платежные системы // Финансово–кредитная система. – С. 206.
6. Система защиты информации в банковских системах (особенности информационной безопасности банковских и платежных систем). [Электронный ресурс]. – Режим доступа: https://files.student–it.ru/previewfile/103285/2#header1020314 (дата обращения: 03.11.2023).
7. *Османов А.А., Юдин Д.Е., Тринкин М.Г., Науменко В.В.* Анализ проблем обеспечения информационной безопасности электронной коммерции // Технические науки: проблемы и перспективы: материалы III Междунар. науч. конф. (г. Санкт–Петербург, июль 2015 г.). – СПб.: Свое издательство, 2015. – С. 99-101. – URL: https://moluch.ru/conf/tech/archive/126/8481/ (дата обращения: 25.11.2023).
8. *Маркина Т.А., Хрупов В.А.* Исследование защищенности систем электронных платежей // Программные продукты и системы. – 2017. – Т. 30, № 2. – С.
9. *Курочкий С.И., Заводцев И.В.* Методы оценки уровня защищенности информационных систем [Текст] // Информационные технологии и безопасность. – 2016. – № . – С. 197–204. (дата обращения: 10.05.2024).
10. Киберугрозы финансовой отрасли: промежуточные итоги 2023 года / [Электронный ресурс] // Positive technologies [сайт]. — URL: https://www.ptsecurity.com/ru–ru/research/analytics/financial–industry–security–interim–2023/?sphrase_id=292851 (дата обращения: 20.11.2023).
11. Информационная безопасность электронных платежных систем [Электронный ресурс]. – Режим доступа: https://searchinform.ru/informatsionnaya–bezopasnost/osnovy–ib/informatsionnaya–bezopasnost–v–otraslyakh/bezopasnost–informatsionnykh–sistem/informatsionnaya–bezopasnost–elektronnykh–platezhnykh–sistem/ (дата обращения: 27.11.2023).

УДК 004.056

В.В. Ткаченко

ОБЕСПЕЧЕНИЯ БЕЗОПСНОСТИ ОБЪЕКТОВ КИИ В ОБОРОННОЙ ПРОМЫШЛЕННОСТИ

В настоящее время значительно увеличился рост кибератак на объекты КИИ в сфере оборонной промышленности. Так как оборонная промышленность является основой национальной безопасности, нарушение работы её объектов критической информационной инфраструктуры может привести к катастрофическим последствиям. Таким образом, целью исследования является рассмотрение процедуры категорирования, которая позволяет выявить объекты критической инфраструктуры и присвоить им соответствующую категорию значимости, для дальнейшего обеспечения безопасности и побора мер защиты в соответствии с законодательством, опираясь на особенности функционирования предприятий в сфере оборонной промышленности. Для выполнения поставленной цели необходимо проанализировать правила категорирования утв. ППРФ-127, организовать выполнение требований законодательства с целью взаимодействия субъекта КИИ с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и Национальным координационным центром по компьютерным инцидентам (НКЦКИ). На основе результата описанной процедуры категорирования рассмотреть особенности обеспечения безопасности объектов КИИ и требования по обеспечению безопасности значимых объектов КИИ утв. Приказом Российской Федерации №239. В результате процедуры категорирования, постоянно действующая комиссия выявляет критические бизнес-процессы и на их основе составляет перечень объектов КИИ. Далле создается акт категорирования и в течении 10 дней направляется во ФСТЭК. Предприятие после подключения к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак при обнаружении компьютерного инцидента обязано оперативно реагировать на уведомления о выявленных угрозах и незамедлительно уведомлять национальный координационный центр по компьютерным инцидентам в соответствии с законодательством и установленным Регламентом. В итоге обеспечение безопасности объектов КИИ в оборонной промышленности требует строгого соблюдения нормативных требований и учета специфики отрасли, включая необходимость защиты государственной тайны, экономических интересов и технологической независимости. Требования по обеспечению безопасности значимых объектов КИИ, установленные Приказом ФСТЭК России № 239, а также Приказа ФСТЭК № 235, предусматривают комплексный подход к созданию и функционированию систем обеспечения информационной безопасности (СОИБ).

Ключевые слова: *критическая информационная инфраструктура, оборонная промышленность, ГосСОПКА, НКЦКИ, категорирование объектов КИИ, обеспечение безопасности, банк данных угроз, меры защиты, требования по защите, законодательство Российской Федерации, значимый объект, критический бизнес-процесс, сфера деятельности.*

Currently, the growth of cyber-attacks on CII facilities in the defense industry has increased significantly. Since the defense industry is the foundation of national security, disruption of its critical information infrastructure facilities can lead to catastrophic consequences. Thus, the purpose of the study is to consider the categorization procedure, which makes it possible to identify critical infrastructure facilities and assign them the appropriate category of significance, in order to further ensure security and take protective measures in accordance with the law, based on the specifics of the functioning of enterprises in the defense industry. To achieve this goal, it is necessary to analyze the rules for categorizing approved documents. PPRF-127, to organize the fulfillment of legal requirements in order to interact with the subject of the CII with the state system for detecting, preventing and eliminating the consequences of computer attacks (GosSOPKA) and the National Computer Incident Coordination Center (NCCC). Based on the result of the described categorization procedure, consider the features of ensuring the safety of CII facilities and the requirements for ensuring the safety of significant CII facilities approved by the By Order of the Russian Federation No. 239. As a result of the categorization procedure, a permanent commission identifies critical business processes and draws up a list of CII facilities based on them. A categorization report is created and sent to the FSTEC within 10 days. After connecting to the state system for detecting, preventing and eliminating the consequences of computer attacks, an enterprise must promptly respond to notifications of identified threats and immediately notify the national computer incident coordination center in accordance with the legislation and established Regulations. As a result, ensuring the safety of CII facilities in the defense industry requires strict compliance with regulatory requirements and consideration of industry specifics, including the need to protect state secrets, economic interests, and technological independence. The requirements for ensuring the security of significant CII facilities, established by Order of the FSTEC of Russia No. 239, as well as Order of the FSTEC No. 235, provide for an integrated approach to the creation and operation of information security systems.

Keywords: *critical information infrastructure, defense industry, state security, NCC, categorization of CII facilities, security, threat database, protection measures, protection requirements, legislation of the Russian Federation, significant facility, critical business process, field of activity.*

Введение

В результате развития информационно-коммуникационных технологий кибератаки стали более сложными и непредсказуемыми [1–4]. Хакеры постоянно разрабатывают новые виды атак, используя технологии и методы, которые ранее не применялись в киберпреступности. За последний год они приобрели все большую изощренность, становясь невозможными для блокирования и приводя к безвозвратному уничтожению информации в компьютерных системах [5]. Согласно данным компании RED Security, в 2024 году количество кибератак на российские компании увеличилось в 2,5 раза. Основная часть из них (это 64%) пришлась на предприятия, относящиеся к критической информационной инфраструктуре, что существенно превышает показатель за 2023 год [6].

Согласно Федеральному закону Российской Федерации №187 [7], субъектам критической информационной инфраструктуры принадлежат системы управления государственными, социальными, финансовыми, энергетическими и другими процессами, функционирование которых напрямую связано с обеспечением национальной безопасности [8]. В связи с этим все больше объектов критической информационной инфраструктуры становятся уязвимыми для киберугроз, что приводит к значительным финансовым потерям, угрозам для жизней людей и подрыву стабильности на уровне государства и бизнеса. В этом случае кибератака рассматривается как умышленное воздействие на объекты КИИ с целью нарушения их работы или полного прекращения их функционирования [9]. Именно поэтому работа по защите информации видеться постоянно. Системы безопасности должны быть адаптированы к быстро меняющимся условиям и новым видам угроз.

Оборонная промышленность занимает ключевую роль в обеспечении национальной безопасности Российской Федерации. Она является стратегически значимой и влияет на экономическое [10], научно-техническое, военно-техническое развитие страны [11]. Данные направления обеспечивают безопасность страны, её независимость от внешней политики и импорта техники. Она включает в себя предприятия, занимающиеся разработкой, производством и обслуживанием вооружений, военной техники и других стратегически важных продуктов.

Субъекты КИИ, функционирующие в сфере оборонной промышленности, могут относится к различным отраслям. Классификация отраслевой принадлежности помогает выявить критические процессы и определить объекты КИИ. Данные объекты критической информационной инфраструктуры представляют собой особую ценность, так как их уязвимость может привести к серьёзным последствиям обороноспособности страны. Нарушение их работы может привести к сбоям в производстве военной техники, утечки секретной информации.

1. Рассмотрение процедуры категорирования

Для субъектов КИИ проводится процедура категорирования объектов КИИ, которая позволяет выявить критические процессы и присвоить им категорию значимости. Так как в зависимости от присвоении или не присвоении объекту КИИ категории значимости будут отличаться требования по обеспечению безопасности.

При категорировании объектов критической информационной инфраструктуры первым этапом необходимо создать постоянно действующую комиссию по категорированию объектов КИИ. Далее разработать и утвердить Положение о постоянно действующей комиссии по категорированию объектов КИИ. Комиссия определяет бизнес-процессы и выявляет критические процессы на предприятии.

Исходя из правил категорирования утв. ППРФ-127 пункта 3 [12] бизнес-процессы обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ. При определении критических процессов в качестве перечня негативных последствий рассматривается Перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений.

Согласно п. 5 правил категорирования, утв. ППРФ-127, к критическим относятся процессы, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.

После того, как были определены критические процессы составляется перечень объектов КИИ и утверждается генеральным директором. Данный перечень направляется во ФСТЭК не позже 5 рабочих дней после его утверждения. Опираясь на Федеральный закон Российской Федерации №187, есть три вида объектов КИИ: информационная система (ИС), автоматизированная система управления (АСУ), информационно-телекоммуникационные сети (ИТКС). В оборонных предприятиях к объектам КИИ чаще всего относят ИС по учёту заработной платы и кадров, автоматизированные системы, осуществляющие управление технологическими и (или) производственными процессами, а также защищенные каналы связи внутри предприятий [13].

Далее непосредственно начинает работу комиссия и определяет категорию значимости объектов КИИ согласно утвержденного Перечня объектов КИИ. Для этого необходимо произвести оценку в соответствии с перечнем показателей критериев значимости ущерба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры.

Таким образом, итогом категорирования является акт категорирования, который направляется во ФСТЭК совместно со сведениями об объекте критической инфраструктуры, результатами анализа угроз безопасности информации объекта КИИ, результаты анализа угроз безопасности информации объекта критической информационной инфраструктуры, реализованные меры по обеспечению безопасности объекта критической информационной инфраструктуры, сведения о присвоенной объекту критической информационной инфраструктуры категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры.

Акт подписывается членами комиссии по категорированию и утверждается руководителем субъекта критической информационной инфраструктуры. В течении 10 дней со дня утверждения акта во ФСТЭК направляются сведения о результатах присвоения объекту КИИ одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из категорий. Данная форма утверждена приказом ФСТЭК России от 22.12.2017 №236 [14].

2. Выполнение требований законодательства с целью взаимодействия субъекта КИИ с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и Национальным координационным центром по компьютерным инцидентам (НКЦКИ)

В целях выполнения законодательства [15], после завершения процедуры категорирования и присвоения объектам КИИ соответствующей категории значимости необходимо осуществить подключение к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). Это является обязательным требованием Федерального закона №187. Для подключения к ГосСОПКА необходимо обратиться в ФСБ России или региональный орган, ответственный за подключение. Организация подаёт заявку, в которой указываются сведения об объектах КИИ, их категории значимости и контактная информация. После одобрения заявки специалисты ГосСОПКА помогают установить и настроить необходимое оборудование для мониторинга сетевого трафика. Это может включать установку специальных датчиков или программных агентов, которые передают данные в систему.

Следующим важным шагом становится налаживание взаимодействия с Национальным координационным центром по компьютерным инцидентам (НКЦКИ). Это позволяет обеспечить комплексный подход к обеспечению безопасности объектов критической информационной инфраструктуры (КИИ) в оборонной промышленности, где требования к защите информации особенно высоки. НКЦКИ выступает в роли координатора, помогая организациям оперативно реагировать на компьютерные инциденты (КИ) и минимизировать их последствия.

Для обеспечения чёткого и эффективного взаимодействия с НКЦКИ необходимо разработать Регламент взаимодействия, который определяет порядок обмена информацией, сроки уведомления о компьютерных инцидентах и формат предоставляемых данных. Типовая форма Регламента дорабатывается с учётом специфики оборонной промышленности, включая требования к защите информации, составляющей государственную тайну, и

особенности технологических процессов. После доработки Регламент утверждается руководством организации и становится основным документом, регулирующим взаимодействие с НКЦКИ.

Таким образом, после заверения процесса подключения к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак, предприятие обязано обеспечивать непрерывную передачу данных в ГосСОПКА и оперативно реагировать на уведомления о выявленных угрозах. При обнаружении компьютерного инцидента необходимо незамедлительно уведомить НКЦКИ в соответствии с утверждённым Регламентом. Для оборонной промышленности, где объекты КИИ имеют категорию значимости, такое взаимодействие является обязательным. Уведомление должно включать подробную информацию об инциденте, включая время обнаружения, характер угрозы и предпринятые меры.

3. Анализ особенностей обеспечения безопасности объектов КИИ в оборонной промышленности и описание требований по обеспечению безопасности значимых объектов КИИ утв. Приказом ФСТЭК №239

Обеспечение безопасности [15] объектов критической информационной инфраструктуры (КИИ) в оборонной промышленности имеет ряд особенностей, которые связаны как с стратегической значимостью этой отрасли, так и с её экономической ролью [17, 18]. Они включают в себя:

- Обработка информации составляющая государственную тайну требует использования специальных средств защиты, сертифицированных ФСТЭК и ФСБ.
- В условиях санкционного давления особое внимание уделяется переходу на отечественное программное обеспечение и оборудование. Переход на отечественное программное обеспечение в оборонной промышленности, несмотря на его стратегическую важность для обеспечения технологической независимости и национальной безопасности, сталкивается с серьёзными трудностями. Отсутствие полноценных аналогов зарубежных решений, проблемы с совместимостью и высокие затраты замедляют процесс.
- Обеспечение безопасности объектов КИИ в оборонной промышленности напрямую связано с защитой экономических интересов страны, т.к. утечка технологий может снизить конкурентоспособность российских предприятий на международном рынке.

В соответствии с Федеральным законом № 187-ФЗ от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации», ФСТЭК России устанавливает требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры (ЗОКИИ) и определены в Приказе ФСТЭК №239 [19]. Требо-

вания к созданию систем обеспечения информационной безопасности (СОИБ) ЗОКИИ определены в приказе ФСТЭК России от 21 декабря 2017 г. № 235 [20], где также регламентированы состав, структура и функции сил обеспечения информационной безопасности.

Для анализа угроз безопасности информации используется банк данных угроз, который ведется ФСТЭК России. После определения актуальных угроз проводится диагностический аудит, направленный на выявление уже реализованных мер защиты и тех, которые необходимо внедрить в процессе создания СОИБ. В рамках аудита осуществляется сопоставление принятых мер безопасности с требованиями, установленными приказом ФСТЭК России от 25 декабря 2017 г. № 239. Это позволяет определить, какие меры выполняются, а какие требуют реализации, а также оценить полноту их выполнения.

Результатом диагностического аудита является формирование плана мероприятий по обеспечению безопасности ЗОКИИ, который утверждается руководителем субъекта КИИ. Данный план включает перечень мер, которые могут быть реализованы с использованием встроенных или наложенных средств защиты.

Таким образом, обеспечение безопасности объектов КИИ в оборонной промышленности требует строгого соблюдения нормативных требований и учета специфики отрасли, включая необходимость защиты государственной тайны, экономических интересов и технологической независимости. Требования по обеспечению безопасности значимых объектов КИИ, установленные Приказом ФСТЭК России № 239, а также Приказа ФСТЭК № 235, предусматривают комплексный подход к созданию и функционированию систем обеспечения информационной безопасности (СОИБ). Кроме того, в соответствии с требованиями приказа ФСТЭК России от 21 декабря 2017 г. № 235, осуществляется внутренний контроль состояния безопасности ЗОКИИ. В рамках контроля проверяется выполнение нормативных правовых актов и организационно-распорядительных документов, а также оценивается эффективность принимаемых организационных и технических мер [21].

Заключение

При рассмотрении процедуры категорирования, итогом является акт категорирования, который направляется во ФСТЭК совместно со сведениями об объекте критической инфраструктуры, результатами анализа угроз безопасности информации объекта КИИ, результаты анализа угроз безопасности информации объекта критической информационной инфраструктуры, реализованные меры по обеспечению безопасности объекта критической информационной инфраструктуры, сведения о присвоенной объекту критической информационной инфраструктуры категории значимости либо об

отсутствии необходимости присвоения ему одной из таких категорий, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры.

Акт подписывается членами комиссии по категорированию и утверждается руководителем субъекта критической информационной инфраструктуры. В течении 10 дней со дня утверждения акта во ФСТЭК направляются сведения о результатах присвоения объекту КИИ одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из категорий. Данная форма утверждена приказом ФСТЭК России от 22.12.2017 №236.

После завершения процедуры категорирования и присвоения объектам КИИ соответствующей категории значимости необходимо осуществить подключение к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). В результате предприятие обязано обеспечивать непрерывную передачу данных в ГосСОПКА и оперативно реагировать на уведомления о выявленных угрозах. При обнаружении компьютерного инцидента необходимо незамедлительно уведомить НКЦКИ в соответствии с утверждённым Регламентом. Для оборонной промышленности, где объекты КИИ имеют категорию значимости, такое взаимодействие является обязательным. Уведомление должно включать подробную информацию об инциденте, включая время обнаружения, характер угрозы и предпринятые меры.

Обеспечение безопасности объектов КИИ в оборонной промышленности требует строгого соблюдения нормативных требований и учета специфики отрасли, включая необходимость защиты государственной тайны, экономических интересов и технологической независимости. Требования по обеспечению безопасности значимых объектов КИИ, установленные Приказом ФСТЭК России № 239, а также Приказа ФСТЭК № 235, предусматривают комплексный подход к созданию и функционированию систем обеспечения информационной безопасности (СОИБ). Кроме того, в соответствии с требованиями приказа ФСТЭК России от 21 декабря 2017 г. № 235, осуществляется внутренний контроль состояния безопасности ЗОКИИ. В рамках контроля проверяется выполнение нормативных правовых актов и организационно-распорядительных документов, а также оценивается эффективность принимаемых организационных и технических мер.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Карцан И.Н., Гончаренко Ю.Ю.* Влияние кибербезопасности на обработку информации в развивающихся новых технологиях // Вопросы контроля хозяйственной деятельности и финансового аудита, национальной безопасности, системного анализа и управления: Материалы VII Всероссийской научно-практической конференции, Москва, 29 декабря 2021 года. – М.: Федеральное государственное бюджетное научное учреждение "Экспертно-аналитический центр", 2022. – С. 471-479.
2. *Гончаренко Ю.Ю., Погуляй Г.С.* Sequential как основа защиты информационных систем // Правовая информатика. – 2024. – № 2. – С. 44-48. – DOI 10.21681/1994-1404-2024-2-44-48.
3. *Карцан И.Н.* Оценка схем и противодействие от кибератак на систему управления, включая и предприятий оборонно-промышленного комплекса // Технологии получения и обработки информации о динамических объектах и системах: Тезисы V Всероссийской научно-практической конференции, Москва, 03 октября 2024 года. – М.: Федеральное государственное бюджетное научное учреждение "Экспертно-аналитический центр", 2024. – С. 359-366.
4. *Мухтаров Д.Д.* Вопросы обеспечения безопасности критической информационной инфраструктуры от кибертеррористических атак. – 60-62.
5. *Бегишев И.Р.* Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. – 2019. – № 1. – С. 27-32.
6. Электронный ресурс. URL: https://www.ec-rs.ru/blog/novosti/trendy-v-kiberatakakh-na-rossiyskie-kompanii-v-2024-godu-/?utm_source=chatgpt.com
7. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Ссылка: https://www.consultant.ru/document/cons_doc_LAW_220885/ (статья 2, пункт 8).
8. *Гончаренко Ю.Ю.* Особенности идентификации радиолокационных целей при обеспечении безопасности критической информационной инфраструктуры // Вопросы кибербезопасности. – 2024. – № 1 (59). – С. 124-131. – DOI 10.21681/2311-3456-2024-1-124-131.
9. *Горелик В.Ю., Безус М.Ю.* О безопасности критической информационной инфраструктуры». – 1439-1442. – URL: https://cyberleninka.ru/article/n/o-bezopasnosti-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii/viewer.
10. Свидетельство о государственной регистрации программы для ЭВМ № 2024686553 Российская Федерация. Категорирование и оценка показателей критериев экономической значимости объектов КИИ: № 2024686324: заявл. 11.11.2024: опубл. 11.11.2024 / Ю.Д. Фот, В.Д. Павлидис; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования "Оренбургский государственный аграрный университет".
11. *Пелись В.В., Контылева Е.А., Егорова А.О.* Метод оценки экономической составляющей при организации информационной безопасности // Энергетические установки и технологии. – 2023. – Т. 9, № 1. – С. 177-181.
12. Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». – URL: https://www.consultant.ru/document/cons_doc_LAW_290595/?ysclid=m413fs93i0869182696.

13. *Цыпкина А.В., Шабурова А.В.* Категорирование объектов КИИ в оборонной промышленности // Интерэкспо Гео-Сибирь. – 2022. – Т. 6. – С. 288-293. – DOI 10.33764/2618-981X-2022-6-288-293. – EDN VALTUP.
14. Приказ ФСТЭК России от 22.12.2017 N 236 (ред. от 21.03.2019) «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».
15. Постановление Правительства Российской Федерации от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры».
16. *Аветисян В.А., Маслова М.А., Белов С.П.* Анализ существующих моделей обеспечения информационной безопасности в организациях // Информационная безопасность в контексте развития общества: Материалы III Международной научно-практической и научно-методической конференции, Белгород, 28 марта 2023 года. – Белгород: Автономная некоммерческая организация высшего образования «Белгородский университет кооперации, экономики и права», 2023. – С. 67-79.
17. *Головань С.А.* Влияние оборонных научных исследований на экономический рост // Управленческий учет. – 2023. – № 11-2. – С. 606-615. – DOI 10.25806/uu11-22023606-615.
18. *Гусева И.Б.* Основные направления оптимизации развития оборонно-промышленного комплекса в условиях экономических санкций // Вестник Астраханского государственного технического университета. Серия: Экономика. – 2023. – № 1. – С. 23-27. – DOI 10.24143/2073-5537-2023-1-23-27.
19. Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. – URL: https://www.consultant.ru/document/cons_doc_LAW_294287/?ysclid=m898hmrnkz737522883.
20. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования».URL:https://www.consultant.ru/document/cons_doc_LAW_291501/?ysclid=m898if3sql275308947.

21. *Егорова А.О., Лагуткина Т.В., Лебедев В.С.* Обеспечение безопасности критической информационной инфраструктуры: учебное пособие. – URL: https://goo.su/fPgrC.

УДК 004.056.2

К.Р. Филатова, Е.А. Маро

Южный федеральный университет, Россия, г. Таганрог

ИССЛЕДОВАНИЕ МЕТОДОВ ВЫЯВЛЕНИЯ СГЕНЕРИРОВАННОГО С ПОМОЩЬЮ DEEPFAKE-ИНСТРУМЕНТОВ ВИДЕО-КОНТЕНТА

В статье представлены результаты исследования методов детекции видеоконтента, сгенерированного с использованием DeepFake-инструментов. Проведён комплексный анализ современных технологий генерации синтетического видео, таких как GAN, VAE и диффузионные модели, рассмотрены угрозы информационной безопасности на основе применения DeepFake-инструментов. Основное внимание уделено разработке и тестированию методов выявления поддельного контента, включая физиологический анализ (моргания глаз, освещённость), демографический и эмоциональный анализ с использованием библиотек Dlib, MediaPipe и DeepFace, а также применение модели MesoNet для классификации кадров. Проведённое исследование подтвердило эффективность комбинированного подхода к детекции применения DeepFake-инструментов, сочетающего визуальные, физиологические и метаданные признаки. Результаты исследования могут быть применены в системах информационной безопасности, биометрической аутентификации и модерации контента для повышения достоверности визуальной информации в цифровом пространстве.

Ключевые слова: *DeepFake, информационная безопасность, поддельное видеоизображение, обнаружение манипуляций с видеоизображением.*

This article presents the results of a куыуфкср on methods for detecting video content generated using DeepFake tools. A comprehensive analysis of modern synthetic video generation technologies, such as GANs, VAEs, and diffusion models, is conducted, along with an examination of the cybersecurity threats posed by DeepFake applications. The primary focus is on the development and testing of methods for identifying manipulated content, including physiological analysis (eye blinking, lighting conditions), demographic and emotional analysis using Dlib, MediaPipe, and DeepFace libraries, as well as the application of the MesoNet model for frame classification. The research confirms the effectiveness of a combined approach to DeepFake detection, integrating visual, physiological, and metadata-based features. The research findings can be applied in cybersecurity systems, biometric authentication, and content moderation to enhance the reliability of visual information in the digital environment.

Keywords: *DeepFake, information security, fake video image, video image manipulation detection.*

Введение

За последние несколько лет технологии генерации медиа, основанные на методах глубокого обучения, достигли такого уровня совершенства, что разрабатываемые алгоритмы позволяют синтезировать аудио- и видеоконтент, практически неотличимый от оригинала. Появление и стремительное развитие DeepFake, где с помощью генеративных моделей создаются реалистичные подделки видеоизображений, ставят перед современным обществом и IT-сообществом новые вызовы. Эти технологии нашли применение как в развлекательной и образовательной сферах, так и в областях, где их использование сопряжено с высокими рисками дезинформации, компрометации безопасности и нарушения биометрической идентификации. Возрастает необходимостью разработки надёжных и адаптивных методов детекции DeepFake. Учитывая как повсеместное проникновение генеративных алгоритмов в массовые медиа, так и их потенциальное использование для обхода систем аутентификации и биометрической проверки, особенно важно создать инструменты, способные эффективно выявлять поддельный контент в условиях реального времени. Кроме того, новые методы генерации синтетических данных постоянно совершенствуются, что требует от исследователей непрерывного анализа существующих алгоритмов детекции и поиска способов их усовершенствования.

Современные методы генерации синтетического видеоконтента, получившие название DeepFake, представляют собой результат эволюции нейросетевых архитектур – от простых автокодировщиков до сложных генеративных моделей, объединяющих видео, аудио и текст в единую мультимодальную структуру. Первоначально использовавшиеся подходы опирались преимущественно на классические архитектуры сверточных сетей, однако по мере роста вычислительных возможностей и доступности данных произошёл переход к более выразительным и адаптивным системам генерации.

Архитектура нейросети – это структура и способ организации нейронов и связей между ними, а также то, какие операции происходят на каждом этапе обработки данных. Типы нейронных сетей, каждая из которых обладает своими архитектурными особенностями и областями применения:

- Генеративно-состязательные сети (GAN, Generative Adversarial Networks) – представляют собой двухкомпонентную архитектуру, состоящую из генератора и дискриминатора. Генератор создает изображения, стремясь «обмануть» дискриминатор, задача которого – отличать реальные данные от синтетических. Такие модели лежат в основе большинства DeepFake-инструментов, включая FaceSwap, DeepFaceLab и другие. Развитие GAN-пространства породило модификации, такие как StyleGAN, CycleGAN и StarGAN, каждая из которых вносила усовершенствования в область реалистичной генерации лиц, эмоций и поз [1, 2].

- Автокодировщики (Autoencoders) и вариационные автокодировщики (VAE) – применяются для компрессии и восстановления изображений с последующей генерацией. Именно такие архитектуры использовались в ранних версиях DeepFake-инструментов, где лицо исходного пользователя кодировалось в латентное пространство и воссоздавалось на другом носителе. Хотя их выразительность ограничена по сравнению с GAN, они до сих пор применяются в задачах, где важна реконструкция, а не максимальная фотореалистичность.
- Мультимодальные трансформеры и диффузионные модели [3] – наиболее современное направление, обеспечивающее генерацию контента не только из видео, но и на основе текстовых описаний, аудио или других типов входных данных. Модели типа Stable Diffusion, DALL·E или Runway Gen-2 формируют изображение или видео по заданному сценарию, фразе или аудиотреку.

Важной тенденцией стало появление интерактивных DeepFake-инструментов, таких как SadTalker или Deep Live Cam, способных в реальном времени трансформировать изображение лица, анимировать фотографию или заменять выражение и движения губ в соответствии с поступающим аудиосигналом. Такие системы используют каскадные архитектуры, включающие модули анализа ключевых точек, трекинга лицевых движений и генерации промежуточных фреймов.

Методы детекции DeepFake

На сегодняшний день эффективное распознавание DeepFake требует не только анализа визуальных артефактов, но и комплексного подхода, включающего физиологические признаки, временные несоответствия, мультимодальные рассогласования и анализ метаданных [4, 5].

Современные методы детекции можно условно разделить на три уровня:

- Низкоуровневый анализ пиксельных аномалий и свёрточные признаки (CNN),
- Высокоуровневый анализ последовательностей и временной согласованности (RNN, LSTM, Transformers),
- Мультимодальные и физиологические методы, ориентированные на реализм поведения (мимика, пульс, синхронизация речи).

Целью проведения исследования является практическая проверка эффективности существующих методов выявления DeepFake на видеоконтенте, сгенерированном с помощью различных DeepFake-инструментов. Для анализа использовались видеоролики, созданные с применением FaceSwap, Deep Live Cam, Runway и SadTalker. В качестве детекторов применялись: Dlib, MediaPipe, DeepFace, MesoNet, XceptoionNet, а также онлайн-сервис Deepfake-detection.

Физиологический анализ: моргания глаз (Dlib, MediaPipe)

Применялись два подхода к анализу морганий: с использованием библиотеки Dlib и с применением фреймворка MediaPipe. Оба подхода опираются на вычисление параметра EAR (Eye Aspect Ratio) – отношения вертикального размера глаза к его горизонтальному. При открытом глазе значение EAR стабильно и превышает порог, при закрытии оно резко снижается. Это делает параметр пригодным для бинарной классификации состояния глаз на открытые и закрытые. На практике использовался порог EAR = 0.25 и условие его превышения не менее чем на двух последовательных кадрах, что минимизирует вероятность ложноположительных срабатываний на микродвижения век [6, 7].

Библиотека Dlib использует модель предоставляющей точные координаты 68 ключевых ориентиров лица. Такая схема демонстрирует устойчивость к умеренному вращению головы и частичному затемнению глазных областей. Однако метод требует предварительной загрузки предобученной модели shape_predictor_68_face_landmarks.dat, что может повлиять на производительность в ресурсозависимых системах. Результаты анализа с помощью библиотеки Dlib представлены в табл. 1.

Таблица 1

Результаты анализа видеоизображений с помощью библиотеки Dlib

Видео	Кол-во морганий	Длительность (мин)	Частота морганий (в мин)	Оценочное заключение
Оригинальное	4	0.06	62.88	Реальное видео
DeepLive (реал. время)	13	0.38	34.51	Реальное видео
DeepLive (предзапись)	15	0.21	70.50	Реальное видео
FaceSwap (70 ч. обучения)	151	2.63	57.34	Реальное видео
FaceSwap (100 ч.)	3	0.43	7.04	Подозрение на DeepFake
SadTalker	0	0.13	0.00	Подозрение на DeepFake
Runway	1	0.08	11.90	Реальное видео

В качестве альтернативного подхода рассматривался анализ морганий с использованием MediaPipe FaceMesh – высокоэффективной системы от Google, реализующей 3D-сегментацию лица с определением до 468 ориентиров. В отличие от Dlib, MediaPipe не требует загрузки внешних моделей, что упрощает развертывание, однако предъявляет более высокие требования к точности выбора координат для расчёта EAR.

Пороговое значение EAR в случае MediaPipe было скорректировано до 0.32, с учётом иной системы координат и масштабов. Детекция морганий производилась при превышении этого порога на трёх и более последовательных кадрах. Результаты анализа представлены в табл. 2.

В дополнение к количественным данным приведены примеры работы программы MediaPipe, визуализирующие процесс анализа морганий для каждого исследуемого видео. На рис. 1-7 представлены кадры из системы реального времени, использующей MediaPipe FaceMesh, где отображаются:

- ключевые ориентиры глазной области, выделяемые моделью;
- текущее значение параметра EAR;
- общее количество зафиксированных морганий;
- график изменения EAR по временной оси.

Таблица 2

Результат анализа с помощью библиотеки MediaPipe

Видео	**Кол-во морганий**	**Длительность (мин)**	**Частота морганий (в мин)**	**Оценочное заключение**
Оригинальное	4	0.06	62.88	Реальное видео
Deep Live Cam (предзапись)	13	0.21	61.10	Подозрение на DeepFake
Deep Live Cam (реальное время)	7	0.38	18.58	Реальное видео
FaceSwap (70 часов обучения)	75	2.63	28.48	Подозрение на DeepFake
FaceSwap (100 часов обучения)	0	0.43	0.00	Подозрение на DeepFake
SadTalker	0	0.13	0.00	Подозрение на DeepFake
Runway	0	0.08	0.00	Подозрение на DeepFake

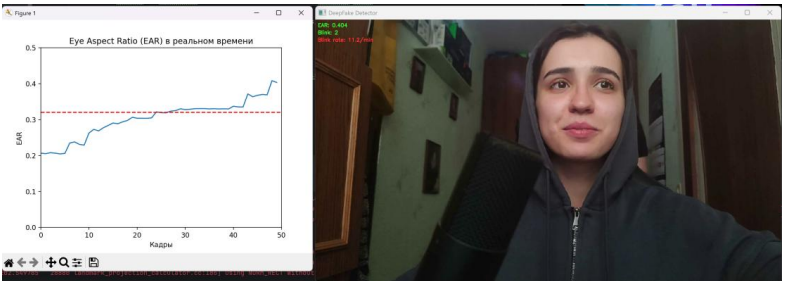


Рис. 1. Анализ настоящего видео

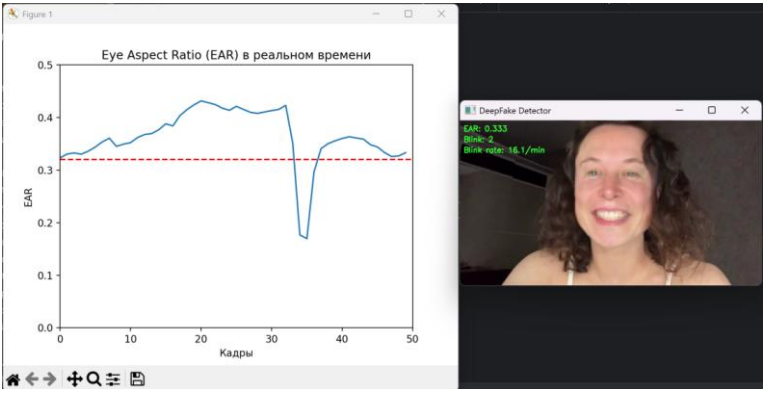


Рис. 2. Анализ видео Deep Live Cam

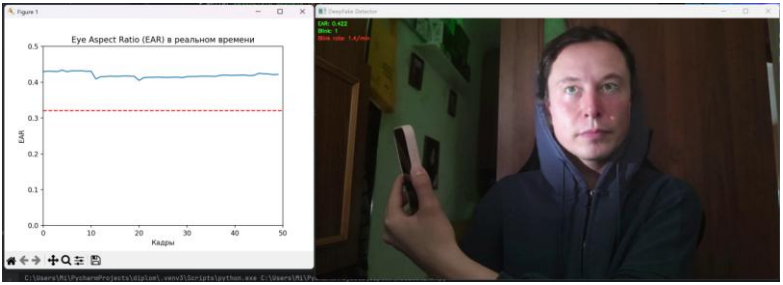


Рис. 3. Анализ видео Deep Live Cam

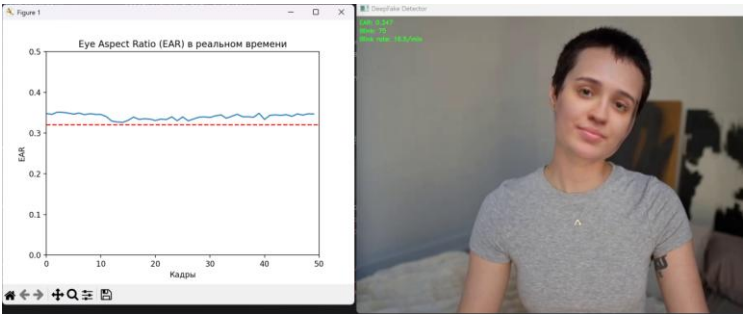


Рис. 4. Анализ видео FaceSwap

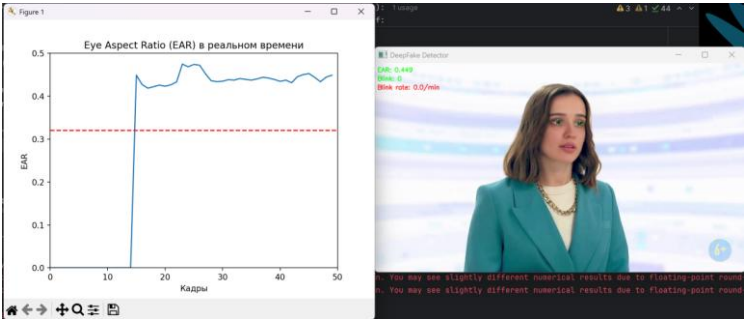


Рис. 5. Анализ видео FaceSwap

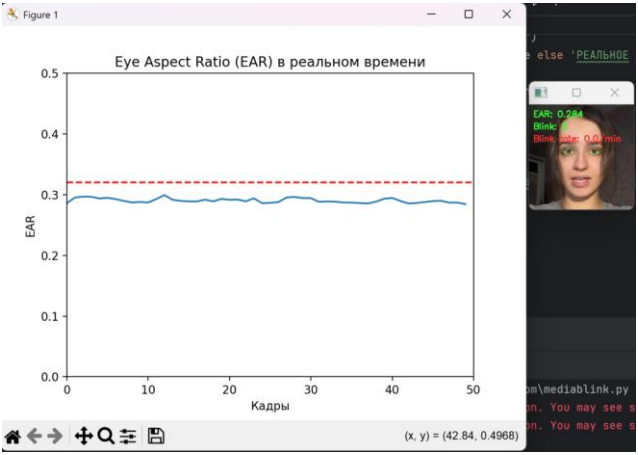


Рис. 6. Анализ видео SadTalker

Рис. 7. Анализ видео RunWay

Оба примененных подхода имеют свои преимущества и ограничения. Dlib обеспечивает стабильность при условии наличия модели и достаточного качества изображения, тогда как MediaPipe обладает высокой скоростью и масштабируемостью, но требует точной настройки. В условиях необходимости автоматического анализа видео в режиме реального времени MediaPipe выглядит перспективным решением, однако его применение в задачах критической безопасности должно сопровождаться этапом калибровки и верификации результатов.

Демографический и эмоциональный анализ DeepFace

Одним из значимых векторов в анализе достоверности видеоизображения является исследование демографических и эмоциональных характеристик лиц, отображённых в кадре. DeepFace предоставляет доступ к модели gender_model, основанной на архитектуре MiniXception, которая обучалась на открытых датасетах с разметкой пола. Модель продемонстрировала устойчивую работу в условиях реального видео, а также высокую чувствительность к генеративным артефактам при анализе синтетических изображений [8].

Анализ проводился на кадрах, извлечённых с заданной периодичностью (каждые 30 кадров при 30 FPS), и включал автоматическое определение трёх ключевых характеристик (табл. 3):

- возраст (age);
- эмоциональное состояние (dominant_emotion);
- пол (dominant_gender).

Таблица 3

Результаты демографического и эмоционального анализа видео с помощью DeepFace

Видео	Кол-во кадров	Стабильность возраста	Главная эмоция	Частота эмоции	Пол (доминирующий)	Оценочное заключение
FaceSwap (70 ч.)	158	4.64	neutral	32.9%	Woman (55%)	Подозрение на DeepFake
FaceSwap (100 ч.)	26	3.29	neutral	76.9%	Woman (77%)	Видео выглядит реальным
Deep Live Cam (предзапись)	13	3.30	neutral	46.2%	Man (69%)	Видео выглядит реальным
Deep Live Cam (реал. время)	46	3.63	neutral	39.1%	Man (95.6%)	Видео выглядит реальным
SadTalker	7	0.69	neutral	100%	Woman (100%)	Подозрение на DeepFake
Runway	5	1.14	fear/sad (по 40%)	–	Woman (60%)	Подозрение на DeepFake

Большинство фальсифицированных видео демонстрируют аномально стабильные или наоборот колеблющиеся показатели по возрасту, а также ограниченное разнообразие эмоций, что косвенно подтверждает гипотезу о некорректной генерации эмоциональной мимики.

Детекция с использованием модели MesoNet

Помимо оценки биометрических и визуальных признаков, в рамках исследования была проведена серия экспериментов с использованием специализированной модели MesoNet, адаптированной для задач выявления DeepFake.

Процедура анализа включала извлечение кадров из видеороликов с интервалом в 5 кадров, масштабирование изображений до 256×256 пикселей и подачу их на вход модели. Результатом работы являлось значение Fake score для каждого кадра, которое затем использовалось для статистического и визуального анализа. Такой подход позволил оценить не только среднюю степень «подозрительности» видео, но и выявить локальные участки с атипичным поведением [9].

На видео, созданном с помощью FaceSwap (70 часов обучения), большинство кадров получили метку FAKE с уверенностью выше 0.75, в том числе с пиками до 0.95, что указывает на наличие устойчивых синтетических признаков. Однако пять кадров были классифицированы как REAL, что, вероятно, связано с техническими ограничениями обработки: часть из них была слишком тёмной, на других лицо отсутствовало или сливалось с фоном. Эти случаи демонстрируют важность учета контекста кадра при интерпретации выходов модели.

Второе видео FaceSwap, созданное после 100 часов обучения, показало однозначную классификацию всех кадров как FAKE, что подтверждает наличие синтетических артефактов, сохраняющихся даже при улучшении параметров генерации. Аналогичный результат был получен при анализе видео, сгенерированного инструментом Deep Live Cam в режиме наложения маски на предзапись: модель MesoNet отметила 100% кадров как поддельные.

Более неоднозначные результаты были зафиксированы при обработке видео, созданного с использованием Deep Live Cam в режиме реального времени. Из общего числа проанализированных кадров восемнадцать были классифицированы как REAL, однако уровень уверенности в этих случаях оставался низким (Fake score в диапазоне 0.19–0.4), что может свидетельствовать как о неопределённости модели, так и о фрагментах видео с отсутствием лица или нарушением структуры входных данных. При этом видео, сгенерированные с помощью SadTalker и Runway, были классифицированы как FAKE практически во всех кадрах, с показателями Fake score, близкими к единице. Это указывает на слабую способность этих моделей к сокрытию синтетических признаков при визуально достоверной анимации.

Модель MesoNet продемонстрировала высокую чувствительность и устойчивость к разным стилям генерации, что делает её эффективным инструментом в задачах покадрового анализа и выявления фальсифицированного контента, особенно в случаях, когда синтетика не очевидна визуально, но оставляет характерные цифровые следы.

Покадровый анализ освещённости

Одним из малозаметных, но потенциально информативных признаков, способных указывать на подделку изображения лица, является локальная неравномерность освещения. При естественном освещении лицо человека демонстрирует определённую закономерность в распределении света: зоны лба, носа и щёк освещаются согласованно, с плавными градиентами. В синтетических масках, созданных с помощью DeepFake-инструментов, такая согласованность может нарушаться – особенно в условиях нестабильного света или при неполной симуляции затенения.

Для оценки освещённости была реализована методика, основанная на выделении четырёх ключевых зон лица: левой щеки, правой щеки, области носа и лобной зоны. Координаты этих участков извлекались с использованием модели landmark-детектора из библиотеки Dlib (shape_predictor_68_face_landmarks.dat). Яркость в каждой зоне измерялась в оттенках серого, полученных путём преобразования изображения в grayscale-формат. На рисунках 8, 9 представлены результаты оценки освещённости. Результаты сравнения реального и синтетического видео представлены в табл. 4.

Рис. 8. Покадровый анализ освещённости лица. Видео Deep Live Cam

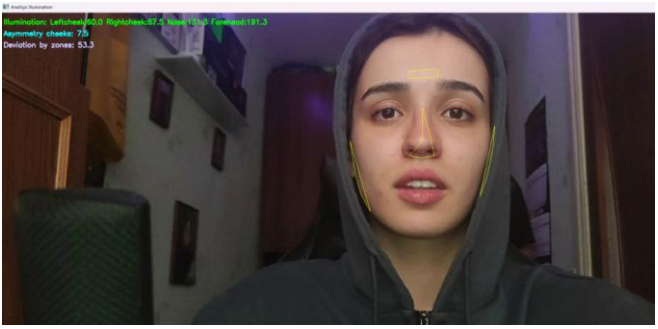


Рис. 9. Покадровый анализ освещённости лица. Оригинальное видео

Анализ локальной освещённости может служить дополнительным и независимым источником признаков при выявлении синтетического видеоконтента. Данный вид анализа не требует глубоких нейросетей и может использоваться в качестве объяснимого и наглядного критерия, особенно в ситуациях, при которых визуальные и физиологические признаки оказываются недостаточно выразительными или противоречивыми.

Таблица 4

Анализ освещенности

Параметр	Реальное лицо	Поддельное лицо
Освещённость левой щеки	62.5	86.8
Освещённость правой щеки	53.9	71.9
Освещённость носа	131.8	101.9
Освещённость лба	191.0	169.7
Асимметрия щёк	8.6	14.9
Отклонение по зонам	55.8	37.4

Метаданные и цифровые следы

Метаданные отражают технические параметры устройства съёмки, программного обеспечения, характеристики кодирования, а также хронологические атрибуты: дату создания, модификации, длительность, частоту кадров и др. В случае с поддельным видео, созданным с использованием генеративных моделей и инструментов DeepFake, в метаданных зачастую отсутствуют или искажены параметры, которые были бы обязательными при записи контента на физическое устройство [10].

Извлечение и интерпретация метаданных производились с использованием утилит ExifTool и MediaInfo, что позволило выявить общие закономерности, представленные в табл. 5.

Таблица 5

EXIF – анализ видеоизображений

Инструмент	Название файла	Разрешение	Длительность	Частота кадров	Битрейт	Кодек / Энкодер
FaceSwap	itog.mp4	1920×1080	2:38	30 fps	~2.03 Mbps	avc1 / Lavf60.16.100
SadTalker	sadtalker.mp4	256×256	7.68 сек	25 fps	~228 kbps	avc1 / Lavf58.76.100
Runway Gen-2	gen_4_turbo.mp4	832×1104	5.04 сек	24 fps	~1.66 Mbps	avc1 / Lavf58.29.100
Deep Live Cam	ilonmasklight.mp4	1920×1080	22.6 сек	60 fps	~5.62 Mbps	avc1 / Lavf59.27.100

Заключение

В условиях стремительного роста объемов фальсифицированных медиа данных, включая дипфейки, возрастает угроза манипуляций общественным мнением, дискредитации публичных лиц, компрометации биометрических систем идентификации, а также нарушений в области кибербезопасности.

На основе анализа современных генеративных моделей, таких как GAN (генеративно-состязательные сети), VAE (вариационные автоэнкодеры) и диффузионные модели, была сформулирована теоретическая база, описывающая архитектуры и принципы функционирования технологий создания дипфейков. Подробно рассмотрены существующие программные инструменты генерации синтетических видео – FaceSwap, Deep Live Cam, Runway ML, SadTalker, а также их архитектурные особенности и применяемые модели.

Основная часть исследования была посвящена методам и практическим подходам к детекции дипфейк-контента. Классификация методов показала, что наибольшую эффективность демонстрируют гибридные подходы, сочетающие извлечение физиологических признаков (например, моргание глаз), демографический анализ, покадровую оценку освещенности и анализ цифровых следов (метаданных). Для реализации детекторов использованы библиотеки dlib, MediaPipe, нейросетевая модель MesoNet, инструмент ExifTool, применяемый для анализа встроенных метаданных мультимедийных файлов, а также внешние онлайн-сервисы, такие как HuggingFace Spaces. Все предложенные методы были апробированы на самостоятельно сгенерированных дипфейках и продемонстрировали различные уровни точности, скорости и ресурсоемкости.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Hong Y., Hwang U., Yoo J., Yoon S.* How Generative Adversarial Networks and Their Variants Work: An Overview // ACM Computing Surveys (CSUR). – 2022.
2. *Gui J., Sun Z., Wen Y., Tao D., Ye J.* A Review on Generative Adversarial Networks: Algorithms, Theory, and Applications // IEEE Transactions on Knowledge and Data Engineering. – 2021.
3. Ho J., Jain A., Abbeel P. Denoising Diffusion Probabilistic Models // arXiv preprint arXiv:2006.11239. – 2020.
4. *Rossler A., Cozzolino D., Verdoliva L., Riess C., Thies J., Nießner M.* FaceForensics++: Learning to Detect Manipulated Facial Images // arXiv preprint arXiv:1901.08971. – 2019.
5. Increasing Threat of DeepFakes: Team Introductions // Международный форум по кибербезопасности. – 2021.
6. Mediapipe Инструменты для анализа и обнаружения дипфейков. – URL: https://habr.com/ru/articles/596043/ (дата обращения: 20.04.2025).
7. *Abdullah M.T., Ali N.H.M.* Facial deepfake performance evaluation based on three detection tools: MTCNN, Dlib, and MediaPipe // Fifth International Conference on Applied Sciences (ICAS2023). – 2024.
8. Репозиторий DeepFace. – URL: https://github.com/serengil/deepface (дата обращения: 01.05.2025).
9. Репозиторий MesoNet (Meso4). – URL: https://github.com/rajanieprabha/FakeVideoDetection/blob/master/Meso4.py (дата обращения: 12.05.2025).
10. ExifTool – инструмент для анализа https://github.com/exiftool/exiftool (дата обращения: 23.05.2025).

УДК 004.055.5

В.А. Чумак, Л.К. Бабенко

Южный федеральный университет, Россия, г. Таганрог

СРАВНЕНИЕ ВРЕМЕНИ РЕАЛИЗАЦИИ АЛГОРИТМА МАГМА ПРИ ИСПОЛЬЗОВАНИИ РАЗЛИЧНЫХ УРОВНЕЙ АБСТРАКЦИИ ИНСТРУМЕНТОВ РАСПАРАЛЛЕЛИВАНИЯ

В данной работе рассматривается параллельная реализация алгоритма шифрования Магма (Magma) с использованием двух различных подходов к организации параллельных вычислений: низкоуровневой библиотеки MPI и высокоуровневой TPL. Алгоритм Магма является симметричным блочным шифром, и его параллельная реализация направлена на повышение производительности при шифровании больших объемов данных. В рамках работы произведено сравнение ускорения шифрования алгоритмом Магма при использовании TPL и MPI на различных конфигурациях вычислительных ресурсов.

Ключевые слова: *алгоритм Магма, параллельные вычисления, шифрование, MPI, TPL, многозадачность, производительность, криптография, распределённые вычисления, синхронизация.*

This paper considers the parallel implementation of the Magma encryption algorithm using two different approaches to organizing parallel computing: the low-level MPI library and the high-level TPL abstraction. The Magma algorithm is a symmetric block cipher, and its parallel implementation is aimed at increasing productivity when encrypting large amounts of data. As part of the work, a comparison was made between the acceleration of encryption by the Magma algorithm when using TPL and MPI on various configurations of computing resources.

Key words: *Magma algorithm, parallel computing, encryption, MPI, TPL, multitasking, performance, cryptography, distributed computing, synchronization.*

Введение

В данной статье рассматривается ускорение симметричного шифрования в зависимости от уровня абстракции инструментов параллелизма, с акцентом на использование .NET Task Parallel Library (TPL) как более высокого уровня и Message Passing Interface (MPI) как более низкого. В качестве симметричного алгоритма выбран Магма из-за его широкого применения в отечественной криптографии и высокой эффективности при обработке больших объемов данных, что делает его идеальным объектом для исследования оптимизации шифрования.

Параллельная реализация алгоритма шифрования Магма

Магма (Magma) – это симметричный блочный криптографический алгоритм, стандартизованный в рамках российского ГОСТ Р 34.12–2015, предназначенный для обеспечения конфиденциальности информации за счет её криптографического преобразования. Принцип его работы базируется на симметричной схеме с фиксированным размером блока данных 64 бита и длиной ключа 256 бит, что обеспечивает необходимый уровень стойкости при обработке чувствительной информации.

В алгоритме реализуется естественный параллелизм обработки данных, связанный с независимостью вычислений при шифровании и дешифровании отдельных блоков открытого текста. Магма работает в режиме простой замены и каждый блок текста зашифровывается независимо от других базовым алгоритмом шифрования, описанным в ГОСТ Р 34.12–2015, а степень масштабируемости напрямую определяется количеством доступных вычислительных ресурсов.

На этапе предварительной подготовки выполняется процедура генерации подключей и разделение открытого текст на блоки по 64 бит. Данный этап реализуется последовательно, поскольку операция инициализации проводится единожды и не оказывает критического влияния на общую производительность параллельной системы.

Алгоритм реализован на языке программирования C++ для использования низкоуровневой библиотеки MPI и на C# для использования высокоуровневой абстракции TPL. Схема реализации алгоритма шифрования с использованием инструментов параллелизма проиллюстрирована в среде с доступными 3 потоками на рис. 1.

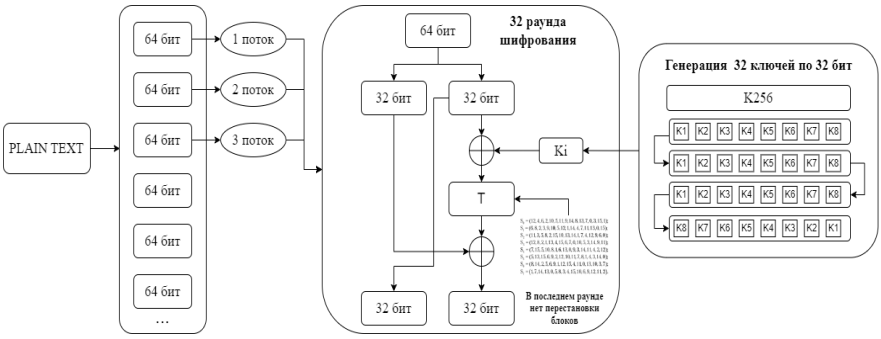


Рис. 1. Схема параллельной реализации алгоритма Магма в среде с 3 потоками

Преимущества низкоуровневой библиотеки MPI

MPI представляет собой промышленный стандарт, предназначенный для организации обмена сообщениями между процессами в распределённых вычислительных системах. Он реализует парадигму параллельных вычислений с использованием модели распределённой памяти, в рамках которой отдельные процессы взаимодействуют посредством явной передачи данных. Особенностью MPI является его низкоуровневая архитектура, обеспечивающая высокую степень контроля над коммуникациями и синхронизацией процессов. Стандарт поддерживает широкий спектр коммуникационных схем, включая точечные взаимодействия и коллективные операции, а также механизмы топологий и виртуальных коммуникаторов, что делает его эффективным инструментом для построения масштабируемых параллельных приложений на суперкомпьютерах и кластерных системах.

В рамках реализации алгоритма шифрования каждый процесс выполняет операции шифрования и дешифрования над выделенным ему подмножеством данных автономно, что исключает необходимость синхронного взаимодействия между вычислителями в ходе основного этапа обработки. В этой задачи отсутствуют зависимости между обрабатываемыми блоками, а степень параллелизма определяется исключительно числом доступных вычислительных ресурсов.

В процессе шифрования с использованием MPI первоначально определяется общее число доступных процессов с помощью функции MPI_Comm_size, а также идентификация ранга (уникального номера) каждого процесса посредством MPI_Comm_rank. На основании полученного количества процессов производится разбиение исходного текста на равные блоки по 64 бит, соответствующие числу задействованных потоков. Для синхронизации количества передаваемых блоков между всеми процессами используется операция MPI_Bcast. Далее блоки текста распределяются между процессами с помощью функции MPI_Scatter, причем передача осуществляется от корневого (root) процесса. После выполнения операций шифрования каждым из процессов, зашифрованные блоки собираются обратно на корневом процессе с использованием функции MPI_Gather.

В коде на языке программирования C++ используются следующие MPI вызовы для параллельной реализации криптографического алгоритма Магма:

- MPI_Comm_size – определяет общее количество процессов, участвующих в вычислениях.

Входные параметры:

- MPI_Comm – это фундаментальная структура, обеспечивающая организацию процессов в логические группы и управление контекстом обмена сообщениями между ними.
- int *size – указатель на переменную, в которую будет записано количество процессов.

Программный код:

```
Int world_size;
MPI_Comm_size(MPI_COMM_WORLD, &world_size);
```

- MPI_Comm_rank – определяет уникальный идентификатор текущего процесса.

Входные параметры:

- MPI_Comm – коммуникатор (обычно MPI_COMM_WORLD).
- int *rank – указатель на переменную, в которую будет записан ранг текущего процесса. Это уникальный номер, который присваивается каждому процессу внутри коммуникатора (от 0 до N-1).

Программный код:

```
int world_rank;
MPI_Comm_rank(MPI_COMM_WORLD, &world_rank);
```

- MPI_Bcast – используется для передачи информации о количестве блоков данных от корневого процесса ко всем остальным процессам.

Входные параметры:

- void *buffer – указатель на данные для передачи.
- int count – количество блоков данных, предназначенных для передачи.
- MPI_Datatype datatype – тип передаваемых данных.
- int root – ранг процесса-отправителя (как правило – 0 ранг).
- MPI_Comm comm – коммуникатор.

Программный код:

```
// Количество блоков данных (по 8 байт)
int num_blocks = text_data.size()/8
+(text_data.size()%8!=0);
MPI_Bcast(&num_blocks, 1, MPI_INT, 0,
MPI_COMM_WORLD);
```

- MPI_Scatter – реализует рассылку данных от корневого процесса ко всем остальным процессам.

Входные параметры:

- const void *sendbuf – указатель на отправляемые данные (значимо только для процесса root).
- int sendcount – количество блоков данных, отправляемых каждому процессу.
- MPI_Datatype sendtype – тип отправляемых данных (в нашем случае – байты).
- void *recvbuf – указатель на переменную, предназначенную для приема блоков данных.
- int recvcount – количество элементов, предназначенных для получения.
- MPI_Datatype recvtype – тип принимаемых данных.

- int root – ранг корневого процесса.
- MPI_Comm comm – коммуникатор.

Программный код:

```
// Распределение блоков данных между процессами
int blocks_per_proc = (num_blocks+world_size-1) / world_size;
// Рассылка блоков данных
std::vector<uint8_t> local_blocks(blocks_per_proc * 8);
MPI_Scatter(text_data.data(), blocks_per_proc*8, MPI_BYTE, local_blocks.data(), blocks_per_proc * 8, MPI_BYTE, 0, MPI_COMM_WORLD);
```

- MPI_Gather – собирает обработанные блоки данных с каждого процесса обратно на корневой процесс.

Входные параметры:

- const void *sendbuf – указатель на отправляемые данные с каждого процесса.
- int sendcount – количество отправляемых блоков от каждого процесса.
- MPI_Datatype sendtype – тип отправляемых данных (в нашем случае – байты).
- void *recvbuf – указатель на переменную, предназначенную для получения собранных блоков данных. (значимо только для процесса root).
- int recvcount – количество принимаемых блоков от каждого процесса.
- MPI_Datatype recvtype – тип принимаемых данных (в нашем случае – байты).
- int root – ранг получающего процесса (как корневой правило – 0).
- MPI_Comm comm – коммуникатор.

Программный код:

```
// Сбор зашифрованных блоков данных на корневом процессе
std::string encrypted_text(num_blocks * 8, '\0');
MPI_Gather(encrypted_blocks.data(), blocks_per_proc * 8, MPI_BYTE, const_cast<char*>(encrypted_text.data()), blocks_per_proc * 8, MPI_BYTE, 0, MPI_COMM_WORLD);
```

Преимущества высокоуровневой абстракции TPL

Task Parallel Library (TPL) – это компонент стандартной библиотеки .NET, предоставляющий высокоуровневую абстракцию для организации параллельных вычислений и асинхронного выполнения задач. В отличие от

низкоуровневых подходов, предполагающих явное управление потоками и синхронизацией, TPL работает в рамках общей памяти, где несколько задач или потоков могут обращаться к общим объектам. Это соответствует модели многопоточности на уровне процесса (внутри одного приложения), где управление потоками делегировано среде выполнения .NET. Такая архитектура упрощает разработку многопоточных приложений, снижает вероятность гонок, взаимных блокировок и других ошибок параллельного программирования, позволяя сосредоточиться на логике обработки данных.

В рамках реализации алгоритма шифрования Магма использование TPL позволяет эффективно распараллелить процесс обработки блоков данных без необходимости в явной организации обмена информацией между потоками. Каждый блок данных, представляющий собой 64-битную порцию исходного текста, обрабатывается независимо. Благодаря этому подходу достигается высокая степень масштабируемости при увеличении количества доступных вычислительных ресурсов, так как автономно вычисляется доступное количество ядер, на которые распределяются подаваемые блоки текста.

Высокоуровневая абстракция TPL обеспечивает автоматическое распределение задач между потоками, используя возможности пула потоков (ThreadPool) и механизмы динамического планирования. Это позволяет минимизировать накладные расходы на создание и уничтожение потоков, а также повысить эффективность использования вычислительных ядер. При этом синхронизация между задачами достигается посредством использования высокоуровневых конструкций, таких как Parallel.For, Parallel.ForEach, а также классов Task и Task<TResult>, которые предоставляют удобные средства управления зависимостями и работы с исключениями.

В данной реализации шифра Магма используется конструкция Parallel.For, позволяющая запускать параллельную обработку всех блоков данных.

Входные параметры:

- int fromInclusive – начальное значение итерации (включительно).
- int toExclusive – конечное значение итерации (исключительно).
- Action<int> body – делегат, описывающий логику, выполняемую на каждой итерации (получает индекс итерации).
- ParallelOptions parallelOptions (необязательно) – объект, содержащий параметры управления параллелизмом.
- Func<int, ParallelLoopState, TLocal, TLocal> body (необязательно) – функция, выполняемая для каждой итерации с доступом к индексу итерации, объекту управления выполнением, текущему значению локального состояния.

Программный код:

```
Parallel.For(0, myString_splited.Count, i =>
{
      byte[] enc = magma.Encrypt(myString_splited[i]);
});
```

Таким образом, использование Task Parallel Library в задаче шифрования предполагает высокую эффективность при минимальных накладных расходах на управление параллелизмом и синхронизацией в однопроцессорной.

Сравнение подходов параллельной реализации MPI и TPL

MPI, как низкоуровневая библиотека, ориентирована на распределенные вычислительные системы, где взаимодействие процессов осуществляется посредством явной передачи сообщений. Такой подход обеспечивает высокий уровень контроля над коммуникацией и синхронизацией, что делает MPI эффективным решением для построения масштабируемых параллельных систем. В контексте реализации алгоритма шифрования Магма, использование MPI позволяет каждому процессу выполнять автономную обработку подмножеств данных, при этом критические точки синхронизации ограничиваются начальными и завершающими коммуникационными операциями (MPI_Bcast, MPI_Scatter, MPI_Gather).

В противоположность этому, TPL предоставляет высокоуровневую абстракцию, работающую в рамках модели с общей памятью, которая особенно эффективна на многоядерных однопроцессорных системах. Благодаря задачно-ориентированной модели программирования TPL освобождает разработчика от необходимости явного управления потоками и синхронизацией. В задаче параллельного шифрования блоков данных алгоритма Магма, это позволяет минимизировать сложность кода и снизить вероятность ошибок, связанных с конкуренцией потоков. Использование таких конструкций, как Parallel.For и Task, обеспечивает автоматическое распределение нагрузки и эффективное использование ресурсов пула потоков, снижая накладные расходы на управление параллелизмом.

С точки зрения масштабируемости, MPI эффективен при работе с распределёнными вычислительными ресурсами и обеспечивает более тонкий контроль над взаимодействием процессов, что критично при проектировании высоконагруженных параллельных приложений, требующих минимизации времени коммуникаций. Однако эта гибкость сопровождается высокой сложностью разработки и необходимостью детальной проработки вопросов синхронизации и обмена сообщениями. TPL, напротив, оптимизирован для удобства разработки многопоточных приложений, предлагая разработчику более простой и интуитивно понятный интерфейс при сохранении высокой эффективности в условиях задач параллелизма данных на многоядерных однопроцессорных системах.

Сравнение ускорения шифрования при использовании MPI и TPL в однопроцессорной системе

В данной задаче шифрования алгоритм Магма применялся для обработки 1320 блоков данных, которые были разделены на части, соответствующие количеству доступных ядер (от 2 до 12). Время выполнения алгоритма на MPI и TPL для разных конфигураций количества ядер на одном процессоре «Intel Core i5-12450H» было измерено для анализа производительности каждой из технологий.

Результаты в табл. 1 показали, что использование TPL значительно ускоряет выполнение шифрования по сравнению с MPI при всех конфигурациях количества ядер. Время работы алгоритма с использованием TPL было меньше, чем с MPI, на всех тестируемых конфигурациях. Это можно объяснить рядом факторов, таких как более высокая степень абстракции и оптимизированное управление параллельными вычислениями в TPL в однопроцессорной системе.

Таблица 1

Время шифрования MPI и TPL

	MPI	TPL
12 ядер	0.829735 с	0.2464007 с
8 ядер	1.28065 с	0.3520778 с
6 ядер	2.02606 с	0.514035 с
4 ядра	3.04172 с	0.6665992 с
2 ядра	5.8386 с	1.0538048 с

Кроме того, TPL работает внутри одного процесса, где потоки выполняют независимые операции, и синхронизация между ними выполняется только на начальной и финальной фазой обработки данных. Это сводит к минимуму накладные расходы на коммуникацию и синхронизацию, что особенно заметно при небольшом числе ядер, где затраты на коммуникацию в MPI становятся более выраженными.

Таким образом ускорение, которое обеспечила TPL по отношению к MPI на разных конфигурациях ядер. Например, для 12 ядер ускорение TPL составило **3.37**, а для 2 ядер – **5.54**. Это подтверждает, что при меньшем числе ядер MPI сталкивается с большими накладными расходами на коммуникацию, что увеличивает общее время выполнения.

Результаты тестов демонстрируют, что для однопроцессорной системы, технология TPL имеет более высокую производительность для задачи шифрования в режиме простой замены.

Заключение

Алгоритм шифрования Магма был реализован с использованием двух различных параллельных подходов: низкоуровневой библиотеки MPI и высокоуровневой абстракции TPL. Задача заключалась в эффективной обработке 1320 блоков данных, где каждый блок представлял собой 64-битный фрагмент исходного текста. В обоих случаях задача была распараллелена на различные конфигурации ядер (от 2 до 12), с целью изучения производительности каждой из технологий в условиях многозадачности и параллельных вычислений.

MPI реализует параллелизм с использованием явной передачи сообщений между процессами, что предполагает взаимодействие между независимыми вычислительными единицами в распределенной памяти. В случае с алгоритмом Магма каждый процесс обрабатывает подмножество блоков данных, что устраняет зависимости между задачами и делает задачу идеально подходящей для параллельной обработки. Основным преимуществом MPI является гибкость и высокая степень контроля над распределением задач и синхронизацией. Однако в контексте данной задачи, где каждый процесс выполняет автономные вычисления, MPI требует синхронизации через операции: передача информации о количестве блоков (MPI_Bcast), рассылка блоков между процессами (MPI_Scatter) и сбор результатов (MPI_Gather).

TPL представляет собой высокоуровневую абстракцию, где управление потоками и синхронизацией делегируется внутренним механизмам среды выполнения .NET. В реализации с использованием TPL все блоки данных обрабатываются независимо, и синхронизация между задачами происходит только на начальных и конечных стадиях, что минимизирует необходимость в явной синхронизации. Одним из главных преимуществ TPL является автоматическое управление распределением блоков между потоками, без использования операций синхронизации, что значительно упрощает разработку и сокращает вероятность ошибок, связанных с конкуренцией и состояниями гонки.

Результаты тестов показали, что TPL продемонстрировал более высокую производительность по сравнению с MPI в задаче реализации алгоритма «Магма» в однопроцессорной системе. Время выполнения с TPL было меньше на всех конфигурациях, что связано с отсутствием необходимости в сложной синхронизации между процессами и минимальными накладными расходами на управление потоками. В MPI на больших числах ядер накладные расходы на коммуникацию и синхронизацию становятся более заметными, что увеличивает время выполнения. Например, в системе с 12-ядерным процессором TPL работает в **3,37** раза быстрее, чем MPI, а при использовании 2 ядер – в **5,54** раза быстрее.

Таким образом, можно сделать вывод, что TPL в однопроцессорной системе является более эффективным инструментом для реализации параллельных вычислений в задачах, подобных алгоритму шифрования Магма, благодаря своей простоте, высокой производительности и минимизации накладных расходов. В то время как MPI требует более сложной организации синхронизации, он сохраняет ключевое преимущество – возможность работы в распределённых системах, что делает его незаменимым при реализации параллелизма в условиях, где ресурсы распределены между несколькими узлами. TPL, в свою очередь, ограничен рамками одной машины и не подходит для распределённых вычислений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Документация MPI [Электронный ресурс] // mpi-forum.org: [сайт]. – URL: https://www.mpi-forum.org/ (дата обращения: 19.03.2025).
2. Документация Task Parallel Library (TPL) [Электронный ресурс] // docs.microsoft.com: [сайт]. – URL: https://docs.microsoft.com/en-us/dotnet/standard/parallel-programming/task-parallel-library-tpl (дата обращения: 19.03.2025).
3. Шифрование Магма: описание и реализация [Электронный ресурс] // cryptography.ru: [сайт]. – URL: https://cryptography.ru/articles/magma-encryption-algorithm (дата обращения: 19.03.2025).
4. Потоковые и параллельные вычисления в C++ [Электронный ресурс] // cppreference.com: [сайт]. – URL: https://en.cppreference.com/w/cpp/thread (дата обращения: 19.03.2025).
5. *Pizlo F., & Jang T.P.* Parallel Computing: Theory and Practice. – Cambridge University Press, 2018.
6. OpenMP API Specification [Электронный ресурс] // openmp.org: [сайт]. – URL: https://www.openmp.org/specifications/ (дата обращения: 19.03.2025).
7. *Хартли Дж.* Алгоритмы и структуры данных для параллельных вычислений. – М.: Изд-во ВШЭ, 2020. – 356 с.

УДК 004.056.2

А.Д. Эпитов, Е.А. Маро

Южный федеральный университет, Россия, г. Таганрог

МЕТОДЫ ИДЕНТИФИКАЦИИ И ИССЛЕДОВАНИЯ КРИПТОГРАФИЧЕСКИХ КОШЕЛЬКОВ

Анализ транзакционной активности и идентификация кошельков становятся ключевыми задачами для правоохранительных органов, служб финансового мониторинга и специалистов по информационной безопасности. В данной работе проведен детальный анализ атаки на криптовалютную биржу Bitfloor, в ходе которой было похищено значительное количество биткойнов, разделенных на пять транзакций для усложнения отслеживания. Используя инструмент Blockchain.com, выявлены временные метки и структура транзакций, каждая из которых имеет два выхода. Для более глубокого исследования применены OSINT-инструменты, такие как Wallet Explorer, Crystal и BitcoinWhosWho, что позволило установить связи между кошельками и выявить паттерны транзакций. Также рассмотрена атака на Ronin Bridge, произошедшая в марте 2022 года. Анализ транзакций с использованием Etherscan и Arkham Intelligence показал связь с хакерской группировкой Lazarus Group из Северной Кореи, а также выявил методы обналичивания средств через биржи, такие как Binance. Проведенное исследование подчеркивает важность знаний и навыков применения различных аналитических инструментов при расследовании преступлений, связанных с криптовалютными системами.

Ключевые слова: *блокчейн, OSINT, криптобиржа, Ronin, Bitfloor, инцидент информационной безопасности, анализ транзакций.*

The analysis of transactional activity and wallet identification have become key tasks for law enforcement agencies, financial monitoring services, and information security specialists. This research presents a detailed analysis of the attack on the cryptocurrency exchange Bitfloor, during which a significant amount of Bitcoin was stolen and divided into five transactions to complicate tracking. Utilizing the Blockchain.com tool, timestamps and transaction structures were identified, each containing two outputs. For a more in-depth investigation, OSINT tools such as Wallet Explorer, Crystal, and BitcoinWhosWho were employed, enabling the establishment of connections between wallets and the identification of transaction patterns. The study also examines the attack on Ronin Bridge that occurred in March 2022. Transaction analysis using Etherscan and Arkham Intelligence revealed links to the North Korean hacker group Lazarus Group and identified methods of cashing out funds through exchanges such as Binance. The research underscores the importance of knowledge and skills in applying various analytical tools when investigating crimes related to cryptocurrency systems.

Keywords: *blockchain, OSINT, cryptocurrency exchange, Ronin, Bitfloor, information security incident, transaction analysis.*

Введение

С ростом популярности криптовалют и расширением сферы их применения возрастает потребность в инструментах, обеспечивающих прозрачность и безопасность операций в блокчейн-среде. Анализ активности транзакций и идентификация кошельков становятся все более важными задачами – как для правоохранительных органов и служб финансового мониторинга, так и для исследователей, аналитиков и специалистов по информационной безопасности. Инструменты анализа криптовалютных кошельков позволяют выявлять связи между адресами, отслеживать транзакции, анализировать поведение участников сети, а также деанонимизировать кошельки, ассоциированные с биржами, сервисами или противоправной деятельностью. Современный рынок предлагает широкий спектр решений – от базовых обозревателей блокчейна до профессиональных аналитических платформ, использующих методы анализа графов и искусственного интеллекта. Для применения подходов по исследованию транзакций и идентификации криптокощельков, требуется провести сравнительный анализ функциональных возможностей различных инструментов идентификации криптовалютных кошельков и определить их применимость в зависимости от поставленных перед экспертом задач. Особый интерес представляет применение аналитических инструментов на практике – в частности, при расследовании инцидентов, связанных с атаками на криптовалютные биржи. Криптовалютные биржи часто становятся мишенью для злоумышленников из-за высокой концентрации цифровых активов и особенностей архитектуры хранения средств. После совершения атаки злоумышленники стремятся вывести похищенные средства на другие криптокошельки, разбить их на мелкие транзакции, использовать миксеры или пытаются иными путями легализовать активы. Несмотря на предпринятые меры маскировки, благодаря специализированным инструментам анализа имеется возможность отследить путь средств, выделить ключевые адреса и даже идентифицировать сервисы или организации, с которым данные адреса аффилированы. Рассмотрены реальные сценарии атак, на примере которых продемонстрирована практическая эффективность исследуемых инструментов анализа. Произведён поэтапный анализ транзакций, начиная с исходного адреса и заканчивая попытками маскировки и запутывания. На основе проведенного анализа транзакций выполнена оценка уровня детализации предоставляемой информации о транзакциях, удобства визуализации и проверка работоспособность функций исследуемых сервисов.

1. Атака на биржевой рынок Bitfloor

1.1. Описание атаки на Bitfloor и методы исследования

Для выполнения анализа методов исследования и идентификации криптовалютных кошельков в рамках OSINT, будет использована атака на Bitfloor, чтобы продемонстрировать как работает каждый из сервисов и показать их эффективность в настоящем расследовании. Атака на биржевой рынок Bitfloor, произошедшая 4 сентября 2012 года, стала одним из знаковых инцидентов в истории криптовалютных бирж. Злоумышленники смогли воспользоваться уязвимостью в системе безопасности платформы, получив доступ к базе данных, в которой хранились приватные ключи пользователей. Это привело к утечке значительного количества средств – 24 078,39 BTC, что по курсу на тот момент составляло 251 600 долларов США (при стоимости 1 BTC в 10,45 долларов) [1]. Впоследствии бирже так и не удалось полностью восстановиться после этого инцидента, и в 2013 году она прекратила свою работу. В процессе изучения атаки на Bitfloor я буду анализировать адреса кошельков, на которые были выведены украденные средства, а также исследовать цепочки транзакций, которые использовались для их дальнейшего перемещения. Это позволит не только выявить возможные связи между различными адресами, но и оценить, какие приемы использовали злоумышленники для сокрытия следов – будь то использование миксеров, транзакций через промежуточные кошельки или других методов анонимизации. Данное исследование позволит проверить эффективность существующих инструментов для анализа криптовалютных транзакций. Я буду использовать различные сервисы, применяемые в OSINT-расследованиях, чтобы определить, какие из них наиболее удобны и информативны для идентификации подозрительных адресов и отслеживания перемещений средств. Несмотря на анонимность, блокчейн остается открытой системой, где каждая транзакция записывается и может быть проанализирована. Это делает возможным выявление закономерностей и построение графов взаимодействий, что особенно полезно в расследованиях киберпреступлений. Опираясь на атаку на Bitfloor, я проведу комплексный анализ задействованных в ней криптовалютных кошельков и транзакций, проверяя работу различных OSINT-инструментов и оценивая их применимость в реальных расследованиях.

1.2. Описание атаки на Bitfloor и методы исследования

1.2.1. Blockchain.com

Путь украденных средств состоит из 5 транзакций [2].

blockchain.info/tx/83f3c30dc4fa25afe57b85651b9bbc372e8789d81b08d6966ea81f524e0a02be —16,120 BTC

blockchain.info/tx/d5d23a05858236c379d2aa30886b97600506933bc46c6f2aab2e05da85e61ad2 — 1,000 BTC

blockchain.info/tx/f9d55dc4b8af65e15f856496335a29e2be40f128a7374c75b75529e864579f93 — 6,400 BTC

blockchain.info/tx/42ea472060118ee5aee801cdedbc4a3403f3708a87340660f766e2669f0afeb0—60 BTC

blockchain.info/tx/358c873892016649ace8e9db4c59f98a6ca8165287ac80e80c52e621f5a26e46 — 498.39 BTC.

Разделение кражи на несколько транзакций могло способствовать сокрытию источника атаки и усложнению процесса ее выявления и остановки. Злоумышленник использовал разные адреса для каждой транзакции, чтобы затруднить отслеживание перевода средств. На рис. 1 изображено время передачи в сеть самой ранней транзакции.

Рис. 1. Время передачи в сеть первой транзакции

Последняя передача в сеть транзакции была в 7 часов 43 минуты 33 секунды 4 сентября 2012 года (на рис. 2 приведено самое позднее время передачи транзакции в сеть).

Рис. 2. Время передачи в сеть последней транзакции

Существует 2 блока, в которых транзакции добывались и были подтверждены.

Блок 197 114, в который входят транзакции 1 и 5, переданные в сеть в 7 часов 7 минут 39 секунд. И блок 197 115, в который входят транзакции 2,3,4, переданные в сеть в 7 часов 43 минуты 33 секунды.

Следующее, что привлекает внимание при исследовании всех 5 транзакций – это количество выходов равное 2 в каждой транзакции, как показано на рис. 3-7.

Рис. 3. Bifloor Hack 1

Рис. 4. Bifloor Hack 2

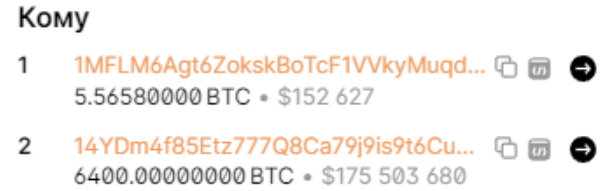


Рис. 5. Bifloor Hack 3

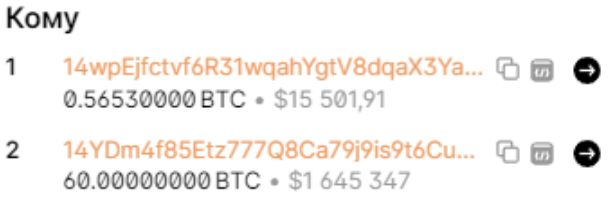


Рис. 6. Bifloor Hack 4

Рис. 7. Bifloor Hack 5

Стоит отметить, что в транзакциях Bitfloor Hack 3 и Bitfloor Hack 4 используется один и тот же адрес (в роли большего выхода). На рис. 8 и 9 показаны выходы транзакции Bitfloor Hack 3 и Bitfloor Hack 4 соответственно.

Рис. 8. Выходы транзакций Bitfloor Hack 3

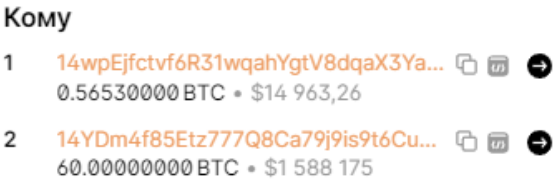


Рис. 9. Выходы транзакций Bitfloor Hack 4

Проанализируем адрес 14YDm4f85Etz777Q8Ca79j9is9t6Cu7rPj, как показано на рис. 10.

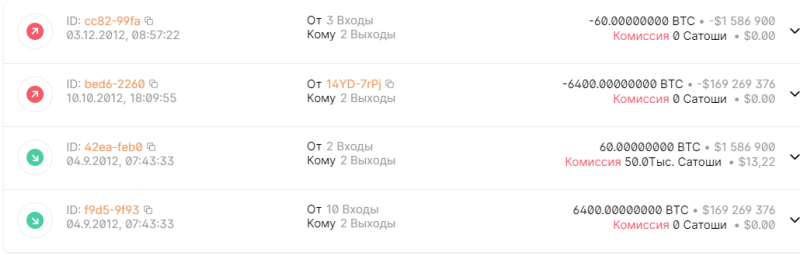


Рис. 10. Информация об адресе 14YDm4f85Etz777Q8Ca79j9is9t6Cu7rPj

Исходя из представленных данных, злоумышленник последние похищенные средства (учитывая все транзакции) списывал 03.12.2012 в 8:57:22. Была установлена комиссия только на Bitfloor Hack 4. Размер комиссии составил 0.00050000 BTC, как показано на рис. 11.

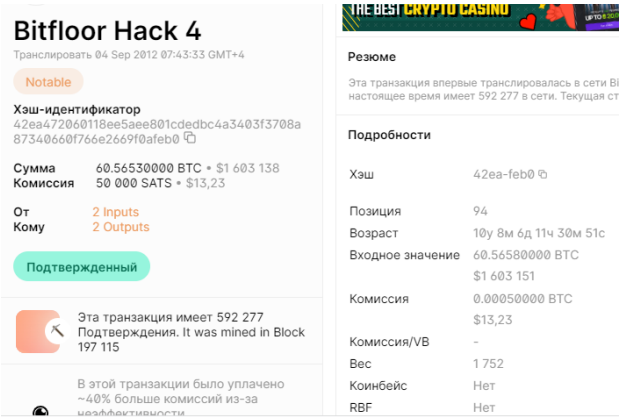


Рис. 11. Комиссия для Bitfloor Hack 4

1.2.2. Сервис Wallet Explorer

С помощью сервиса WalletExplorer [3] дополним информацию об адресе 14YDm4f85Etz777Q8Ca79j9is9t6Cu7rPj. Сервис WalletExplorer позволяет исследовать, какие кошельки владеют определенными криптовалютными средствами, изучать паттерны транзакций и выявлять связи между различными кошельками и пользователями. На рис. 12 показаны совершенные переводы, связанные с этим адресом.

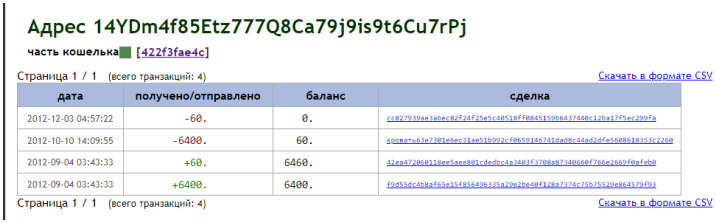
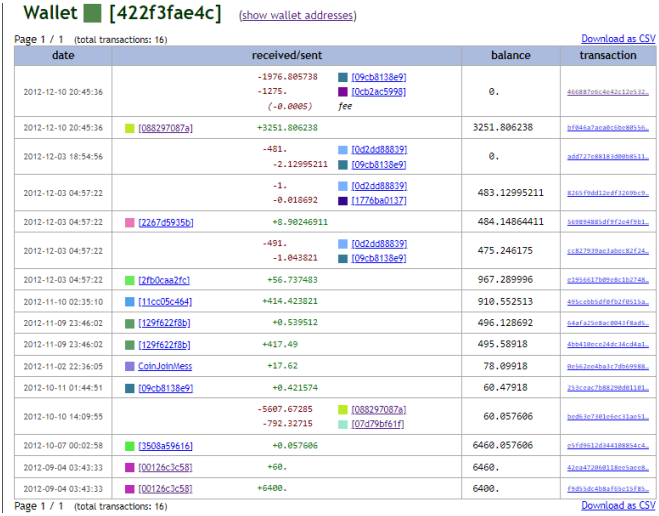


Рис. 12. Анализ кошелька с помощью сервиса WalletExplorer

На рис. 13 определен криптокошелек, который позволяет управлять своими криптовалютными активами, в то время как адрес – это уникальный идентификатор, который позволяет отправлять и получать криптовалютные транзакции в блокчейне. Исходя из проанализированных данных видно, что чаще всего переводы происходили на следующие кошельки: [09cb8138e9][1], [0d2dd88839][2].

[1] https://www.walletexplorer.com/wallet/09cb8138e9367996.
[2] https://www.walletexplorer.com/wallet/0d2dd8883978b0ff.



Wallet [422f3fae4c] (show wallet addresses)

Page 1 / 1 (total transactions: 16) Download as CSV

date	received/sent	balance	transaction
2012-12-10 20:45:36	-1976.805738 [09cb8138e9] -1275. [0cb2ac5998] (-0.0005) fee	0.	466887e6c4e42c12c532…
2012-12-10 20:45:36	[088297087a] +3251.806238	3251.806238	bf846a7aca8c8bc88b56…
2012-12-03 18:54:56	-481. [0d2dd88839] -2.12995211 [09cb8138e9]	0.	add727e88184d00b8311…
2012-12-03 04:57:22	-1. [0d2dd88839] -0.018692 [1776bba0137]	483.12995211	8269f0d12e6f32609bc9…
2012-12-03 04:57:22	[2267d5935b] +8.90246911	484.14864411	569894885df9f2e4f9b1…
2012-12-03 04:57:22	-491. [0d2dd88839] -1.043821 [09cb8138e9]	475.246175	cc8279392ac1abcc82f24…
2012-12-03 04:57:22	[2fb0caa2fc] +56.737483	967.289996	c19566178d92c8c1b2748…
2012-11-10 02:35:10	[11cc05c464] +414.423821	910.552513	495ccbbbdf0fb2f0513a…
2012-11-09 23:46:02	[129f622f8b] +0.539512	496.128692	64afa25e8ac8043f8ad5…
2012-11-09 23:46:02	[129f622f8b] +417.49	495.58918	4bb410ece24dc34cd4a1…
2012-11-02 22:36:05	CoinJoinWess +17.62	78.09918	8e162ee4ba1c7dfe6988…
2012-10-11 01:44:51	[09cb8138e9] +0.421574	60.47918	213ccac7b8829bd81181…
2012-10-10 14:09:55	-5607.67285 [088297087a] -792.32715 [07d79bf61f]	60.057606	bed61e7381e6cc31ac51…
2012-10-07 00:02:58	[3508a59616] +0.057606	6460.057606	e1fd9612d34418885fc4…
2012-09-04 03:43:33	[00126c3c58] +60.	6460.	42ea4720b0118ee5ace8…
2012-09-04 03:43:33	[00126c3c58] +6400.	6400.	f9b53dc4b8af63c15f85…

Page 1 / 1 (total transactions: 16) Download as CSV

Рис. 13. Информация о кошельках, используемых для вывода средств

Установим принадлежность адресов к кошелькам с помощью инструмента WalletExplorer. Для начала установим принадлежность адресов на малых выходах (рис. 14-18).

Bitfloor Hack 1 – малый выход (172Ztr7G4nRgvTjbtpMkUiNFnSNJy3vybJ)

Bitfloor Hack 2 – малый выход (1HWtDRYpo5p31squPsvWWfc2LEFcdChCKa)

Bitfloor Hack 3 – малый выход (1MFLM6Agt6ZokskBoTcF1VVkyMuqd82XBk)

Bitfloor Hack 4 – малый выход (14wpEjfctvf6R31wqahYgtV8dqaX3YanY8)

Bitfloor Hack 5 – малый выход (18ARVHSkQzr5egFZaCqmc2VFYXdpAinXbG)

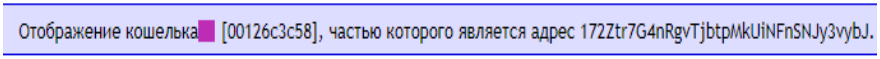


Рис. 14. Малый выход Bitfloor Hack 1

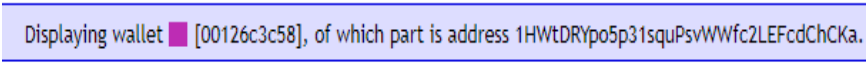


Рис. 15. Малый выход Bitfloor Hack 2

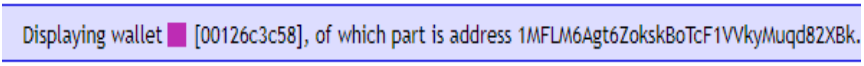


Рис. 16. Малый выход Bitfloor Hack 3

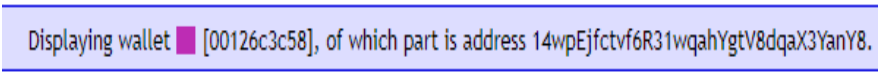


Рис. 17. Малый выход Bitfloor Hack 4

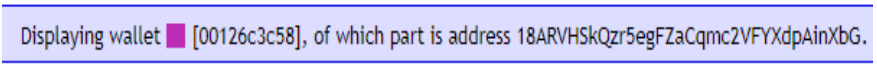


Рис. 18. Малый выход Bitfloor Hack 5

Далее установим принадлежность адресов на больших выходах, как показано на рис. 19-23.

Bitfloor Hack 1 – большой выход (1GU88GyRcxPTKdXbXEubsgPrrrt2c32Z4F)

Bitfloor Hack 2 – большой выход (1JkReEC6qDczSfmD5t2P9vCxcdj1Wotm9j)

Bitfloor Hack 3 – большой выход (14YDm4f85Etz777Q8Ca79j9is9t6Cu7rPj)

Bitfloor Hack 4 – большой выход (14YDm4f85Etz777Q8Ca79j9is9t6Cu7rPj)

Bitfloor Hack 5 – большой выход (12D5ytymtCW97NarFN61s81uM471LRf2W8)

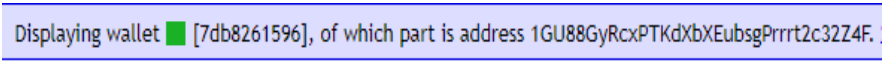


Рис. 19. Больший выход Bitfloor Hack 1

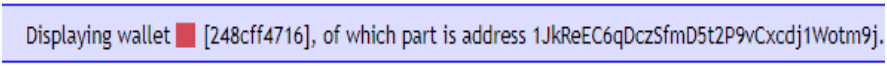


Рис. 20. Больший выход Bitfloor Hack 2

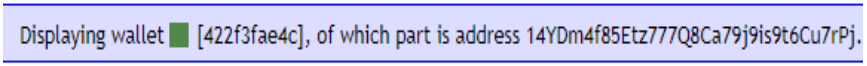


Рис. 21. Больший выход Bitfloor Hack 3

Displaying wallet [422f3fae4c], of which part is address 14YDm4f85Etz777Q8Ca79j9is9t6Cu7rPj.

Рис. 22. Больший выход Bitfloor Hack 4

Displaying wallet [c0ed5617a4], of which part is address 12D5ytymtCW97NarFN61s81uM471LRf2W8.

Рис. 23. Больший выход Bitfloor Hack 5

1.2.3. Сервис Crystal

Визуализируем транзакцию Bitfloor Hack 4 с помощью сервиса Crystal [4], который предназначен для аналитики и оперативной разведки для расширения возможностей финансовых учреждений, правительств и регулирующих органов в борьбе с криптовалютной преступностью. На рис. 24 показана визуализация транзакции Bitfloor Hack 4. Красная точка имеет адрес транзакции: 42ea472060118ee5aee801cdedbc4a3403f3708a87340660f766e2669f0afeb0.

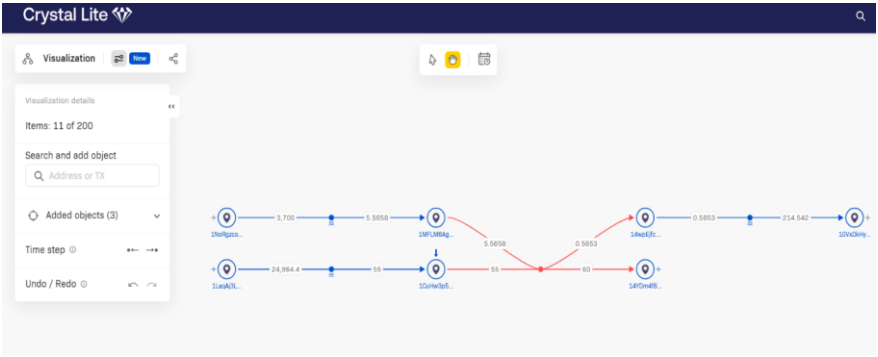


Рис. 24. Визуализация транзакции Bitfloor Hack 4

На рис. 25 показана дополнительная информация по транзакции, которую может предоставить сервис Crystal.

1.2.4. Сервис BitcoinWhosWho.com

BitcoinWhosWho – это сервис для анализа адресов, который помогает идентифицировать владельцев адресов – определять, кому принадлежит тот или иной биткоин-адрес (если он был ранее задокументирован), проверять на мошенничество – база данных содержит информацию о биткоин-адресах, связанных с мошенническими схемами, фишингом, вымогательством и другими незаконными действиями [5]. Помогает анализировать транзакции: предоставляет сведения о входящих и исходящих переводах, балансе и активности адреса, а также позволяет оставлять отзывы – пользователи могут комментировать и

добавлять информацию о подозрительных адресах. На рис. 26 показан результат проверки адреса 14YDm4f85Etz777Q8Ca79j9is9t6Cu7rPj на сервисе BitcoinWhosWho.

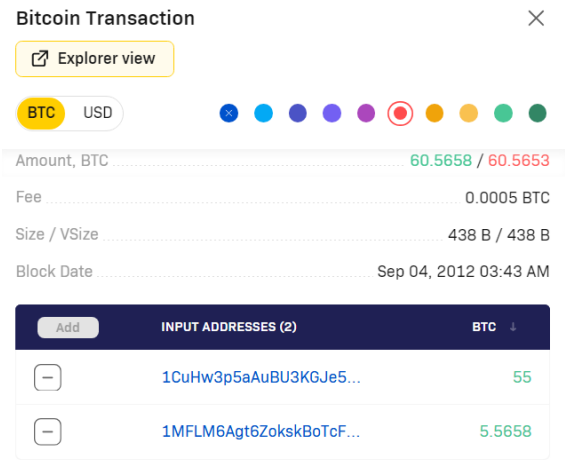


Рис. 25. Информация по транзакции в сервисе Crystal

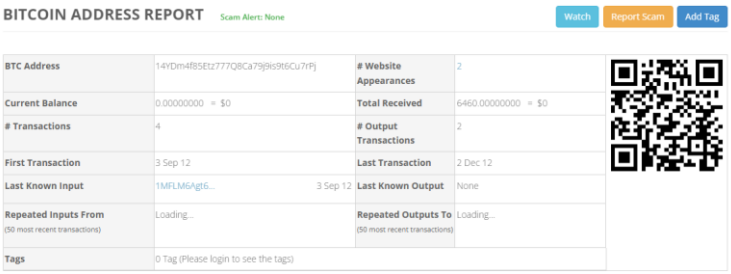
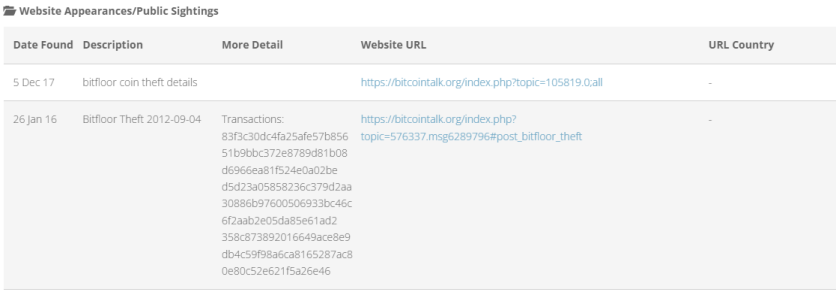


Рис. 26. Результат проверки кошелька в сервисе BitcoinWhosWho

На рис. 26 видно, что в результате проверки параметр **Scam Alert** задан с отметкой **None**. Это означает, что адрес проверяемого кошелька не подозревается в мошенничестве. Вероятнее всего, это связано с тем, что адрес кошелька может быть скрыт за сложной схемой, чтобы затруднить его анализ. В таких случаях сервис не позволяет однозначно не определить, является ли адрес подозрительным. Сервисы анализа адресов кошельков полагаются на различные источники данных для определения мошеннической активности. Если информация о мошеннической активности недоступ-

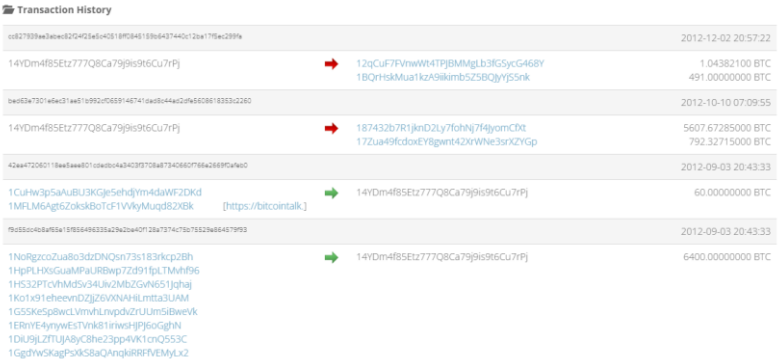
на или неполна в используемых источниках данных, сервис не обнаружит подозрительную активность. Также можно увидеть, что в строке «**Tags**» написано «0 tag». Это означает, что никто из пользователей не оставлял никаких тегов по данному адресу. На рис. 27 показаны источники, в которых упоминается данный адрес кошелька. Полученная история транзакций показана на рис. 28.



Website Appearances/Public Sightings

Date Found	Description	More Detail	Website URL	URL Country
5 Dec 17	bitfloor coin theft details		https://bitcointalk.org/index.php?topic=105819.0;all	-
26 Jan 16	Bitfloor Theft 2012-09-04	Transactions: 83f3c30dc4fa25afe57b85651b9bbc372e8789d81b08d6966ea81f524e0a02bed5d23a058582836c379d2aa30886b97600506933bc46c6f2aab2e05da85e61ad2358c873892016649ace8e9db4c59f98a6ca8165287ac80e80c52e621f5a26e46	https://bitcointalk.org/index.php?topic=576337.msg6289796#post_bitfloor_theft	-

Рис. 27. Источники, в которых встречается упоминание исследуемого адреса



Transaction History

cc827899ee3ebec82f4f25e5c40818ff0846159bb6437440c12ba17f5ec299fa			2012-12-02 20:57:22
14YDm4f85Etz777Q8Ca79j9is9t6Cu7rPj	→	12qCuF7FVnwWt4TPJBMMgtLb3fGSycG468Y 1BQrHskMua1kzA9ikimb5Z5BQjyYjS5nk	1.04382100 BTC 491.00000000 BTC
be0d3e7301e6e31ee51b992cf0669146741dad8c44ae2dfe5608618383cd260			2012-10-10 07:09:55
14YDm4f85Etz777Q8Ca79j9is9t6Cu7rPj	→	187432b7R1jknD2Ly7fohNj7f4JyomCfXt 17Zua49fcdoxEY8gwnt42XrWNe3srXZYGp	5607.67285000 BTC 792.32715000 BTC
42aa4720601188ea5aea801cdadbc4a3403f3708a87340660f766a2669f0a9a60			2012-09-03 20:43:33
1CuHw3p5aAuBU3KGje5ehdjYm4daWF2DKd 1MfLM6Agt6ZokskBoTcF1VVkyMuqd82XiBk [https://bitcointalk.]	→	14YDm4f85Etz777Q8Ca79j9is9t6Cu7rPj	60.00000000 BTC
f9d55cc4b8af68a15ff8864963335a29a2be40f128a7374c7bb78529a866479f93			2012-09-03 20:43:33
1NoRgzcoZua8o3dzDNQsn73s183rkcp2Bh 1HpPLHXsGuaMPaURBwp7Zd91fpLTMvhf96 1HS32PTcVhMdSv34Uiv2MbZGvN651Jqhaj 1Ko1x91eheevnDZJjZ6VXNAHiLmtta3UAM 1G55KeSp8wcLVmvhLnvpdvZrUUmSiBweVk 1ERnYE4ynywEsTVnk81iriwsHJPJ6oGghN 1DiU9jLZfTUJA8yC8he23pp4VK1cnQ553C 1GgdYwSKagPsXkS8aQAnqkiRRFfVEMyLx2	→	14YDm4f85Etz777Q8Ca79j9is9t6Cu7rPj	6400.00000000 BTC

Рис. 28. История транзакций исследуемого адреса

2. Атака на побочную блокчейн сеть Ronin

2.1. Описанием блокчейн сети Ronin и сценария атаки

Ronin – это побочная (sidechain) блокчейн-сеть, созданная специально для игры Axie Infinity, одной из крупнейших блокчейн-игр. Ronin не является частью Ethereum, но интегрирован через мост – это специальный смарт-контракт. Данный смарт-контракт состоит из функционала, с помощью кото-

рого у пользователя есть возможность переводить токены из Ethereum в Ronin и обратно. Если показать на примере, то пользователь отправляет ETH в Ethereum в Ronin Bridge, и получает эквивалент ETH в сети Ronin, токены блокируются на Ethereum, а в Ronin создаются "обёрнутые" аналоги (wrapped tokens). В табл. 1 показаны характеристики блокчейн сети Ronin.

Ronin стал жертвой атаки злоумышленников, так как проблема была не в Ethereum и не в смарт-контрактах, а в централизации Ronin. Чтобы максимизировать TPS (транзакций в секунду), децентрализация и отсутствие доверия были проигнорированы в пользу модели Proof of Authority, в которой всего девять валидаторов. Из этих девяти валидаторов для одобрения операций по депозитам и снятию средств необходим консенсус пяти. Четыре валидатора управляются Sky Mavis, а это значит, что в случае нарушения безопасности для управления сетью потребуется всего лишь одна дополнительная подпись. Хотя официальное оповещение сообщества не содержит подробностей о том, как были скомпрометированы валидаторы Sky Mavis, в нем указывается на уязвимость, которая позволила злоумышленникам получить контроль над требуемой пятой подписью. злоумышленники авторизовали два вывода, сняв сначала 173 600 ETH, а затем 25,5 млн USDC с контракта Ronin Bridge. 25,5 млн USDC были обменены на ETH через другие адреса, прежде чем были возвращены на основной кошелек [6]. В попытке усложнить поиск, 6250 ETH были переведены с кошелька, часть из которых с тех пор была переведена на FTX и Crypto.com. Адрес также изначально финансировался из Binance. Для подтверждения перевода с моста нужно было 5 из 9 валидаторов, хакеры скомпрометировали 4 валидатора Sky Mavis и 1 внешний, это дало им полный контроль, чтобы вывести 173,600 ETH и 25.5 млн USDC.

Таблица 1

Характеристики Ronin

Параметр	Значение
Тип	Sidechain (вспомогательная сеть Ethereum)
Создана	Компанией Sky Mavis
Запущена	2021 год
Поддерживает	ETH, USDC, AXS, SLP (игровые токены)
Цель	Снизить комиссии и ускорить транзакции для пользователей Axie Infinity
Консенсус	PoA (Proof of Authority) с ограниченным числом валидаторов

2.2. Разбор атаки на Ronin с помощью инструментов анализа криптокошельков

2.2.1. Инструмент Etherscan

Etherscan – это самый популярный и авторитетный блокчейн-эксплорер для сети Ethereum, дает возможность отслеживать транзакции, адреса, токены, смарт-контракты и многое другое [7]. Исходя из источников был найден хеш транзакции 0xc28fad5e8d5e0ce6a2eaf67b6687be5d58113e16be590824d6cfa1a94467d0b7, которая показана на рис. 29. Сервис Etherscan указывает на параметры данной транзакции, по которым видно, какой статус был у транзакции и каким образом были задействованы средства. Если обратить внимание на параметр Transaction Action, то в данном параметре отмечено, что Function by Ronin Bridge Exploiter on Axie Infinity: Ronin Bridge – говорит о том, что эту транзакцию инициировал злоумышленник и она связана с мостом Ronin, используемым для переноса активов между блокчейнами в экосистеме Axie Infinity. Стороны, вовлечённые в транзакцию указаны в параметре **From**: 0x098B716B8Aaf21512996dC57EB0615e2383E2f96 (Ronin Bridge Exploiter). Поле From соответствует адресу злоумышленника, который использовал уязвимость моста Ronin для выполнения операции. В параметре **To**: 0x1A2a1c938CE3eC39b6D47113c7955bAa9DD454F2 (Axie Infinity: Ronin Bridge) указан адрес контракта моста Ronin в экосистеме Axie Infinity. В деталях перевода можно увидеть сумму 173,600 ETH, что соответствует количеству эфира (ETH), которое было перемещено через мост. Объем переведенных средств представляет собой значительную сумму, что указывает на серьезность атаки на инфраструктуру моста Ronin. Поле From Wrapped Ether представляет собой токен Wrapped Ether (wETH), на который был выполнен перевод. Поля To Axie Infinity: Ronin Bridge – эти токены были направлены в контракт моста Ronin. Затем средства (173,600 ETH) были переведены обратно на адрес злоумышленника (Ronin Bridge Exploiter).

Далее была произведена вторая транзакция, то есть был совершен ещё один эпизод из цепочки атаки на (взлома) Ronin Bridge, который произошёл 23 марта 2022 года. В данном эпизоде злоумышленник (Ronin Bridge Exploiter) совершает вывод 25,500,000 USDC (стабильной монеты, привязанной к доллару США) с моста Ronin. Найдено ХЭШ значение транзакции в Etherscan xed2c72ef1a552ddaec6dd1f5cddf0b59a8f37f82bdda5257d9c7c37db7bb9b08, как показанаона рис. 30. Если смотреть по параметру Timestamp, то становится понятно, что данная транзакция была реализована 23 марта 2022 года, 13:31 UTC – через 2 минуты после транзакции с 173,600 ETH (предыдущая транзакция). Параметр **From**:0x1A2a1c938CE3eC39b6D47113c7955bAa9D D454F2 – это смарт-контракт моста Ronin (Axie Infinity: Ronin Bridge). Параметр **To:** 0x098B716B8Aaf21512996dC57EB0615e2383E2f96, это адрес злоумышленника – Ronin Bridge, который участвовал в крупнейшем взломе

моста Ronin. В этой конкретной транзакции он получил 25.5 млн USDC, отправленных напрямую с контракта моста Axie Infinity. Это была вторая часть серии транзакций (первая – с 173,600 ETH), проводимых в ходе одного и того же взлома.

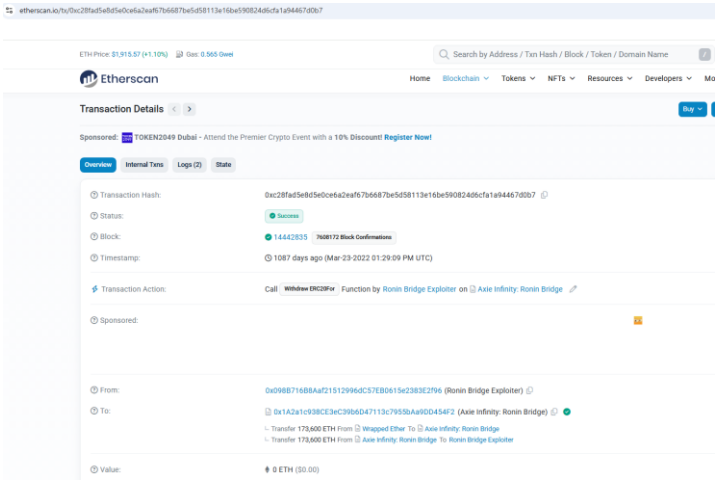


Рис. 29. ХЕШ-значение транзакции 0xc28fad5e8d5e0ce6a2eaf67b6687be5d58113e16be590824d6cfa1a94467d0b7

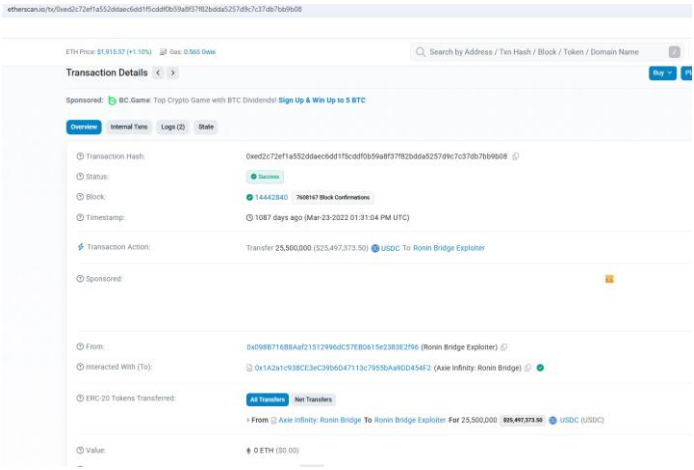


Рис. 30. ХЕШ-значение транзакции 0xed2c72ef1a552ddaec6dd1f5cddf0b59a8f37f82bdda5257d9c7c37db7bb9b08

На рис. 31 показан адрес кошелька: 0xe708f17240732bBfa1BaA8513F66b665Fbc7ce10. Адрес был профинансирован напрямую от атакующего Ronin Bridge, то есть это дочерний кошелёк злоумышленника. Этот адрес – вспомогательный кошелёк, использованный в процессе атаки, всего задействовано 6 транзакций. Была попытка временно замаскировать происхождение средств, но после этого они были переведены обратно.

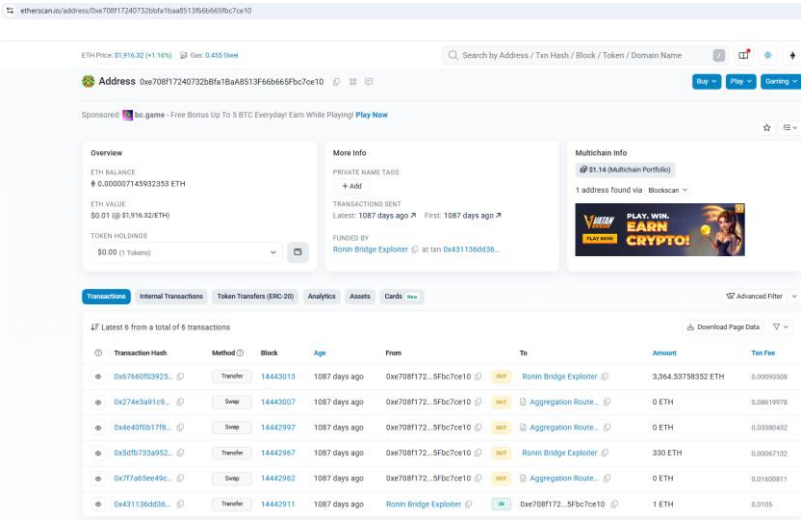


Рис. 31. Адрес кошелька 0xe708f17240732bBfa1BaA8513F66b665Fbc7ce10

На рис. 32 показан адрес злоумышленника 0x098B716B8Aaf21512996dC57EB0615e2383E2f96, связанный с крупнейшей атакой (взломом) Ronin Bridge. В тегах указано, что адрес внесён в санкционный список OFAC (Министерство финансов США) с тегом OFAC-Sanctioned. Используется тег «blocked», который показывает, что активность по данному адресу заблокирована на большинстве платформ. Учитывая, что на пике атаки было 173,600 ETH, а остаток минимален – большая часть средств была перемещена, обналичена, отмыта или заморожена. Анализируемый адрес был изначально пополнен с биржи Binance через адрес Binance 20, то есть злоумышленник зарегистрировал аккаунт на Binance для легального пополнения. Надпись в красной рамке говорит о том, что данный адрес был задействован при взломе Ronin Bridge.

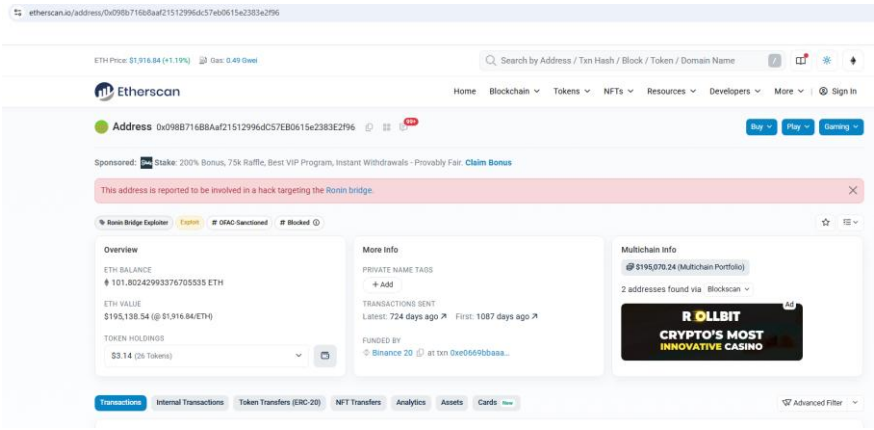


Рис. 32. Адрес злоумышленника, связанный с крупнейшим атакой на Ronin, 0x098B716B8Aaf21512996dC57EB0615e2383E2f96

2.2.2. Инструмент Arkham Intelligence

Arkham Intelligence – это блокчейн-аналитическая платформа, специализирующаяся на деанонимизации и отслеживании криптовалютных транзакций [8]. С помощью Arkham Intelligence можно связать адреса кошельков с реальными организациями, биржами, фондами, трейдерами и другими субъектами. Через данную платформу осуществлен анализ определенного ранее кошелька злоумышленника, который был проверен в сервисе Etherscan. На рис. 33 показан анализ адреса злоумышленника – 0x098B716B8Aaf21512996dC57EB0615e2383E2f96 на платформе Arkham Intelligence. В данной платформе используются аналогичные инструменту Etherscaner теги. При анализе данного кошелька показаны использованы теги: Suspicious (подозрительный), Hacker (хакер), OFAC Sanctioned (санкционный список OFAC (Министерство финансов США)), Banned by USDC, Banned by USDT. В результате проверки кошелька инструментом Arkham Intelligence указано, что данный кошелек подписан платформой как «Lazarus Group: Ronin Bridge Exploiter (OFAC Sanctioned)», это означает, что адрес кошелька 0x098B716B8Aaf21512996dC57EB0615e2383E2f96 напрямую связан с хакерской группировкой Lazarus Group из Северной Кореи [9].

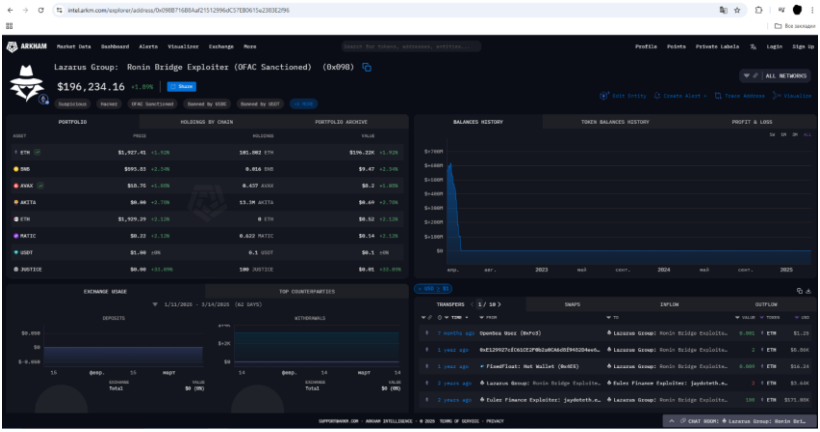


Рис. 33. Проверка 0x098B716B8Aaf21512996dC57EB0615e2383E2f96 в Arkham Intelligence

На рис. 34 показан анализ вывода средств с адреса злоумышленника. Почти все средства были выведены на Binance, что являлось попыткой обналичить средства, также были задействованы FixedFloat – децентрализованный обменник с возможностью анонимного обмена и Hotbit – CEX-биржа.

Рис. 34. Анализ вывода средств в Arkham Intelligence

На рис. 35 показан TOP COUNTERPARTIES – это список, который указывает, какие основные контрагенты были задействованы при взломе, а также количество транзакций, на первом месте расположен Lazarus Group с 31 транзакцией и суммой 563 миллиона долларов. На рис. 36 показан график истории баланса исследуемого кошелька.

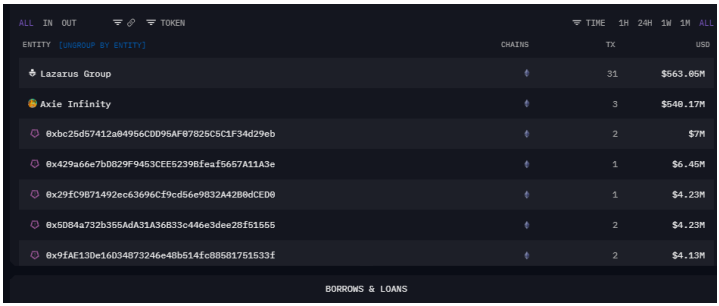


Рис. 35. Список TOP COUNTERPARTIES исследуемой атаки на Ronin

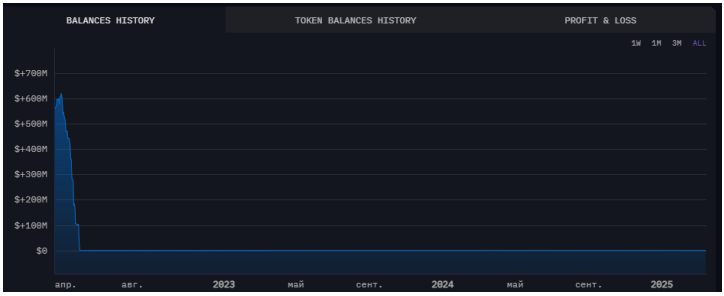


Рис. 36. График баланса исследуемого кошелька

3. Сравнительная характеристика инструментов для анализа криптовалютных кошельков

В табл. 2 приведена полученная в ходе исследовательской работы сравнительная характеристика инструментов для анализа криптовалютных кошельков, которая содержит метрики, исходя из которых можно оценить, какой инструмент исследования следует применять для различных целей в рамках OSINT подхода.

Для сравнительной оценки используемых инструментов в проведенном исследовании выбраны следующие метрики:

1. Поддерживаемые сети: перечислены криптовалюты, с которыми работает каждый инструмент. Например, Blockchain.com поддерживает Bitcoin и Ethereum, в то время как Arkham Intelligence охватывает BTC, ETH и другие сети.

2. Идентификация владельцев: указано, насколько эффективно каждый инструмент может идентифицировать владельцев кошельков. Некоторые инструменты, такие как Wallet Explorer и Arkham Intelligence, предлагают полную идентификацию, в то время как другие имеют ограниченные возможности.

3. Визуализация транзакций: отмечено, предоставляет ли инструмент графическую визуализацию транзакций. Crystal и Arkham Intelligence предлагают графы связей, в то время как другие инструменты не имеют этой функции.

4. Цена/Доступ: все перечисленные инструменты доступны бесплатно, но некоторые из них имеют ограничения на функциональность.

5. Целевая аудитория: указаны основные группы пользователей для каждого инструмента. Например, Wallet Explorer ориентирован на исследователей, а Arkham Intelligence – на аналитиков.

6. Доступность (интерфейс): описана доступность интерфейса, где большинство инструментов имеют открытый веб-интерфейс, но некоторые требуют авторизации для доступа к полному функционалу.

Проведенное исследование позволяет быстро оценить функциональные возможности и целевую аудиторию различных инструментов анализа криптовалют, что способствует быстрому определению наиболее подходящих инструментов в зависимости от потребностей пользователей.

Таблица 2

Сравнение инструментов для анализа криптовалютных кошельков

Метрика	**Blockchain .com**	**Wallet Explorer**	**Crystal**	**BitcoinWhos Who.com**	**Etherscan**	**Arkham Intelligence**
Поддерживаемые сети	Bitcoin, Ethereum	Bitcoin	BTC, ETH	Bitcoin	Ethereum	BTC, ETH, другие
Идентификация владельцев	Частично	Да	Частично	Да	Частично (биржи и контракты)	Да (деанонимизация)
Визуализация транзакций	Нет	Нет	Да (граф связей)	Нет	Да	Да
Цена/Доступ	Бесплатно	Бесплатно	Бесплатно (ограничено)	Бесплатно	Бесплатно	Бесплатно (ограничено)
Целевая аудитория	Широкая	Исследователи	Аналитики	Широкая	Пользователи, разработчики	Аналитики
Доступность (интерфейс)	Открытый, веб-интерфейс	Открытый простой веб-интерфейс	Открытый, с авторизацией	Открытый, просто веб-интерфейс	Открытый, расширенный	Открытый, с авторизацией

Заключение

Проведен подробный анализ атаки на Bitfloor, включая описание транзакций, использованных в процессе кражи, и применение различных OSINT-инструментов для исследования криптовалютных кошельков. В результате атаки было похищено значительное количество биткойнов, разделенных на несколько транзакций для затруднения отслеживания. Выделено пять основных транзакций, каждая из которых использует разные адреса для усложнения анализа. Произведен анализ транзакций с помощью инструмента Blockchain.com, в результате которого обнаружено, что все транзакции имеют по два выхода, определены временные метки атаки: первая транзакция была передана в сеть 4 сентября 2012 года, последняя – 3 декабря 2012 года. Для исследования атаки были использованы следующие OSINT-инструменты: Wallet Explorer, Crystal, BitcoinWhosWho. Wallet Explorer позволил исследовать связи между кошельками и выявить паттерны транзакций, в результате обнаружены адреса, на которые чаще всего переводились средства. Инструмент Crystal применялся для визуализации транзакций, что помогает исследователю в анализе и выявлении связей между адресами. Инструмент BitcoinWhosWho позволяет проводить проверку адреса на наличие мошеннической активности, в результате проверки исследуемый адрес не имеет отметок о мошенничестве, что может указывать на сложную схему сокрытия.

Атака на Ronin Bridge, произошедшая в марте 2022 года, стала одной из самых значительных в истории криптовалют, затронув экосистему Axie Infinity. Основные аспекты этой атаки можно рассмотреть через призму уязвимостей, связанных с централизацией и недостатками в механизме консенсуса. Злоумышленники смогли получить доступ к необходимым валидаторам и авторизовать вывод средств. В результате были украдены 173,600 ETH и 25.5 млн USDC. Эти средства были переведены через различные адреса, чтобы скрыть их происхождение, что указывает на тщательно спланированную атаку. Используя инструменты анализа, такие как Etherscan и Arkham Intelligence, можно отследить транзакции, связанные с атакой. Например, транзакция с хеш 0xc28fad5e8d5e0ce6a2eaf67b6687be5d58113e16be590824d6cfa1a94467d0b7 показала, что средства были переведены от контракта моста Ronin к адресу злоумышленника. Аналогично, вторая транзакция с хеш 0xed2c72ef1a552ddaec6dd1f5cddf0b59a8f37f82bdda5257d9c7c37db7bb9b08 подтвердила вывод 25.5 млн USDC. Анализ адреса злоумышленника с помощью Arkham Intelligence показал, что адрес связан с хакерской группировкой Lazarus Group из Северной Кореи. Это подтверждается используемыми тегами, такими как "Suspicious", "Hacker" и "OFAC Sanctioned". Большая часть украденных средств была выведена на биржи, такие как Binance, что указывает на реализацию обналичивания средств.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Bitcoin, криминальные хроники: Bitfloor PWND! – URL: https://habr.com/ru/articles/151034/ (дата обращения: 15.03.2025).
2. Официальный сайт блокчейн-обозревателей Blockchain.com. – URL: https://www.blockchain.com/ (дата обращения: 15.03.2025).
3. Сервис анализа транзакций и адресов в сети Bitcoin – WalletExplorer. – URL: https://www.walletexplorer.com/ (дата обращения: 15.03.2025).
4. Онлайн-платформа для анализа и отслеживания криптовалютных транзакций и адресов – Crystal Lite – URL: https://lite.crystalintelligence.com/ (дата обращения: 15.03.2025).
5. Онлайн-ресурс по идентификации владельцев биткоин-адресов – BitcoinWhosWho. – URL: https://www.bitcoinwhoswho.com/ (дата обращения: 15.03.2025).
6. Ronin Network – REKT. – URL: https://rekt.news/ronin-rekt/ (дата обращения: 15.03.2025).
7. Онлайн-сервис Etherscan. – URL: https://etherscan.io/ (дата обращения: 15.03.2025).
8. Платформа Arkham Intelligence. – URL: https://intel.arkm.com/ (дата обращения: 15.03.2025).
9. North Korea Designation Update (OFAC's SDN List). – URL: https://ofac.treasury.gov/recent-actions/20220414 (дата обращения: 15.03.2025).

УДК 004

Р.М. Яппаров, А.Р. Вафин

Уфимский университет науки и технологий, Россия, г. Уфа

К ВОПРОСУ О ЗАКОНОДАТЕЛЬНОМ ЗАКРЕПЛЕНИИ ПОНЯТИЯ «ЭТИЧНЫЙ ХАКЕР»

Статья посвящена актуальной на сегодняшний день проблеме, а именно определению правового статуса этичного хакера в российском законодательстве. Целью исследования является предложения по обоснованию необходимости законодательного закрепления правового положения этичного хакера. В содержании статьи проведено анализа нормативно-правовых актов в сфере информационного законодательства РФ. На основании проведенного исследования сделан соответствующий вывод о необходимости легализации деятельности этичных хакеров, предложены решения, закрепляющие их правовое положение.

Ключевые слова: *этичный хакер, нормативно-правовой акт, информационная безопасность, защита информации, Уголовный кодекс Российской Федерации, правовой статус.*

This article addresses a pressing issue: defining the legal status of ethical hackers in Russian law. The aim of the study is to propose a justification for the need for legislatively enshrining the legal status of ethical hackers. The article analyzes regulatory legal acts in the field of information law in the Russian Federation. Based on the research, a corresponding conclusion is reached regarding the need to legalize the activities of ethical hackers and solutions are proposed to enshrine their legal status.

Keywords: *ethical hacker, regulatory legal act, information security, information protection, Criminal Code of the Russian Federation, legal status.*

Сегодня вопрос информационной безопасности является одним из ключевых в развитии общества и государства. Со временем информация, приобретя самостоятельный статус, переросла из характеристики предметов в один из главных ресурсов человечества. Поэтому её защита является приоритетным направлением в обеспечении информационной безопасности.

В 2023 году количество кибератак на российские информационные системы увеличилось на 65% по сравнению с прошлым годом [1]. Самые серьезные угрозы исходят от международных хакерских группировок, которые находят слабые места в IT-инфраструктуре и цифровых платформах, используя современные методы киберразведки. Их стратегии проникновения в информационную систему непрерывно эволюционируют, а средства для проведения атак становятся все более продвинутыми.

Защитой информации занимаются соответствующие специалисты. В их число входят и «этичные хакеры». Также их еще называют «белыми хакерами» (пентестерами). Этичные хакеры занимают важную роль в обеспечении информационной безопасности объектов информатизации. В настоящее время их правовое положение не определено.

Термин "этичный хакер" не имеет четкого юридического определения. Обычно так называют специалистов по информационной безопасности, которые используют свои знания для поиска и устранения уязвимостей в системах с согласия их владельцев, предотвращая тем самым утечку данных и мошеннические действия. Основная цель таких профессионалов – проведение этичного взлома для выявления слабых мест и способов их устранения, что способствует повышению уровня информационной безопасности. Для этого они применяют те же методы, что и злоумышленники, однако вместо использования найденных уязвимостей, они предлагают рекомендации по их устранению, помогая компаниям усилить защиту своих систем.

Уместно провести сравнение с другими видами хакеров. Помимо белых существуют также «чёрные» и «серые».

Чёрный хакер – это хакер, который проводит несанкционированный взлом информационных систем, чтобы получить личную выгоду. Действуют соответственно противозаконно.

Серые хакеры – хакеры, которые могут действовать как в законных, так и в незаконных целях. Их мотивы могут варьироваться от любопытства до финансовой выгоды.

Разобравшись с видами хакеров, можно перейти к вопросу, который касается действий этичных хакеров. Из вышесказанного, можно сделать вывод о том, что деяния «белых» хакеров направлены в положительную сторону, в отличии от других «черных» и «серых» хакеров. Проблема состоит в том, что способы, методы и средства работы таких специалистов не отличаются от аналогичных, применяемых злоумышленниками. Следовательно, правовой статус этичного хакера равен правовому статусу его визави. В судебной практике встречается множество примеров, когда законопослушным специалистам по информационной безопасности был вынесен обвинительный приговор суда на несанкционированный доступ.

Сегодня деятельность «белых» хакеров не запрещена, но и не разрешена, то есть, не регламентирована. К ним применяют те же правовые нормы, что и для киберпреступников. Из-за этого возникают проблемы обеспечения информационной безопасности [3].

В действующем законодательстве нет определения для специалистов по кибербезопасности, которые по заказу организации тестируют защищенность ее инфраструктуры, ПО и систем для выявления уязвимостей. Соответственно, не закреплены в правовом поле такие формы тестирования, как

«пентест» и «баг-баунти» [6], не описаны их процедуры и инструменты. Правовая оценка деятельности «белых» хакеров неоднозначна, а риски высоки, вплоть до лишения свободы в рамках уголовной ответственности.

Уместно провести анализ основного закона, который регламентирует виды уголовной ответственности для специалистов по тестированию на проникновение. Этот закон, который ограничивает деятельность для пентестеров. Этим законом является Глава 28 УК РФ «Преступления в сфере компьютерной информации». Конечно, существует много других законов, которые так или иначе связаны с защитой информации, но именно по Главе 28 совершаются разбирательства, которые касаются деятельности хакеров [2].

Ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». Статья 272 УК РФ устанавливает ответственность за неправомерный доступ к компьютерной информации, который включает в себя ознакомление, копирование, блокирование, модификацию или уничтожение информации без согласия владельца. Для состава преступления необходимо наличие всех трех признаков: незаконный доступ, последствия (уничтожение, блокирование, модификация или копирование информации) и причинная связь между ними. Незаконный доступ может быть осуществлен через проникновение в компьютерные системы, использование специальных программных средств или незаконное использование паролей. Недостаточно просто проникнуть в систему, необходимо также причинить ущерб информации.

Ст. 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ». Объективная сторона состава преступления, предусмотренного ст. 273 УК РФ, выражается в создании, распространении или использовании компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, – вредоносных компьютерных программ либо иной компьютерной информации. Основной состав преступления сконструирован как формальный. Ответственность установлена за сам факт создания, распространения или использования вредоносных компьютерной программы или иной компьютерной информации. Наступления последствий для признания деяния оконченным не требуется. В законе говорится о создании, распространении или использовании вредоносных компьютерных программ или иной компьютерной информации. Компьютерная программа – это объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств, в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Ст. 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». Объективная сторона состава преступления, предусмотренного ст. 274 УК РФ, включает три обязательных признака: 1) деяние – нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям; 2) последствия – уничтожение, блокирование, модификация либо копирование охраняемой законом информации, причинившее крупный ущерб; 3) причинную связь между деянием и последствиями. Диспозиция статьи является бланкетной. Она отсылает к инструкциям и положениям, устанавливающим правила эксплуатации средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям.

Ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». На территории Российской Федерации с 1 января 2018 года действует Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Предметом всех предусмотренных ст. 274.1 УК РФ преступлений являются как компьютерная информация, которая содержится в критической информационной инфраструктуре, так и объекты инфраструктуры в виде информационных систем, информационно-телекоммуникационных сетей, а также автоматизированных систем управления. Объективная сторона состава преступления, предусмотренного ч. 1 ст. 274.1 УК РФ, выражается в создании, распространении и (или) использовании вредоносных компьютерных программ либо иной компьютерной информации. Она полностью совпадет с объективной стороной состава преступления, предусмотренного ст. 273 УК РФ.

Ст. 274.2 «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования». К нему относят нарушение порядка установки, эксплуатации и модернизации в сети связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования либо несоблюдение технических условий их установки или требований к сетям связи при использовании указанных технических средств, совершенные должностным лицом или индивидуальным предпринимателем.

Практически все инструменты, используемые этичным хакером, находятся вне закона, что вынуждает многих пентестеров работать анонимно. В настоящее время в качестве временной меры, гарантирующей определённые обязательства для обеих сторон подписываются трудовой договор, где оговариваются обстоятельства и иные вопросы по работе специалиста. Этот документ уточняет правовые взаимоотношения между специалистом по тестированию и компанией. Без него любой пентестер может быть привлечён к уголовной ответственности согласно действующим статьям Уголовного кодекса.

Даже штатный сотрудник компании, занимающийся информационной безопасностью, рискует оказаться под судом за использование нелегального программного обеспечения, если это было сделано с целью защиты или расследования инцидента. Поэтому работодателю или заказчику необходимо предельно чётко прописывать права, обязанности и ответственность привлекаемого специалиста в договоре и сопутствующих документах [5]. Однако даже такие меры не исключают риски наступления юридической ответственности.

Существуют, множество примеров из судебной практики, когда сотруднику отдела информационной безопасности был вынесен обвинительный приговор суда со всеми вытекающими последствиями. Такие случаи редки, но показательны.

Необходимо упомянуть о том, что компания, которая нанимает сотрудника для проведения этичного хакинга, обязана иметь лицензию ФСТЭК России на техническую защиту конфиденциальных данных, включающую в себя:

- услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
- услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

Наличие этих пунктов в лицензии – обязательное условие. Все требования к лицензиатам ФСТЭК прописаны в постановлении Постановление Правительства РФ от 3 февраля 2012 г. №79 «О лицензировании деятельности по технической защите конфиденциальной информации».

Одним из направлений практической реализации правового статуса этичного хакера является Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14

сентября 2022 № 525н. В нём впервые дано толкование о разграничениях трудовых функций специалистов по защите информации в автоматизированных системах, по сути дела упомянут тот самый этичный хакинг, но под другой трактовкой.

В этом вопросе интересен опыт зарубежных стран. Их законодательство направлено на легализацию деятельности «белых» хакеров, а также на раскрытие информации об анонимах. Во многих странах активно поддерживается стремление быть открытыми и публичными. Приветствуются специалисты по кибербезопасности, которые делятся такого рода информацией с остальными через социальные сети и профессиональные платформы. То есть, если «белый» хакер действует в пределах установленных правил, ему нечего опасаться – его защищают законы. Любые действия, выходящие за эти рамки, могут рассматриваться как нарушение, хотя наказания для участников программ баг-баунти обычно менее суровы.

В 2022 году Министерство юстиции США заявило, что в соответствии с Законом о компьютерном мошенничестве и злоупотреблении (CFAA), оно перестанет преследовать добросовестных хакеров, стремящихся повысить уровень безопасности. Это изменение в политике было названо историческим событием [4].

Несмотря на существующее неоднозначное положение дел в сфере обеспечения информационной безопасности, требуется еще множество комплексных решений по дальнейшему закреплению правового статус этичного хакера в российском законодательстве. Именно из-за этого добросовестные хакеры желают оставаться в анонимном статусе, чтобы обезопасить себя от обвинений в нарушении закона. Данный положение дел ограничивает их возможности и в следствие дает выигрыш хакерам со злым умыслом. Необходимо в ближайшей перспективе разработать и принять соответствующие законы, регламентирующие правовой статус этичного хакера. Практика поможет сделать это в нашей стране. Эти нормативно-правовые акты помогут поднять уровень информационной безопасности, а, следовательно, и национальной безопасности ы целом.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Каверин Д.* Вице-премьер Чернышенко заявил о росте на 65% числа кибератак на информационные системы РФ // Сайт «www.gazeta.ru». – https://www.gazeta.ru/tech/№ews/2023/03/03/19878991.shtml (дата обращения: 01.12.2024).
2. *Попов А.Н.* Преступления в сфере компьютерной информации // Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации. – 2018. – С. 21-42.
3. *Жигулин Г.П.* Организационное и правовое обеспечение информационной безопасности. – СПб.: СПб НИУ ИТМО, 2014. – С. 109-112.

4. *Coker J.* DoJ: White Hat Hackers Will №o Lo№ger Face Prosecutio№» // Сайт «www.i№fosecurity-magazi№e.com. – https://www.i№fosecurity-magazi№e.com/№ews/doj-white-hat-hackers-prosecutio№/ (дата обращения: 03.12.2024).
5. Постановление Правительства РФ от 15 июля 2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)».
6. Что такое баг-баунти. Журнал Яндекс Практикума Код. – https://thecode.media/bug-bounty/.

УДК 004

Р.М. Яппаров, В.Ф. Ахмадиева, В.Ф. Ахмадиева

Уфимский университет науки и технологий, Россия, г. Уфа

ИСПОЛЬЗОВАНИЕ ПЛАТФОРМЫ ПО ОСУЩЕСТВЛЕНИЮ ФИШИНГОВЫХ АТАК ДЛЯ ОБУЧЕНИЯ ПЕРСОНАЛА ОСНОВАМ КИБЕРБЕЗОПАСНОСТИ

Целью данного исследования является разработка и внедрение платформы для повышения осведомленности сотрудников о киберугрозах, в частности о фишинговых атаках, с использованием симуляционных методов на базе дистрибутива Linux. Актуальность работы обусловлена растущим числом кибератак, направленных на получение конфиденциальной информации через фишинг, что требует повышения уровня компетентности сотрудников в области кибербезопасности. Основные задачи исследования включают: анализ современных методов фишинговых атак, проектирование платформы для симуляции атак, разработку обучающих сценариев и оценку эффективности обучения сотрудников. В рамках исследования предложен подход, основанный на создании контролируемой среды для обучения, где сотрудники могут безопасно изучать методы атак и развивать навыки их распознавания. Использование платформы позволяет моделировать реалистичные сценарии фишинговых атак, такие как почтовый фишинг, веб-сайт фишинг и вредоносный фишинг, что способствует повышению осведомленности и формированию культуры безопасности в организации. Результаты исследования показали, что обучение с использованием симуляционных методов значительно повышает способность сотрудников распознавать фишинговые атаки и снижает риск успешного проникновения злоумышленников. Внедрение подобной платформы позволяет не только минимизировать убытки, связанные с кибератаками, но и повысить общий уровень кибербезопасности организации. В заключение подчеркивается важность регулярного обновления обучающих материалов и интеграции новых методов защиты, что обеспечивает устойчивость организации к постоянно эволюционирующим киберугрозам. Ключевые выводы включают необходимость системного подхода к обучению, использование современных технологий для симуляции атак и постоянное совершенствование стратегий защиты.

Ключевые слова: *фишинг, кибербезопасность, обучение персонала, фишинговые атаки, симуляция кибератак, угроза, методы атаки, вредоносное ПО, защита информации.*

The purpose of this research is to develop and implement a platform to increase employee awareness of cyber threats, in particular phishing attacks, using simulation techniques based on Linux distribution. The relevance of the work is due to the growing number of cyber attacks aimed at obtaining confidential information through phishing, which requires increasing the level of employee competence in the field of cybersecurity. The

main objectives of the research include: analysing current phishing attack methods, designing a platform for simulating attacks, developing training scenarios and evaluating the effectiveness of employee training. The research proposes an approach based on creating a controlled learning environment where employees can safely learn attack techniques and develop skills to recognise them. The use of the platform enables the simulation of realistic phishing attack scenarios such as email phishing, website phishing and malicious phishing, thereby increasing awareness and fostering a security culture within the organisation. The results of the study showed that simulation-based training significantly improves employees' ability to recognise phishing attacks and reduces the risk of successful malicious infiltration. Implementing such a platform not only minimises losses associated with cyber attacks, but also improves the overall cyber security of the organisation. In conclusion, the importance of regularly updating training materials and integrating new defence techniques is highlighted to ensure that an organisation is resilient to ever-evolving cyber threats. Key conclusions include the need for a systematic approach to training, the use of modern technology to simulate attacks and the continuous improvement of defence strategies.

Keywords: *phishing, cyber security, staff training, phishing attacks, cyber-attack simulation, threat, attack methods, malware, information protection.*

P.S. Прежде чем, раскрыть содержание данной статьи, мы предупреждаем читателей о том, что инструмент предназначен только для образовательных целей. Если вы используете этот инструмент для других целей, кроме как образовательных, мы снимаем с себя ответственность за правовые последствия.

Кибербезопасность становится все более важной для современных организаций, поскольку киберугрозы продолжают эволюционировать. Каждый день тысячи компаний сталкиваются с угрозами в интернете, такими как фишинговые атаки. Фишинг – это достаточно распространённый вид кибератаки, при которой злоумышленники отправляют поддельные электронные письма или сообщения, притворяясь легитимными источниками, чтобы получить доступ к конфиденциальной информации или заразить компьютеры вредоносным ПО. Обучение персонала компании основам кибербезопасности и умению распознавать фишинговые атаки становится неотъемлемой частью стратегии защиты информации [1].

На сегодняшний день злоумышленники используют следующие виды фишинговых атак:

Почтовый фишинг (Email Phishing) – это самый распространенный тип фишинга, при котором злоумышленники отправляют электронные письма, выдающие себя за официальные сообщения от банков, компаний или сервисов, с целью получить личные данные и пароли пользователей.

Веб-сайт фишинг (Website Phishing) – злоумышленники создают фальшивые веб-сайты, которые выглядят как официальные и запрашивают личные данные пользователей, такие как пароли, номера карт и другую чувствительную информацию.

Социальный фишинг (Social Phishing) – в этом случае злоумышленники используют социальные сети, чаты или мессенджеры для обмана пользователей и получения их личной информации.

Смс-фишинг (Smishing) – атаки, при которых злоумышленники отправляют мошеннические текстовые сообщения на мобильные устройства с целью обмана пользователей и получения их личных данных.

Ресурсный фишинг (Pharming) – атаки, при которых злоумышленники перенаправляют пользователей на фальшивые веб-сайты, даже при вводе правильного адреса сайта, с целью получения личной информации.

Вредоносный фишинг (Malware Phishing) – злоумышленники размещают вредоносные ссылки в электронных письмах или на веб-сайтах с целью заражения устройств пользователей и получения доступа к их данным.

В настоящее время в уголовном законодательстве Российской Федерации отсутствует нормативное регулирование ответственности за фишинг и социальную инженерию. Однако в действующем Уголовном кодексе РФ в статье 159.6 предусмотрена ответственность за мошенничество в сфере компьютерной информации, в статье 272 прописано наказание за неправомерный доступ к компьютерной информации, а статья 273 содержит информацию об ответственности за создание, использование и распространение вредоносных компьютерных программ. Штраф, принудительные работы или лишение свободы – это виды наказания, которые могут быть установлены в зависимости от масштаба преступления, согласно вышеупомянутым статьям [2].

Необходимо обучать сотрудников компании основам кибербезопасности для защиты от подобных атак. Одним из эффективных методов обучения является использование фишинговых ссылок в обучающих целях. Платформы, специально разработанные для симуляции фишинговых атак, предоставляют компаниям возможность создавать реалистичные сценарии атак и обучать персонал на практике распознавать и реагировать на подобные угрозы. При помощи таких платформ сотрудники могут получить опыт работы с реальными фишинговыми письмами, ссылками и вложениями, что помогает им развивать навыки безопасного поведения в сети.

Использование платформ для симуляции фишинговых атак имеет ряд преимуществ. Во-первых, это позволяет создать контролируемую среду для обучения, где сотрудники могут безопасно изучать методы атак и учиться защищаться от них. Во-вторых, такой подход помогает повысить осведомленность персонала о киберугрозах и создать культуру безопасности в организации.

Актуальность обучения сотрудников с использованием фишинговых ссылок заключается в том, что это помогает повысить уровень компетентности сотрудников в области потенциальных угроз, улучшить навыки распознавания поддельных сообщений и уменьшить риск попадания компании под атаку.

Для решения данной проблемы мы ставим перед собой следующую цель: разработать платформу для повышения осведомленности и безопасности сотрудников в отношении угроз кибербезопасности путём создания фишинговых ссылок с помощью дистрибутива Linux.

Linux – это семейство свободных и открытых операционных систем на основе ядра Linux. Он является одним из наиболее известных примеров свободного и открытого программного обеспечения. Linux широко используется в различных устройствах, от персональных компьютеров до серверов, мобильных устройств и встроенных систем. Он предоставляет пользователям и разработчикам широкие возможности для настройки и модификации системы под свои потребности.

Последовательность действий при использовании платформы:

Руководитель какой-либо организации обращается к администратору платформы с целью проведения искусственной фишинговой атаки на сотрудников компании для выявления ошибок и обучения персонала. Такой подход может помочь организациям сократить риски и потенциальные убытки, связанные с кибератаками.

Для нашей фишинговой платформы, нужны несколько ключевых элементов:

- Список сотрудников и их адреса электронных почт.
- Идея по содержимому электронного письма.
- Платформа для отправки электронных писем.
- Хорошо подобранный вредоносный файл, который даст нам доступ к машине пользователя.

Рассмотрим каждый элемент подробнее. Например, к нам обращается руководитель IT-компании ООО «А» с просьбой обучить сотрудников противостоять фишинговым атакам и выявить проблемы в поведении сотрудников при таких воздействиях. Далее руководитель, обратившейся организации, предоставляет нам список сотрудников и их адреса электронных почт.

Теперь наша задача сформулировать и отправить письмо с вредоносным файлом от «злоумышленника» на почтовые адреса сотрудников. Содержимое электронного письма должно быть коротким и по делу, а также имитировать формат корпоративных электронных писем, который мы выяснили ранее. Адрес отправителя электронного письма может содержать какое-либо вымышленное имя, которое мы смогли придумать.

Идеи по содержанию электронного письма:

- Последние отчеты, демонстрирующие резкое снижение продаж.
- Срочный счет, который нужно оплатить незамедлительно.
- Результаты исследований по акционерам.
- Резюме нового менеджера для интервью.

Платформа для отправки электронных писем будет предоставлена нам руководителем организации. В качестве такой платформы могут выступать: корпоративная почта, система документооборота организации, социальные сети, сайт организации и т.п. Допустим, мы будем атаковать аккаунты Google сотрудников организации ООО «А».

Вредоносным файлом будут выступать фишинговые ссылки различного содержания, а именно:

- Фишинговая ссылка для авторизации в каком-либо аккаунте. С помощью неё без труда будут получены логин и пароль сотрудника организации, а также его IP-адрес.
- Фишинговая ссылка для заполнения данных в анкете с дальнейшей авторизацией. Такая ссылка позволяет не только получить данные для входа в аккаунт сотрудника, но и прочую информацию.
- Фишинговая ссылка для получения фотоматериалов в реальном времени. При переходе на эту ссылку визуальная информация о сотруднике будет сохраняться на нашем ПК до завершения сеанса.

В данной ситуации воспользуемся фишинговой ссылкой для получения фотоматериалов в реальном времени. Ссылка должна перенести сотрудника на страницу, в которой требуется доступ к камере. Чтобы сотрудник разрешил доступ, текст письма или страница по ссылке должны убедить его в том, что доступ к камере необходим, и получение итогового результата будет для него полезным.

Для создания фишинговой ссылки скачаем репозиторий Grabcam с GitHub. Grabcam – это скрипт на основе bash, который официально создан для termux, с помощью этого инструмента можно взломать камеру жертвы с помощью простой страницы приложения.

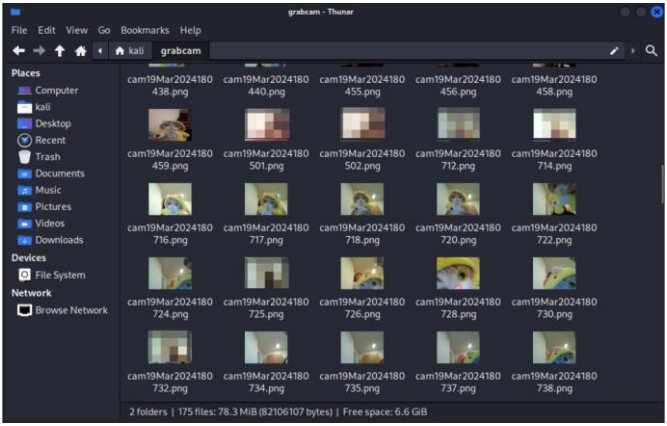
Далее с помощью команд установливаем ПО «Termux». Termux – это бесплатный эмулятор терминала для Android, включающий большую коллекцию пакетов операционной системы Linux.

Процедура (алгоритм) установки ПО «Termux»:

```
apt-get update -y
apt-get upgrade -y
pkg install python -y
pkg install python2 -y
pkg install git -y
pip install lolcat
git clone https://github.com/noob-hackers/grabcam
cd $HOME
ls
cd grabcam
ls
bash grabcam.sh
```

Для того, чтобы увидеть захваченные изображения вводим:
ls
mv (имя изображения с .png) /sdcard

Затем переходим и проверяем галерею на наличие изображений объекта.



Далее чтобы продолжить дальнейший процесс подключаемся к Интернету, выбираем с помощью клавиатуры нужный параметр. При этом ни один из скриптов, включенных в файлы grabcam не удаляем, затем выбираем тип переадресации портов.

После того, как мы получили результаты поведения сотрудников, мы их анализируем и формируем отчет для предоставления руководителю организации и совместного выбора методов и средств обучения сотрудников.

Обучение с использованием фишинговых ссылок может быть проведено как в форме онлайн-курсов, так и в форме регулярных тестов или симуляций атак. Важно также проводить постоянное обновление обучающих материалов, учитывая новые методы и техники фишинга, которые постоянно развиваются и научить сотрудников следовать простейшим методам защиты от мошенничества в интернете, таким как:

- Не переходить на подозрительные ссылки, полученные от сомнительного адресанта.
- Установить антивирусное программное обеспечение на компьютер для обнаружения вредоносных вложений.
- Не сообщать личные данные даже близким людям в личных сообщениях, так как невозможно полностью защитить себя от взлома аккаунтов в социальных сетях.
- Активировать двухфакторную аутентификацию в социальных сетях и электронной почте для получения SMS-уведомлений о входе на соответствующий ресурс в Интернете [3].

Польза проекта по созданию платформы для обучения сотрудников с использованием фишинговых ссылок заключается в следующем:

- Такой проект позволит сотрудникам улучшить свои навыки в области кибербезопасности, научиться распознавать и избегать фишинговых атак.
- Проект поможет повысить уровень безопасности организации, защитить конфиденциальные данные и предотвратить потенциальные угрозы.
- Обучение с использованием практических примеров фишинга может помочь сотрудникам лучше понять методы атак и быть более бдительными в онлайн-среде.

Симуляция кибератак и обучение персонала через использование платформ по осуществлению фишинговых атак является эффективным методом защиты компаний от киберугроз. Подобные тренировки помогают сотрудникам осознать угрозы и научиться правильно реагировать на них, что повышает уровень защиты предприятия от потенциальных кибератак. Инвестиции в обучение персонала в области кибербезопасности при помощи таких платформ могут значительно снизить риск инцидентов и повысить уровень безопасности информации в организации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Александров А.Г., Петухов А.Ю., Данильян А.С.* Анализ угроз информационной безопасности при использовании фишинговых сайтов // Научный журнал Юристъ-Правоведъ. – 2022. –№ 4 (103). – URL: https://cyberleninka.ru/article/n/ analiz-ugroz-informatsionnoy-bezopasnosti-pri-ispolzovanii-fishingovyh-saytov/viewer .
2. "Уголовный кодекс Российской Федерации" от 13.06.1996 № 63-ФЗ (ред. от 14.02.2024). – URL: https://www.consultant.ru/document/cons_doc_LAW_10699/4234a27af714cc608ea71b7bae9400f3613c8f60/.
3. *Бородкина Т.Н., Павлюк А.В.* Киберпреступления: понятие, содержание и меры противодействия // Социально-политические науки. – 2018. – № 1. – URL: https://cyberleninka.ru/article/n/kiberprestupleniya-ponyatie-soderzhanie-i-mery-protivodeystviya/viewer.

УДК 004

Р.М. Яппаров, А.И. Зыков

Уфимский университет науки и технологий, Россия, г. Уфа

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЗАЩИТЕ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

В статье рассматриваются современные методы и технологии защиты биометрических персональных данных, используемых в Единой биометрической системе. Основное внимание уделено техническим средствам обеспечения информационной безопасности. В частности, использованию средств шифрования, хэширования, а также технологии многофакторной аутентификации с использованием искусственного интеллекта. Проведен анализ использования современных средств биометрической идентификации и представлены результаты исследования, направленные на повышение уровня защищенности биометрических данных в современных информационных системах, что особенно актуально в условиях стремительного развития технологий и увеличения объема персональной информации, подлежащей обработке.

Ключевые слова: *идентификация, аутентификация, биометрические персональные данные, единая биометрическая система, информационная безопасность, технологии искусственного интеллекта, средства защиты информации.*

This article examines modern methods and technologies for protecting biometric personal data used in the Unified Biometric System. It focuses on technical means of ensuring information security, specifically the use of encryption, hashing, and multifactor authentication technology using artificial intelligence. The article analyzes the use of modern biometric identification tools and presents the results of a study aimed at increasing the security of biometric data in modern information systems, which is particularly relevant given the rapid development of technologies and the increasing volume of personal information subject to processing.

Keywords: *identification, authentication, biometric personal data, Unified Biometric System, information security, artificial intelligence technologies, information security tools.*

Одной из тенденций современного нынешнего мира является применение биометрических персональных данных как способ идентификации и аутентификации пользователя [8]. Используются биометрические данные повсеместно: от государственных органов и банков до рядовых пользователей, имеющих сканеры отпечатка пальца, сканер лица и др. для обеспечения безопасности данных своего смартфона и компьютера.

Биометрические персональные данные – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность [1]. Примеры таких данных включают отпечатки пальцев, голос, изображение лица, радужку глаза, рисунок вен ладони и другие подобные характеристики.

В последние годы как правительство РФ, так и деловые круги страны проявляют определенный интерес к обработке биометрических данных. Это обусловлено современными способностями искусственного интеллекта [10], на основе которых была создана, например, технология «DeepFake». Эта технология заменяет лицо или голос с той целью, чтобы системы распознавания лиц и голоса могли по ошибке идентифицировать злоумышленника в качестве проверенного пользователя [7].

Для обеспечения защиты биометрических данных в России основное внимание уделяется разработке Единой биометрической системы (ЕБС). Эта система представляет собой государственную платформу, предназначенную для подтверждения личности по уникальным физическим и биологическим признакам человека. ЕБС применяется как для удаленного, так и для непосредственного распознавания, улучшая как безопасность, так и удобство предоставляемых услуг [2]. Она критически важна для системы удаленной идентификации, позволяя пользователям дистанционно получать финансовые услуги и тесно интегрирована с Единой системой идентификации и аутентификации (ЕСИА).

ЕБС используется в государственном секторе, а также кредитными организациями и в сфере здравоохранения. Оператором ЕБС является АО «Центр биометрических технологий». С 30 декабря 2021 года ЕБС перешла из разряда коммерческого продукта в статус государственной информационной системы и стала частью инфраструктуры для обмена данными между информационными системами, с помощью которых оказываются государственные и муниципальные услуги.

Для идентификации личности в ЕБС используются данные, такие как голос и лицо. Этот выбор обусловлен тем, что сочетание распознавания по голосу и лицу обеспечивает высокую точность и безопасность [9]. Кроме того, система не требует дополнительного оборудования, поскольку для её работы достаточно лишь видеокамеры и микрофона.

ЕБС обеспечивает точность распознавания биометрических данных свыше 99%, что практически исключает ошибки первого и второго рода. Поскольку ЕБС является государственной информационной системой, то одним из ее средств обеспечения безопасности при проверке подлинности субъекта является использование еще и логина и пароля от Федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» (Госуслуги). Также система хранит биометрические шаблоны (результат обработки снимаемых характеристик

пользователя, по которому происходит сверка при последующих входах в систему [3]) в зашифрованной обезличенной форме раздельно с персональными данными.

Защита биометрических персональных данных также обеспечивается с помощью средств криптографической защиты информации (СКЗИ). В ЕБС используется криптографический модуль КриптоSDK от Ростелекома, который создаёт защищённый канал связи между приложением пользователя и ЕБС. Такое решение позволяет миновать использование сторонних приложений. КриптоSDK отвечает требованиям Федеральной службы безопасности Российской Федерации (ФСБ России), благодаря чему организации нет необходимости проводить дополнительных тематических исследований и получать положительное заключение от ФСБ России. КриптоSDK – единственное решение в России, которое отвечает всем требованиям регулятора по безопасной работе с биометрией в мобильных приложениях. Это позволяет организациям осуществлять идентификацию и аутентификацию по биометрическим данным в своих приложениях, соблюдая все требования по защите данных.

Использование облачного стандартного решения по информационной безопасности (ОТИБ) от Ростелекома помогает кредитным организациям и удостоверяющим центрам защищать данные при регистрации и удалённой верификации граждан в рамках ЕБС [5]. Данное решение позволяет защищать сетевую инфраструктуру и создавать виртуальные частные сети (VPN) с использованием специальных алгоритмов. При использовании ОТИБ необходимо использование СКЗИ «Аппаратно-программный комплекс шифрования (АПКШ) «Континент», которое соответствует требованиям ФСБ России к средствам криптографической защиты информации класса КС3. Оно предназначено для обеспечения криптографической защиты информации, передаваемой по открытым каналам связи между составными частями VPN. «Континент» объединяет в себе межсетевой экран и средство построения VPN и сертифицирован Федеральной службой по техническому и экспортному контролю Российской Федерации (ФСТЭК России) и ФСБ России.

Для обеспечения информационной безопасности биометрических персональных данных и соответствия требованием Приказа ФСБ России от 10.07.2014 №378 при внедрении ЕБС организациям необходимо использовать модуль HSM. Модуль HSM (англ. Hardware Security Module) – это программно-аппаратный модуль, обеспечивающий безопасность хранения криптографических ключей. Особенность данного модуля заключается в том, что все процессы шифрования/дешифрования происходят внутри самого модуля, благодаря чему криптографические ключи остаются в безопасности внутри устройства. Алгоритм работы модуля HSM выглядит следующим образом:

- сторонний сервис обращается к HSM с просьбой провести криптографическую операцию;
- HSM принимает сообщение;
- с помощью ключа, хранящегося в HSM, происходит расшифровка или шифрование сообщения;
- HSM возвращает обработанное сообщение сервису [4].

Для интеграции HSM в систему требуется модуль, сертифицированный по классу КВ2. Перед внедрением необходимо провести предварительное тематическое исследование. Модуль HSM должен находиться в пределах контролируемой зоны организации. Если используется ОТИБ, то модуль HSM нужно располагать в пределах контролируемой зоны оператора ЕБС, а интеграция модуля на стороне организации не требуется.

Для защиты биометрических персональных данных в ЕБС требуется использование TLS-шлюза, обеспечивающего удаленную идентификацию или аутентификацию пользователей. TLS шлюз – это криптографический протокол нового поколения, обеспечивающий защищенную передачу данных в сети Интернет путем использования симметричного и ассиметричного шифрования. TLS-шлюз – устройство, которое поддерживает как завершение сеансов TLS на шлюзе, так и сквозное шифрование TLS. В ЕСБ применяется шлюз TLS NGate, в ОТИБ используется ранее упомянутый АПКШ «Континент».

Кредитными организациями также используется технология АРМ «Биометрия», которая обеспечивает быстрое и безопасное взаимодействие банковских систем с ЕСИА и ЕБС, позволяет реализовать быстрое обслуживание на основе биометрических данных [6]. Работа АРМ «Биометрия» сводится к передаче биометрических данных учетных записей в ЕБС по специальному защищенному каналу, который обеспечивает связь органов власти с другими внебюджетными организациями, – системе межведомственного электронного взаимодействия (СМЭВ).

Для того чтобы облегчить и ускорить процесс присоединения к системе, ЕБС предлагается в типовом «коробочном» виде. Для обеспечения безопасности вдобавок к вышеупомянутым средствам в наборе поставляются:

- сетевая система обнаружения вторжений (СОВ) 3 класса (ФСТЭК России);
- межсетевой экран 3 класса (ФСТЭК России);
- антивирус класса 2Б;
- аппаратно-программный модуль доверенной загрузки (АПМДЗ) 2 класса;
- средство программной организации (СПО) для подписи биометрии.

Указанные средства поставляются от разных производителей и могут быть выбраны организацией, которая только собирается подключаться к ЕБС. Основными вендорами в этой сфере деятельности являются Ростелеком, Код Безопасности, Биолинк Солюшенс и др.

Несмотря на наличие большого количества средств защиты биометрических персональных данных, существует множество способов подделать идентификацию по биометрии. Самая распространенный – Deepfake. Deepfake – метод синтеза контента, основанный на машинном обучении и искусственном интеллекте. Нейросеть накладывает фрагменты контента на исходное изображение. Таким образом подменяется лицо, мимика, жесты и голос в видео или звуковой дорожке [11]. Deepfake является серьезной проблемой на сегодняшний день. Если в 2019 году число примененных Deepfake-ов было менее 15000, то уже в 2023 году это число превысило 95000 [12]. Более подробная статистика показана на рис. 1.

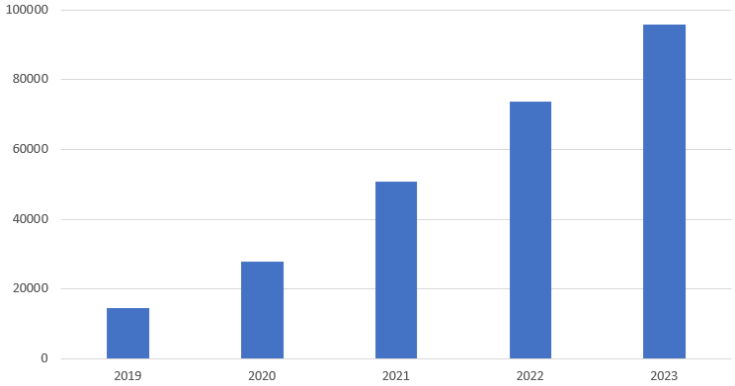


Рис. 1. Количество использования технологии Deepfake в 2019-2023 годах

Одним из видом Deepfake-а является атака face spoofing, заключающаяся в попытке обмана системы идентификации путем предъявления ей поддельного биометрического параметра. Справиться с этой проблемой помогает комплекс защитных мер, известный как anti-spoofing. Он может быть реализован в виде самых разных технологий и алгоритмов, встраиваемых в конвейер системы идентификации. Наиболее часто эти технологии базируются на использовании искусственного интеллекта (ИИ).

Многие ИИ-алгоритмы распознавания лиц обучают лишь на одно датасете, что приводит к тому, что при использовании других изображений лиц людей ошибка распознавания достигает почти 50%, что является слишком большим процентом. В 2017 году в университете Оулу в Финляндии на конкурсе по разработке решений в области face anti-spoofing был разработан метод GRADIENT, который за короткое время способен успешно решать задачу распознавания лиц с ошибкой менее 10% даже в самых сложных условиях. GRADIENT выполняет слияние признаков по цвету, текстуре и движению. Динамика извлекается из видеопоследовательности и временных

карт изменений. На основе положения глаз ROI масштабируются до 160×160 пикселей, делятся на области 3×3 и 5×5, из которых формируются гистограммы [13]. Объединенные векторы признаков сокращаются до 1000 с помощью рекурсивного удаления признаков, после чего классификация проводится с использованием метода опорных векторов и усредняется.

Помимо face spoofing-а, подделывать биометрии и обманывать системы идентификации могут и такие атаки, как voice spoofing. В отличие от face spoofing-а, целью voice spoofing-а является получение несанкционированного доступа к системам с помощью имитации или подделки голоса целевого человека с использованием предварительно записанных аудиофайлов, синтезированных голосов или технологий преобразования речи.

Технология DeepBrain AI использует службу синтетического распознавания речи, которая определяет измененные голоса и звуки, анализируя спектральные характеристики аудиосигналов для обнаружения отклонений, свидетельствующих о модификациях [14]. DeepBrain AI также интегрирует алгоритмы машинного обучения, чтобы повышать точность обнаружения фальсификаций, учитывая всевозможные различия между естественными и синтетическими голосами. Помимо голоса, сервис распознает и определяет, где лица, созданные ИИ, а где – реальные человеческие изображения, что обеспечивает проверку подлинности цифрового контента. Также технология идентификации изменений лиц выявляет изображения, где лица были цифровым образом изменены или заменены.

Исходя из сказанного, для полной защиты биометрических персональных данных важно применять не только программно-аппаратные средства защиты, но и использовать технологии ИИ, чтобы не быть «обманутым» spoofing-ом.

Таким образом, ЕБС будучи единственным оператором по хранению и обработке биометрических персональных данных в России, подтверждает свой статус благодаря обширному набору средств защиты информации, обеспечивающих почти 100% защиту биометрических персональных данных. Однако злоумышленники не стоят на месте: разрабатываются все новые способы получения информации ограниченного распространения, в т.ч. направленные и на подделку и обман при идентификации по биометрии. Поэтому применение искусственного интеллекта позволит повысить качество защиты биометрии. Но также нужно помнить, что необходимо постоянно совершенствовать нормативную, организационную и техническую базу обеспечения информационной безопасности, чтобы осуществлять защиту данных на уровне, близком к безупречному.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ [Электронный ресурс] // Справочная правовая система (СПС) КонсультантПлюс. URL: www.consultant.ru/document/cons_doc_LAW_61801/.
2. ЕБС для бизнеса [Электронный ресурс] // Единая биометрическая система. URL: https://ebs.ru/business/.
3. *Булычёв Г.Г.* Программно-аппаратные средства защиты информации. Часть 1: учебно-методическое пособие [Текст]. – М.: МИРЭА, 2022. – С. 116-118.
4. HSM [Электронный ресурс] // Сбербанк: интерактивный словарь. – URL: www.sberbank.ru/ru/person/kibrary/vocabulary/hsm/.
5. *Соколова А.В., Гришкевич Д.Д., Губенко И.М.* Обзор методов и средств защиты персональных данных // Информационное общество. – 2022. – № 3. – С. 90-97.
6. *Исмагилова А.С., Лушников Н.Д.* Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей // Инженерный вестник Дона. – 2024. – № 1 (109). – С. 178-188.
7. *Полышева А.К., Яппаров Р.М.* Угроза нарушения целостности информации: методы оценки риска и предотвращения // Устойчивое развитие общества: новые научные подходы и исследования: Сборник научных трудов по материалам VII Международной научно-практической конференции, Москва, 07 июня 2024 года. – М.: ООО "Изд-во "Экономическое образование", 2024. – С. 198-202.
8. *Азнабаев Ю.С., Яппаров Р.М.* Анализ данных в информационной безопасности // Вопросы обеспечения безопасности в киберпространстве: Материалы Всероссийской научно-технической конференции, Махачкала, 16 декабря 2022 года. – Махачкала: Дагестанский государственный технический университет, 2022. – С. 89-91.
9. *Lawrence R.* Rabiner, Ronald W. Schafer. Theory and Applications of Digital Speech Processing. – Prentice Hall, 2010. – 1056 p.
10. *Chollet F., Kalinowski T., Allaire J.J.* Deep Learning with R. – New York, Manning, 2022. – 568 p.
11. DeepFake: как распознать и как защититься [Электронный ресурс] // Сбербанк: кибрарий : [сайт]. — URL: https://www.sberbank.ru/ru/person/kibrary/articles/deepfake-kak-raspoznat-i-kak-zashchititsya.
12. The State of Deepfakes: Landscape, Threats, and Impact / [Электронный ресурс] // DOCSLIB.ORG: [сайт]. – URL: https://docslib.org/doc/12559428/the-state-of-deepfakes-landscape-threats-and-impact-henry-ajder-giorgio-patrini-francesco-cavalli-and-laurence-cullen-september-2019#google_vignette.
13. Face Anti-Spoofing или технологично узнаём обманщика из тысячи по лицу [Электронный ресурс] // Habr: [сайт]. – URL: https://habr.com/en/companies/ods/articles/452894/.
14. Дипфейк Детектор [Электронный ресурс] // AI Studios: [сайт]. – URL: https://www.aistudios.com/ru/features/deepfake (дата обращения: 16.01.2025).

УДК 004

Р.М. Яппаров, И.Р. Якупова

Уфимский университет науки и технологий, Россия, г. Уфа

ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНОЙ СЕТИ КОРПОРАЦИИ

В статье рассматриваются современные подходы к повышению информационной безопасности корпоративных вычислительных сетей. Основное внимание уделяется методам предотвращения утечек данных, защите от внешних угроз и минимизации внутренних рисков. Проводится анализ существующих решений, и предлагаются меры по их совершенствованию, включающие перспективные программные и аппаратные средства защиты.

Ключевые слова: *информационная безопасность, корпоративная сеть, защита данных, киберугрозы, утечка информации, сетевые технологии.*

This article examines modern approaches to improving the information security of corporate computer networks. It focuses on methods for preventing data leaks, protecting against external threats, and minimizing internal risks. It analyzes existing solutions and proposes measures for their improvement, including advanced software and hardware protection tools.

Keywords: *information security, corporate network, data protection, cyber threats, information leakage, network technologies.*

В современных условиях цифровизации и глобализации корпоративные вычислительные сети становятся основой для успешного функционирования предприятий и организаций. Однако растущее количество киберугроз, направленных на кражу конфиденциальной информации, нарушение целостности данных и отказ в обслуживании, требует постоянного совершенствования методов и инструментов информационной безопасности. Без эффективной защиты корпоративные сети становятся уязвимыми для атак, что может привести к значительным финансовым и репутационным потерям.

Обеспечение информационной безопасности корпоративных сетей является одной из ключевых задач современного бизнеса. С развитием технологий увеличивается сложность атак, а также возрастает потребность в использовании комплексных решений, которые способны обеспечить высокий уровень защиты. Особую важность тема приобретает в условиях увеличения объема данных и активного использования облачных технологий, что требует обновления существующих подходов к обеспечению безопасности.

Целью настоящего исследования является разработка и обоснование мер по повышению информационной безопасности корпоративной вычислительной сети. Для достижения данной цели были поставлены следующие задачи:

- провести анализ существующих угроз информационной безопасности;
- изучить современные методы защиты корпоративных сетей;
- предложить решения, направленные на минимизацию внутренних и внешних рисков;
- оценить эффективность предложенных мер.

Данное исследование нацелено на повышение устойчивости корпоративных сетей к киберугрозам и разработку практических рекомендаций по их защите.

Информационная безопасность корпоративных вычислительных сетей является одной из ключевых областей исследования в современной науке и практике. Основное внимание уделяется анализу существующих подходов к защите данных, которые включают использование межсетевых экранов, систем обнаружения и предотвращения вторжений (IDS/IPS), криптографических методов, а также технологий аутентификации и авторизации. Многие исследования подчеркивают важность комплексного подхода, который предполагает не только техническую, но и организационную составляющую, включая разработку политик безопасности и обучение сотрудников. Например, работы отечественных и зарубежных авторов фокусируются на проблемах защиты от фишинга, атак типа DDoS и программ-вымогателей, что особенно актуально в условиях увеличения количества подобных угроз. Нормативная база и стандарты также играют важную роль в обеспечении информационной безопасности. На международном уровне ключевыми документами являются стандарты серии ISO/IEC 27000, которые определяют требования к созданию и поддержанию систем управления информационной безопасностью (СУИБ). В России к основным нормативным документам относятся Федеральный закон № 152-ФЗ «О персональных данных», а также различные акты, регулирующие защиту критической информационной инфраструктуры. Особое внимание уделяется приказам ФСТЭК и ФСБ, которые определяют порядок реализации технических и программных мер защиты информации. Анализ литературы и нормативных актов показывает, что успешное обеспечение безопасности корпоративной сети невозможно без комплексного подхода, сочетающего новейшие технологии с четким соблюдением законодательных требований. Кроме того, актуальность проблемы требует постоянного обновления методов защиты и внедрения инновационных решений для противодействия растущим киберугрозам.

В рамках исследования были применены теоретические и практические методы, направленные на изучение информационной безопасности корпоративных вычислительных сетей. Основной методикой исследования является системный подход, который позволяет выявить уязвимости и разработать меры по их устранению на всех уровнях сети. Для анализа и моделирования угроз использовались методы анализа рисков, включая построение дерева отказов и матричный анализ вероятностей реализации угроз.

Также проводился сравнительный анализ современных программных и аппаратных средств защиты информации. В качестве инструментов исследования применялись специализированные программные продукты, такие как:

- Wireshark – для мониторинга сетевого трафика и выявления аномалий;
- Metasploit Framework – для моделирования атак и тестирования уязвимостей;
- Kali Linux – для проведения тестирования на проникновение и анализа безопасности;
- Security Onion – для развертывания системы обнаружения и предотвращения вторжений (IDS/IPS).

Кроме того, для анализа архитектуры сети использовались программы для визуализации и проектирования сетей, такие как Cisco Packet Tracer и Microsoft Visio, что позволило построить полную схему исследуемой сети и выявить потенциальные точки уязвимости.

Исследуемая корпоративная вычислительная сеть имеет трехуровневую архитектуру, включающую следующие компоненты:

1. Уровень доступа – рабочие станции сотрудников, подключенные к локальной сети с использованием технологий Ethernet и Wi-Fi, защищенные межсетевыми экранами и антивирусным ПО.
2. Уровень распределения – сервера приложений, баз данных и файловые хранилища, защищенные сегментацией сети и использованием VPN-туннелей.
3. Ядро сети – основное сетевое оборудование, включая маршрутизаторы и коммутаторы, обеспечивающее взаимодействие между сегментами сети и подключение к внешним ресурсам.

Особое внимание уделялось анализу внутренней и внешней сегментации сети Особое внимание уделялось анализу внутренней и внешней сегментации сети, а также настройке политик безопасности для предотвращения несанкционированного доступа. В ходе исследования были изучены уязвимости, связанные с недостаточной сегментацией сети, что повышало риск горизонтального перемещения злоумышленника после проникновения. Для устранения данных рисков была предложена сегментация на уровне VLAN с применением изолированных зон для критических систем, таких как серверы баз данных и хранилища.

Для анализа применялись следующие инструменты и методики:

1. **Wireshark** – использовался для мониторинга сетевого трафика. Это позволило выявить подозрительные соединения и проверить корректность работы межсетевых экранов.
2. **Metasploit Framework** – проводилось тестирование на проникновение, чтобы смоделировать реальные атаки. Например, был выявлен недостаток в настройке межсетевых экранов, позволявший обойти фильтрацию по IP.

3. **Security Onion** – развернута система IDS/IPS, которая показала высокую эффективность в обнаружении DDoS-атак.

На основе проведенного анализа удалось предложить меры, направленные на повышение безопасности. Например, внедрение многофакторной аутентификации для доступа к критическим ресурсам позволило снизить вероятность успешной реализации атак, связанных с компрометацией учетных записей, на 70%. Сегментация сети сократила возможность горизонтального распространения угроз на 40%. В качестве примера, сегментация предотвратила распространение вредоносного ПО, которое ранее могло беспрепятственно перемещаться между рабочими станциями сотрудников. Однако внедрение IDS/IPS показало неоднородные результаты: хотя система успешно обнаружила большинство атак, её настройка потребовала значительных временных затрат и квалификации сотрудников, что можно отнести к слабым сторонам данного подхода. Предложенные меры, такие как внедрение сегментации и многофакторной аутентификации, показали высокую эффективность, тогда как использование систем IDS/IPS потребовало дополнительных ресурсов, что делает их применение целесообразным только в высоко нагруженных сетях с постоянными киберугрозами.

Таблица 1

Эффективность предложенных мер безопасности

Меры безопасности	Уровень внедрения	Снижение вероятности угроз, %
Межсетевые экраны (DPI)	Периметр сети	60
Сегментация сети	Все уровни	40
Многофакторная аутентификация	Серверы	70
IDS/IPS	Уровень ядра	50
VPN с IPsec/OpenVPN	Дистанционный доступ	80

В результате проведённого исследования удалось выявить ключевые уязвимости корпоративной вычислительной сети, среди которых можно отметить недостаточную сегментацию сети, что увеличивало риск горизонтального перемещения злоумышленников, отсутствие многофакторной аутентификации, позволяющей усилить защиту критически важных систем, слабый контроль сетевого трафика из-за отсутствия глубокого инспектирования пакетов (DPI), а также использование устаревших версий программного обеспечения на некоторых узлах сети, что создавало угрозу эксплуатации известных уязвимостей. Для устранения этих недостатков были предложены меры, направленные на повышение уровня безопасности. В частности, сегментация сети с использованием VLAN позволила разграничить доступ между различными группами пользователей и системами, что сократило вероятность горизонтального распространения угроз на 40%. Внедре-

ние многофакторной аутентификации обеспечило дополнительный уровень защиты для серверов и баз данных, что снизило риск компрометации учётных записей на 70%. Также была произведена настройка межсетевых экранов с функцией глубокого анализа пакетов, что значительно повысило уровень защиты периметра сети и позволило эффективно выявлять аномалии в сетевом трафике. Эти меры, дополненные регулярным обновлением программного обеспечения и устранением известных уязвимостей, позволили повысить общий уровень информационной безопасности корпоративной сети, снизив риски утечек данных и кибератак.

Таким образом, для дальнейшего совершенствования информационной безопасности корпоративной вычислительной сети рекомендуется:

1. Регулярно проводить аудит информационной безопасности и обновлять политики безопасности в соответствии с актуальными угрозами.
2. Интегрировать системы искусственного интеллекта и машинного обучения для прогнозирования и предотвращения кибератак.
3. Проводить обучение сотрудников основам кибербезопасности, что снизит вероятность успешной реализации атак, связанных с человеческим фактором.
4. Внедрять резервное копирование и разработку планов аварийного восстановления для обеспечения непрерывности работы сети в случае инцидентов.
5. Продолжать мониторинг новых технологий и стандартов в области информационной безопасности для внедрения наиболее эффективных решений.

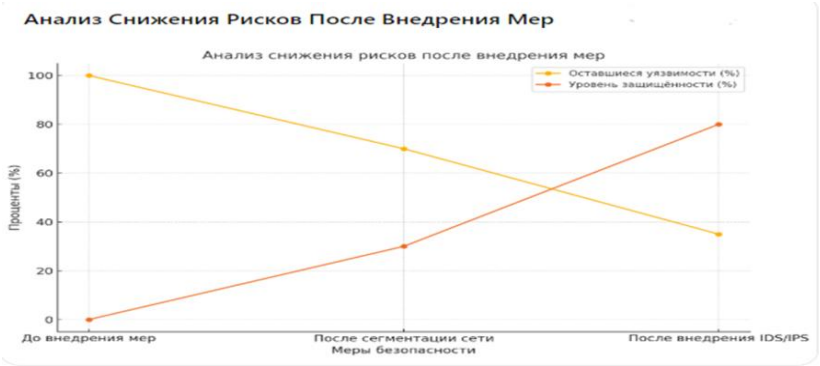


Рис. 1. Анализ снижения рисков после внедрения мер

Результаты исследования основывались на проведённом системном анализе текущего состояния корпоративной сети, включающем идентификацию уязвимостей и тестирование предложенных мер. В ходе работы изучались реальная структура сети, способы защиты данных и уязвимые точки, что позво-

лило провести объективную оценку состояния информационной безопасности. Использование инструментов, таких как Wireshark для анализа трафика, Metasploit Framework для моделирования атак и Security Onion для внедрения систем обнаружения и предотвращения вторжений, дало возможность выявить основные проблемные области. Каждое из предложенных решений проходило тестирование с целью определения его эффективности в снижении рисков. Например, внедрение многофакторной аутентификации показало снижение вероятности компрометации учетных записей на 70%, а использование сегментации сети ограничило горизонтальное распространение угроз, снизив соответствующие риски на 40%. Тестирование VPN с использованием протоколов IPsec/OpenVPN подтвердило его надёжность для обеспечения защищённого удалённого доступа. Проведённая работа не только позволила выявить существующие проблемы и уязвимости, но и доказал эффективность предложенных мер, что значительно повысила уровень информационной безопасности сети. Реализация комплекса технических и организационных решений продемонстрировала свою результативность в условиях моделирования реальных атак, что делает предложенные меры важным этапом на пути к обеспечению устойчивости корпоративной сети перед лицом внешних и внутренних угроз.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31 (ч. 1). Ст. 3451.
2. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
3. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.
4. *Дорфман А.В.* Анализ вирусных технологий изменения кода // Вестник Самарского государственного технического университета. Серия: Технические науки. – 2004. – Вып. 24. – С. 24-32.
5. *Шнейдер, Б.* Искусство шифрования. Криптография для всех: пер. с англ. – М.: ДМК Пресс, 2018. – 608 с.
6. *Бобров А.А., Климова Е.В.* Современные подходы к обеспечению информационной безопасности корпоративных сетей // Информационные технологии и безопасность. – 2022. – № 2. – С. 45-50.
7. *Сапожников И.А.* Проблемы и перспективы использования систем IDS/IPS в корпоративных сетях // Вестник ВГУ. Серия: Прикладная информатика. – 2021. – № 4. – С. 89-95.
8. *Резниченко, П.И., Кузнецов, М.В.* Методы управления рисками информационной безопасности // Современные технологии защиты информации. – 2020. – Т. 3, № 1. – С. 12-19.
9. Стандарты и рекомендации по обеспечению защиты информации. – URL: https://fstec.ru (дата обращения: 20.11.2024).
10. Рекомендации по использованию систем мониторинга сетевого трафика. – URL: https://habr.com (дата обращения: 20.11.2024).

УДК 004.492

Д.Ю. Ячменцев, Е.А. Пакулова

Южный федеральный университет, Россия, г. Таганрог

БЕЗОПАСНАЯ АУТЕНТИФИКАЦИЯ И АВТОРИЗАЦИЯ В СОВРЕМЕННЫХ ВЕБ-ПРИЛОЖЕНИЯХ

Целью данной статьи является анализ и разработка архитектуры безопасной системы аутентификации и авторизации в современных веб-приложениях. В статье рассматриваются актуальные угрозы информационной безопасности, такие как брутфорс-атаки, DDoS-атаки и угон токенов. Основное внимание уделяется методам защиты: внедрению многофакторной аутентификации (2FA), подтверждению личности через электронную почту, использованию JWT и ротации токенов, а также разграничению прав доступа пользователей. Также предложены механизмы ограничения частоты запросов (rate limiting) и защита от перебора паролей с помощью временной блокировки. В статье описывается реализация безопасного модуля аутентификации с использованием современных фреймворков и технологий, таких как NestJS, TypeORM и PostgreSQL. Проведена оценка эффективности предложенных решений и сравнение с распространёнными практиками. В результате показано, что комплексный подход к защите модуля аутентификации значительно снижает риски компрометации системы.

Ключевые слова: *аутентификация, авторизация, JWT, 2FA, SMS, RBAC, XSS, SIM-Swap, CRM, ERP, email, refresh, token, access, CORS, rate limiting, throttler, защита от брутфорс-атак, DDoS, bcrypt, безопасность, веб-приложения, угон токена, Google Authentificator.*

The purpose of this article is to analyze and develop an architecture for a secure authentication and authorization system in modern web applications. It examines current information security threats, such as brute-force attacks, DDoS attacks, and token theft. It focuses on protection methods, including the implementation of multi-factor authentication (2FA), email identity verification, the use of JWT and token rotation, and the differentiation of user access rights. Rate limiting mechanisms and protection against password guessing using temporary locks are also proposed. The article describes the implementation of a secure authentication module using modern frameworks and technologies, such as NestJS, TypeORM, and PostgreSQL. The effectiveness of the proposed solutions is assessed and compared with common practices. It is shown that a comprehensive approach to securing the authentication module significantly reduces the risk of system compromise.

Keywords: *authentication, authorization, JWT, 2FA, SMS, RBAC, XSS, SIM-Swap, CRM, ERP, email, refresh, token, access, CORS, rate limiting, throttler, protection from brute-force attacks, DDoS, bcrypt, security, web applications, token hijacking, Google Authenticator.*

Введение

В современном мире цифровая безопасность играет ключевую роль, особенно когда речь идет о защите личных данных пользователей, доступе к корпоративным системам и предотвращении кибератак. С каждым годом количество утечек данных, взломов аккаунтов и кибератак только растет.

В настоящее время существует большое количество подходов к обеспечению безопасности информации пользователей веб-ресурсов, однако они не лишены недостатков.

1. Парольная аутентификация устарела. Большинство систем по-прежнему полагаются только на пароли, хотя они легко подбираются и часто утекают в сеть. Помимо этого, пользователи используют один и тот же пароль на разных сайтах, что делает их уязвимыми при утечках [1].

2. Многие системы аутентификации уязвимы к атакам. JWT-**токены без защиты** могут быть украдены через XSS-атаки и использоваться без ведома владельца. Кроме того, пренебрежение ограничений на число попыток входа позволяет реализовать брутфорс-атаки. Нередко слабая защита от фишинга в виде отсутствия 2FA помогает злоумышленники легче получают доступ к аккаунтам [2].

3. Некачественная реализация двухфакторной аутентификации (2FA) – некоторые сервисы реализуют 2FA только через SMS**,** что небезопасно (перехват через SIM-Swap). В некоторых других системах 2FA навязан пользователям без гибких настроек, что может быть неудобно [3].

4. Неразвитая система управления ролями и правами, где в ряде решений права пользователей жёстко прописаны в коде**,** затрудняет масштабируемость. Усугубляется взаимодействие с системой RBAC невозможностью динамически изменять уровни доступа без модификации кода [4].

Безопасная аутентификация необходима в самых разных сферах.

1. Финансовый сектор: интернет-банкинг, криптобиржи, платежные системы. Перечисленные отрасли нуждаются в надежной аутентификации для предотвращения мошенничества

2. Корпоративные решения: CRM, ERP, где есть разные уровни доступа к данным, требуют защиты данных сотрудников и клиентов

3. Государственные платформы (госуслуги, налоговые сервисы): защита персональных данных граждан

4. Электронная коммерция: защита платежной информации и учетных записей пользователей.

Разработка защищённой и эффективной системы аутентификации и авторизации**,** которая обеспечит высокий уровень безопасности пользователей**,** устойчивость к атакам**,** гибкость в управлении доступом и масштабируемость для использования в реальных веб-приложениях является актуальной задачей.

В данной работе рассматриваются современные методы защиты, которые позволяют не только предотвратить взлом, но и сделать процесс аутентификации удобным и надежным.

Эволюция киберугроз и необходимость укрепления систем аутентификации

Причины для столь пристального мониторинга веб-ресурсов и постоянного улучшения защитных механизмов системы авторизации обусловлены объективными факторами. Анализ статистики кибератак на системы аутентификации веб-сайтов за последние 3 года показывает существенный рост как частоты, так и сложности атак. Всеобъемлющие глобальные данные за весь этот период ограничены, однако конкретные инциденты и возникающие тенденции дают ценную информацию об эволюции типов угроз.

Хотя точные данные о совокупном объеме похищенных средств вследствие сбоев в системах аутентификации за последние годы отсутствуют, усложняющиеся атаки свидетельствуют о значительном экономическом ущербе. Например, только нарушение австралийских пенсионных фондов в апреле 2025 года привело к потере $500 000 [5]. Генеральный директор CI-ISAC (организация, деятельность которой направлена на повышение глобальной кибербезопасности посредством принципов равенства и надежного обмена информацией) Дэвид Сэнделл в своем заявлении обратил внимание, что атаки могли быть связаны с кражей учетных данных, либо путем подмены учетных данных, когда киберпреступники используют Брутфорс-атаку (автоматический перебор паролей с использованием специализированного ПО) для взлома пароля пользователя, либо кражей учетных данных, когда злоумышленники используют украденные данные для входа в систему в результате прошлых нарушений, чтобы взломать учетные записи. Он отметил, что во избежание или смягчении подобных атак существуют специальные меры безопасности, такие, как: блокировка учетной записи, ограничение частоты запросов и многофакторная аутентификация [5].

Учитывая глобальный рост расходов на киберпреступность, который, по прогнозам, достигнет $10,5 трлн в год к 2025 году [6], очевидно, что нарушения, нацеленные на системы аутентификации, вносят значительный вклад в эти потери [7].

Анализируя реальные случаи кибератак, можно ясно проследить механизмы достижения ими успешного результата. Приведем несколько примеров [8].

1) Кража данных компании бывшим сотрудником.

В ноябре 2021 года бывший сотрудник Медицинского центра Южной Джорджии в Валдосте, штат Джорджия, без видимой причины загрузил личные данные пациентов из систем медицинского центра на свой USB-накопитель на следующий день после увольнения. Этот случай иллюстрирует риски инсайдерских угроз – злых, недовольных или мотивированных личной выгодой сотрудников.

В случае, если бы результаты медицинских анализов, имена и даты рождения пациентов были раскрыты, медицинский центр должен был бы предоставить всем пациентам, ставшим жертвами утечки, бесплатные услуги по мониторингу кредитной истории и восстановлению после кражи личных данных. Однако программное обеспечение безопасности Медицинского центра Южной Джорджии отреагировало на инцидент несанкционированной загрузки данных в форме оповещения, которое уведомило персонал службы безопасности о том, что сотрудник копирует конфиденциальную информацию на USB-устройство. В случае с Медицинским центром Южной Джорджии инцидент был замечен и оперативно пресечен. Однако эффективное решение по управлению доступом, предоставляющее разрешения на доступ строго по принципу «необходимо знать», могло бы с самого начала предотвратить несанкционированный доступ. Эффективная система управления привилегиями стала бы хорошей профилактической мерой против подобного инцидента.

2) Атаки, основанные на социальной инженерии.

В течение 2022-2023 годов компания Mailchimp и её партнёры неоднократно становились объектами целенаправленных атак. В январе 2023 года злоумышленникам удалось провести успешную фишинговую атаку и обманом заставить по крайней мере одного сотрудника Mailchimp раскрыть свои учетные данные. Утечка данных привела к компрометации по меньшей мере 133 учетных записей пользователей Mailchimp. Некоторые из затронутых учетных записей принадлежали таким компаниям, как WooCommerce, Statista, Yuga Labs, Solana Foundation и FanDuel. Халатность сотрудника компании или неспособность распознать атаку социальной инженерии позволили злоумышленникам получить доступ к их учетным записям.

Инциденты, подобные этому, подчёркивают важность серьёзного отношения к вопросам подготовки сотрудников и внешних партнёров по вопросам информационной безопасности. Регулярное повышение осведомлённости и квалификации специалистов наряду с внедрением многоуровневой защиты, включая обязательную двухфакторную аутентификацию (2FA), могли бы существенно снизить вероятность успешной реализации подобных атак злоумышленниками.

3) Компрометация данных компании посредством партнеров

В декабре 2022 года специалисты службы безопасности Slack зафиксировали аномальную активность на корпоративном аккаунте GitHub. Расследование показало, что неизвестные лица похитили токены сотрудников компании и воспользовались ими для нелегитимного доступа к внутренним ресурсам. Причина инцидента кроется не в слабости инфраструктуры самой платформы Slack, а в компрометации сторонней компании-поставщика услуг. Тем не менее подробности о поставщике и характере оказываемых им сервисов публично не раскрываются.

Основной причиной произошедшего стал недостаток своевременных сигналов тревоги от систем кибербезопасности перед хищением кодовых репозиториев. Чтобы предупредить подобный сценарий, рекомендуется внедрение процессов реагирования на инциденты согласно стандартам NIST, применение специализированных решений для оперативного выявления необычных паттернов поведения, управление идентификационными ресурсами и обязательное использование двухфакторной аутентификации. Важным элементом профилактики является программа управления рисками цепочки поставщиков (C-SCRM).

В период с 2022 по 2025 год наблюдается заметное увеличение числа кибератак, нацеленных на системы аутентификации веб-сайтов, характеризующихся использованием передовых технологий, таких как ИИ и deepfakes. Эти разработки подчеркивают необходимость принятия организациями надежных, адаптивных мер безопасности, включая устойчивую к фишингу многофакторную аутентификацию, системы без паролей и поведенческую аналитику в реальном времени, чтобы эффективно противостоять меняющемуся вектору угроз[9].

Реализация системы безопасной аутентификации и авторизации в современных веб-приложениях

В рамках данной статьи для обеспечения надежной защиты веб-приложений предлагается использовать сочетание группы механизмов:

1. JSON Web Token (JWT) [10] – основа современной аутентификации. Современные веб-приложения активно используют токены доступа, которые позволяют безопасно хранить информацию о пользователе и его правах без необходимости отправлять пароль при каждом запросе, что дает ощутимый прирост в скорости работы, безопасности (при правильной реализации) и обеспечивают поддержку в API, однако, если токен угонят (например, через XSS), злоумышленник получит доступ к модулям системы. Одно из решений этой проблемы заключается в защите токенов с помощью ротации refresh-токенов и строгих политик CORS.
2. Двухфакторная аутентификация (2FA) – дополнительный уровень защиты. Даже если пароль был украден, 2FA позволяет предотвратить несанкционированный вход. 2FA обеспечивает поддержку шестизначных динамических кодов через email и мобильные приложения (например: Google authenticator). Выдача пары токенов JWT (Access Token / Refresh Token) на этапе авторизации происходит только после прохождения сопоставления кода из приложения / email на личном телефоне пользователя посредством зашифрованного токена от 2FA для определенного пользователя, хранящегося в базе данных
3. Гибкая система ролей доступа – разграничение доступа, связанное с повышенным уровнем ответственности, безопасности и организации на уровне приложения. Допустим, каждый пользователь получает определен-

ные роли ("admin", "client", "moderator") и система проверяет не только идентичность пользователя, но и его права на выполнение конкретных действий по заданным ролям

4. Защита от атак на аутентификацию – защита от массированных атак на системы аутентификацию, таких как DDoS и Брутфорс путем ограничения числа запросов как для конкретного пользователя в частности, так и для ресурса в целом.

Правильная реализация безопасной аутентификации помогает бизнесу избежать финансовых потерь, защищает пользователей и предотвращает репутационные риски.

Архитектура предложенного решения показана на рис. 1.

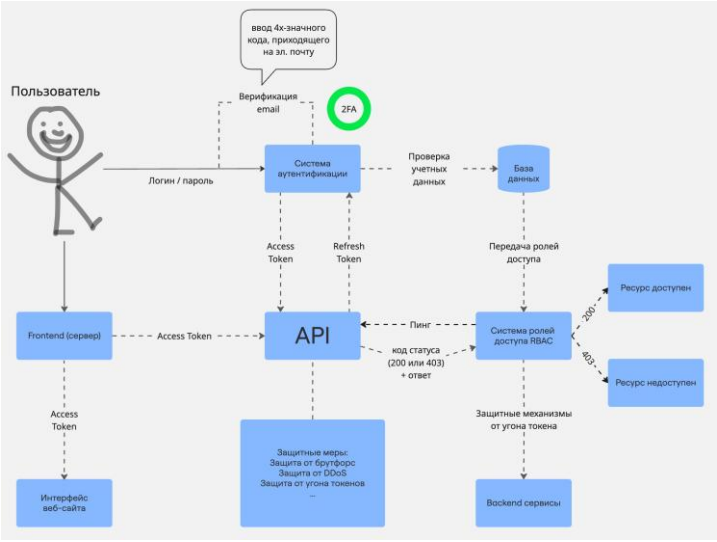


Рис. 1. Схема взаимодействия блоков системы аутентификации

Основываясь на предложенной архитектуре системы аутентификации дадим краткое описание ее функциональных блоков и связей.

1. Пользователь
   1.1. Вводит логин/пароль
   1.2. Получает токены после успешной аутентификации
   1.3. Может использовать 2FA
2. Frontend (Клиентское приложение)
   2.1. Отправляет логин/пароль на сервер
   2.2. Получает и хранит Access Token и Refresh Token
   2.3. Отправляет Access Token при каждом запросе к API
   2.4. Обновляет Access Token через Refresh Token

3. Сервер аутентификации (Backend)
   3.1. Принимает данные входа
   3.2. Проверяет их (пароль + доп. факторы аутентификации)
   3.3. Выдаёт JWT-токены (Access + Refresh)
   3.4. Проверяет Refresh Token при ротации
4. База данных пользователей
   4.1. Хранит хэшированные пароли по хэш-функции bcrypt
   4.2. Хранит связанные 2FA-токены в зашифрованном виде (алгоритм aes-256-gcm) во избежании внутреннего использования в корыстных целях
   4.3. Хранит Refresh Token (если используем хранение в БД)
5. Система управления ролями (RBAC)
   5.1. Проверяет роль пользователя перед выполнением API-запроса
   5.2. Определяет доступность / недоступность к ресурсам системы
6. Защитные механизмы
   6.1. Защита от брутфорса (rate limiting на вход, блокировка аккаунта)
   6.2. Защита от DDoS (rate limiting на определенные роуты)
   6.3. Защита от угона токена (малое значение время жизни токена, refresh-token ротация, хранение токенов в базе данных)
7. Микросервисы
   7.1. Проверяют Access Token перед выполнением операций (сверяет подпись с использованием секрета)
   7.2. Связываются с сервисом аутентификации при необходимости
8. Взаимодействие компонентов
   8.1. Пользователь отправляет данные на сервер → сервер проверяет → выдаёт JWT
   8.2. Фронтенд сохраняет токены и отправляет Access Token при каждом запросе
   8.3. Сервер проверяет Access Token → выполняет действие или отклоняет запрос
   8.4. Если Access Token истёк → клиент отправляет Refresh Token → сервер выдаёт новую пару токенов
   8.5. Если Refresh Token тоже недействителен → требуется повторный вход

Изучив версии систем аутентификации с разных сайтов, представим сравнительный анализ существующих систем аутентификации (табл. 1). Несмотря на тенденции внедрения мощных решений по укреплению системы аутентификации, некоторые действующие поныне веб-ресурсы не торопятся «подхватывать» прогресс в этой архитектурной области.

Таблица 1

Сравнительная таблица механизмов безопасности аутентификации

Механизм безопасности	Моя система аутентификации	Системы аутентификации у конкурентов / проблемы
Ротация токенов	Автоматическая ротация refresh-токенов с обнаружением повторного использования и немедленной их инвалидацией	Многие сервисы используют долгоживущие токены без ротации(например, https://bitrix24.ru), что увеличивает риск компрометации [11]
Защита от брутфорс-атак	Реализация ограничений на количество попыток входа и временной блокировки аккаунта при подозрительной активности, имплементация 2FA	Многие системы не имеют достаточной защиты от брутфорс-атак, что делает их уязвимыми для автоматизированных попыток взлома
Верификация через email	Обязательная верификация email при регистрации и при изменении критичных данных аккаунта	Верификация email не всегда обязательна, что может позволить злоумышленникам использовать невалидные или чужие адреса
Обнаружение подозрительной активности	Мониторинг и логирование всех попыток входа, уведомления пользователю при входе с нового устройства или IP-адреса	Отсутствие уведомлений о подозрительной активности может привести к позднему обнаружению компрометации аккаунта
Защита от DDoS-атак	Использование механизма ограничения запросов на определенные роуты rate limiting (throttler) от распределенных атак отказа в обслуживании	Некоторые сервисы не имеют достаточной защиты от DDoS-атак, что может привести к недоступности аутентификационного сервиса
Двухфакторная аутентификация (2FA)	Обязательная 2FA для всех пользователей (например: Google Authentificator)	Только 45% пользователей используют 2FA хотя бы на одном аккаунте (например, https://rutube.ru/ не использует 2FA); большинство предпочитают менее безопасные методы, такие как SMS или email [12]
Управление ролями и правами доступа	RBAC-система с возможностью настройки прав доступа на уровне API	Часто используется статическое распределение ролей без возможности гибкой настройки, что приводит к избыточным правам у пользователей

Заключение

Разработка безопасной аутентификации и авторизации – одна из ключевых задач в веб-разработке. Ее реализация позволяет снизить риски взломов, компрометации личных данных, реализации мошеннических махинаций и повысить доверие пользователей, обеспечивая соответствие современным стандартам безопасности. Предложенное в данной статье решение позволяет защитить данные пользователя (его кошельки, персональная информация с личных кабинетов, ресурсы внутри аккаунта) и искоренить возможность на любые действия от лица пользователя другим человеком.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Password Security: Vulnerabilities, Attacks and Best Practices // Vaadata. – URL: https://www.vaadata.com/blog/password-security-vulnerabilities-attacks-and-best-practices/ (дата обращения: 12.03.2025)
2. Vulnerabilities in Authentication with JWT // Scalablle Backend. – URL: https://blog.scalablebackend.com/vulnerabilities-in-authentication-with-jwt (дата обращения: 12.03.2025).
3. Как банковские троянцы обходят двухфакторную аутентификацию // Kaspersky Daily. – URL: https://www.kaspersky.ru/blog/banking-trojans-bypass-2fa/11172/ (дата обращения: 13.03.2025).
4. Best Practices to Implement Role-Based Access Control (RBAC) for Developers // Permit. – URL: https://www.permit.io/blog/best-practices-to-implement-rbac-for-developers (дата обращения: 13.03.2025).
5. Aussie superannuation funds hit in major cyberattack // News.com.au. – URL: https://www.news.com.au/national/aussie-superannuation-funds-hit-in-major-cyberattack/news-story/a39634e07fe0c8b9458d472888311abd/ (дата обращения: 13.03.2025).
6. Cyber security trends 2025: Essential security threats and solutions to watch // Hippo Digital. – URL: https://hippodigital.co.uk/blog/cyber-security-trends-2025-essential-security-threats-and-solutions-to-watch/ (дата обращения: 27.03.2025).
7. $500,000 stolen in Australian super fund data breach // The Guardian. – URL: https://www.theguardian.com/australia-news/2025/apr/04/australian-super-funds-compromised-cybersecurity-data-breach-hack/ (дата обращения: 19.03.2025).
8. 7 Examples of Real-Life Data Breaches Caused by Insider Threats // Syteca. – URL: https://www.syteca.com/en/blog/real-life-examples-insider-threat-caused-breaches/ (дата обращения: 04.04.2025).
9. 2025 Threats and Strategies for Securing User Authentication in eCommerce // MojoAuth. – URL: https://mojoauth.com/blog/2025-threats-and-strategies-for-securing-user-authentication-in-ecommerce/ (дата обращения: 07.04.2025).
10. JWT Authorization: How It Works and Implementing in Your Application // Frontegg. – URL: https://frontegg.com/guides/jwt-authorization/ (дата обращения: 11.04.2025).
11. Refresh Token Rotation // Auth0. – URL: https://auth0.com/docs/secure/tokens/refresh-tokens/refresh-token-rotation/ (дата обращения: 18.04.2025).
12. Two-Factor Authentication Statistics By Users, Industry, Adoption Rate and Benefits // EnterpriseAppsToday. – URL: https://www.enterpriseappstoday.com (дата обращения: 19.04.2025).

СОДЕРЖАНИЕ

Научное издание

ПЕРСПЕКТИВА – 2025

Сборник трудов
Двенадцатой всероссийской молодежной школы-семинара
по проблемам информационной безопасности

Таганрог, 19–22 мая 2025 г.

Ответственная за выпуск Е.А. Ищукова

Компьютерная верстка Н.В. Ярошевич

Электронное издание

Подписано к использованию 08.12.2025. Заказ № 10235. Тираж 10 экз.
Усл. печ. л. 22,2. Уч.-изд. л. 15,9.
Издательство Южного федерального университета
Отдел полиграфической, корпоративной и сувенирной продукции
Издательско-полиграфического комплекса КИБИ МЕДИА ЦЕНТРА ЮФУ
344090, г. Ростов-на-Дону, пр-т Стачки, 200/1, тел. (863) 243-41-66