УДК 004.056.55

СОВЕРШЕНСТВОВАНИЕ МОНИТОРИНГА И АУДИТА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

IMPROVING MONITORING AND AUDIT OF INFORMATION SECURITY EVENTS

Орлова Татьяна Степановна, д.ф.н., профессор кафедры информационных технологий и статистики ФГБОУ ВО «Уральский государственный экономический университет» (УРГЭУ)

Саулич Никита Евгеньевич, магистрант кафедры информационных технологий и статистики ФГБОУ ВО «Уральский государственный экономический университет» (УРГЭУ)

Orlova Tatyana Stepanovna, Doctor of Philosophy, Professor of the Department of Information Technology and Statistics of the Ural State University of Economics (USUE)

Saulich Nikita Evgenievich, Master's student at the Department of Information Technology and Statistics at the Ural State University of Economics (USUE)

Аннотация. Статья посвящена вопросам совершенствования мониторинга и аудита событий информационной безопасности в контексте информационных систем Федеральной налоговой службы России (ФНС России). Акцент делается на растущей угрозе кибератак и утечек данных в государственных информационных ресурсах, особенно в условиях киберкриминальной активности и политически мотивированных атак. В статье анализируются типовые векторы атак, а также раскрываются современные требования к системам аудита и мониторинга, в частности к системам централизованного аудита событий информационной безопасности.

Abstract. This article examines improving the monitoring and auditing of information security events in the context of the information systems of the Federal Tax Service of Russia (FTS of Russia). It focuses on the growing threat of cyberattacks and data leaks in government information resources, particularly in the context of cybercriminal activity and politically motivated attacks. The article analyzes typical attack vectors and discusses modern requirements for audit and monitoring systems, particularly for centralized auditing of information security events.

*Ключевые слова: и*нформационная безопасность, Киберугрозы, мониторинг событий, кибератаки, системы SIEM.

Keywords: information security, cyber threats, event monitoring, cyber-attacks, SIEM systems.

Информационные системы ФНС России обеспечивают обработку налоговой отчетности, межведомственное электронное взаимодействие и предоставление цифровых услуг физическим и юридическим лицам. При этом осуществляется обработка значительных объемов информации ограниченного доступа, включая персональные данные и сведения, составляющие налоговую тайну, что требует обеспечения высокого уровня информационной безопасности [1].

В условиях роста количества компьютерных атак на государственные информационные ресурсы проблема защиты информации приобретает особую актуальность. Согласно аналитическим материалам ФСТЭК России, ENISA Threat Landscape 2025 и IBM X-Force Threat Intelligence Index 2025, государственный сектор остается одной из наиболее атакуемых сфер цифровой инфраструктуры. По данным компании «ECA Про», в 2025 году на государственные организации пришлось 73% всех утечек данных в России, а общий объем скомпрометированных данных превысил 105 млн строк [2]. Значительная часть атак связана с политически мотивированными действиями и кибершпионажем.

Эффективность защиты государственных информационных систем во многом зависит от процессов регистрации, мониторинга и анализа событий безопасности. Традиционные методы локального журналирования и ручного анализа становятся недостаточно эффективными из-за роста объемов данных и сложности современных атак. В связи с этим возрастает необходимость внедрения централизованных систем мониторинга и корреляции событий информационной безопасности (SIEM), позволяющих автоматизировать выявление инцидентов и повысить оперативность реагирования.

Особое значение для построения систем аудита имеет приказ ФСТЭК России от 11 апреля 2025 года № 117, вступающий в силу с 1 марта 2026 года [3]. Документ устанавливает требования к централизованному сбору, хранению и защите журналов аудита, а также к регулярной оценке защищенности государственных информационных систем.

Для исследования процессов обеспечения информационной безопасности применяются методы структурно-функционального моделирования и имитационного проектирования. Информационная инфраструктура ФНС России представляет собой сложную распределенную систему, обеспечивающую централизованное хранение и обработку данных, межведомственное взаимодействие и поддержку электронного документооборота. Основными функциями информационных систем ФНС являются: обработка налоговой

отчетности; автоматизация налогового администрирования; предоставление электронных сервисов; хранение и обработка персональных данных; межведомственный электронный обмен информацией.

Эмпирическое исследование предметной области направлено на сбор и анализ фактических данных, характеризующих текущее состояние киберугроз в государственном секторе, закономерности распространения инцидентов безопасности, типовые векторы атак на государственные информационные системы, а также реальные эксплуатационные требования к системам централизованного аудита событий безопасности. Данный анализ формирует необходимую эмпирическую базу для последующего обоснования проектных решений, выбора конфигурации системы и разработки имитационной модели.

Общая динамика кибератак. В первом квартале 2025 года с помощью хонипотов было выявлено 607,7 тыс. атак, что в 2,5 раза превышает аналогичный показатель предыдущего года, что свидетельствует как о повышении общей активности злоумышленников, так и о развитии инструментария обнаружения. По итогам 2025 года зафиксировано 9,3 млн случаев заражений в 38,5 тыс. организаций, при этом средняя интенсивность атак на одну компанию выросла на 51% по сравнению с предыдущим периодом [4]. Согласно отчету Positive Technologies, в большинстве случаев злоумышленники стремились получить доступ именно к защищаемым данным, а каждая пятая атака носила идеологический характер [5].

Структура выявленных угроз. На основе детального анализа инцидентов высокого уровня критичности, проведенного Центром кибербезопасности F6 за период 2024–2025 годов, выявлена следующая структура угроз. Наиболее распространенным типом вредоносной активности остались майнеры криптовалют – 37% всех критичных инцидентов (снижение с 42% во втором полугодии 2024 года до 31% в первом полугодии 2025 года). Второе место заняли атаки с ручным управлением (хищники) – 15%, требующие непосредственного взаимодействия атакующего с скомпрометированной инфраструктурой. Третье место заняли бэкдоры (программные закладки для скрытого удаленного управления) – 14% всех критичных случаев. Доля инцидентов с троянами удаленного доступа выросла с 4% до 13% [6].

Статистика утечек данных в государственном секторе. Согласно данным компании «Еса Про», государственные организации стали основной целью хакерских атак в 2025 году: на них пришлось 73% всех утечек данных в России, что превышает 105 млн строк данных с записями о пользователях и компаниях. Всего за отчетный период в открытом доступе оказалось более 145 млн строк данных [7]. В компании F6 зафиксировали рост объема утекших строк почти на

68% (до 767 млн) при сокращении количества слитых баз данных на 50% – до 225 единиц, что свидетельствует о росте объемов каждой конкретной утечки [8].

Анализ основных векторов атак. Главным вектором атак стали загрузки пользователями вредоносных программ из непроверенных источников – 70% всех инцидентов за год. В первой половине 2025 года их доля выросла с 60% до 74% [7]. Фишинг остается ключевым первоначальным вектором атак APT-группировок: злоумышленники не ограничиваются простой рассылкой, используют вредоносные файлы, замаскированные под официальные документы, и многослойные техники обхода систем защиты [9]. Доля зараженных съемных носителей составила 9% от общего числа инцидентов, что особенно актуально для закрытых сегментов ГИС.

Атаки через привилегированные учетные записи. По данным команды BI.ZONE TDR, 39% киберинцидентов связаны с использованием или компрометацией привилегированных учетных записей. Наиболее распространенные техники: компрометация действующих учетных данных (57% случаев), манипуляции с учетными записями (создание скрытых администраторских прав) – 40% случаев, использование легитимных учетных записей для удаленного подключения (например, через SSH или RDP) – 15% случаев [10].

Тактики злоумышленников по MITRE ATT&CK. Согласно анализу, распределение тактик выглядит следующим образом: Defense Evasion (TA0005) – 30% инцидентов; Privilege Escalation (TA0004) – 20%; Execution (TA0002) – 17%; Persistence (TA0003) – 17%. В 2025 году выросла доля атак с выполнением и повышением привилегий, что коррелирует с общим усложнением атак и усилением мер аутентификации [11].

Эксплуатационные требования к SIEM-системам для крупных ГИС. Ключевым показателем производительности SIEM является количество событий, обрабатываемых в секунду (EPS). Крупные государственные информационные системы генерируют нагрузку от 5 000 до 100 000 EPS в зависимости от количества контролируемых устройств. Для ГИС ФНС России с учетом распределенной инфраструктуры прогнозируемый пик EPS составляет 10 000–20 000. Общий требуемый объем хранилища складывается из горячего хранения (NVMe/SSD, 3–7 суток) и холодного архива (до 5 лет с обеспечением неизменяемости). При среднем размере нормализованного события 0,5–1,5 КБ и коэффициенте репликации 2 объем горячего хранилища может достигать 12 ТБ [12].

Требования к вычислительным ресурсам. Для SIEM-систем, построенных на кластерной архитектуре, требования определяются целевым значением EPS.

Уровень до 2 500 EPS требует 8 ГБ оперативной памяти; уровень 5 000–7 500 EPS – 48 ГБ; уровень 7 500–10 000 EPS – от 48 до 256 ГБ ОЗУ на кластерный узел [13]. Для масштаба ГИС ФНС (ориентировочно более 10 000 EPS) требуется кластер из нескольких узлов с горизонтальным масштабированием.

Международные нормативные требования (сопоставление). NIST SP 800-92 (базовый документ по управлению журналами) рекомендует централизованную агрегацию логов, определение критических источников и защиту целостности с использованием защищенных протоколов. ГОСТ Р ИСО/МЭК 27001-2021, гармонизированный с ISO/IEC 27001:2013, в разделах по логированию закрепляет обязательную регистрацию аутентификационных событий, детальное логирование действий администраторов и централизованную агрегацию [14]. Эти требования согласуются с российскими нормативными актами (приказ ФСТЭК № 117).

Обобщенные требования к системе аудита. На основе проведенного эмпирического исследования сформулированы следующие требования: обработка пиковых нагрузок EPS (до 10 000–20 000) с масштабируемой кластерной архитектурой; приоритет правил корреляции для контроля привилегированных учетных записей (PAM); обязательное использование защищенных каналов передачи (Syslog TLS) и механизмов неизменяемости логов (цифровая подпись, WORM); внедрение профилирования поведения (UEBA) или пороговых правил для детектирования аномалий; контроль действий со съемными носителями и веб-фильтрация.

Таким образом, в заключении отметим следующие основные аспекты. Для защиты государственных информационных ресурсов чрезвычайно важно использование централизованных систем мониторинга и корреляции событий (SIEM), которые способствуют оперативному обнаружению и реагированию на инциденты информационной безопасности. Анализ показал, что значительная часть инцидентов связана с использованием или компрометацией привилегированных учетных записей. Это требует установления жесткого контроля и применения механизмов регулярной оценки защищенности государственных информационных систем. Реализация эффективной стратегии защиты информации должна опираться на комплексный подход, включающий как технические средства защиты, так и методы административного регулирования и контроля. Укрепление информационной безопасности также невозможно без систематического обучения работников принципам безопасности и методам противодействия потенциальным угрозам.

С учетом современных вызовов и возрастающей сложности атак, государственные органы должны не только использовать современные технологии для защиты данных, но и постоянно совершенствовать методы анализа и предотвращения инцидентов, а также усиливать международное сотрудничество в данной области.

Список литературы

1. Кострикина А.О., Лазунин К.А. Информационная безопасность в критической информационной безопасности // Проблемы научной мысли. – 2024. – Т. 4, № 1. – С. 82–85. – EDN NODVRW.
2. Нестеров А.В. Существует ли информационная безопасность, или Некоторые аспекты законопроекта Технического регламента «О безопасности информационных технологий» // Правовые вопросы связи. – 2007. – № 1. – С. 31–35. – EDN JTIUCG.
3. Противодействие фишингу: комплексный подход к защите пользователей и бизнеса / Н. С. Кольева, Т. С. Орлова, И. А. Жиделев, П. А. Козлов // Актуальные вопросы современной экономики. – 2026. – № 1. – С. 510–515. – EDN CRQVCV.
4. Сапега А.В. Анализ рисков информационной безопасности предприятия // E-Scio. – 2023. – № 2(77). – С. 44–49. – EDN CTZCXW.
5. Баторов Б.О. Некоторые проблемы нормативно-правового регулирования защиты информации в органах внутренних дел Российской Федерации и пути их разрешения // Труды Академии управления МВД России. – 2022. – № 2 (62). – С. 121–127. – DOI 10.24412/2072-9391-2022-262-121-127. – EDN EOCSJV.
6. Павлов Е.О., Резниченко С.А. Организационно-правовые особенности аудита информационной безопасности в кредитных организациях Российской Федерации // Вестник РГГУ. Серия: Информатика. Информационная безопасность. Математика. – 2025. – № 3. – С. 36–53. – DOI 10.28995/2686-679X-2025-3-36-53. – EDN CEQJST.
7. Кольева Н.С., Кортенко Л.В., Кротова В.А. Анализ и диагностика цифровой трансформации IT-компании // Экономические системы. – 2025. – Т. 18, № 4. – С. 90–106. – DOI 10.29030/2309-2076-2025-18-4-90-106. – EDN OVMKUQ.
8. Косоруков А.А. Технологии искусственного интеллекта в сфере цифровой безопасности // Эффективное управление: научный альманах памяти профессора М.И. Панова: Сборник статей. Выпуск 6 (11). – Москва: ООО «Издательство «Перо», 2025. – С. 134–155. – EDN MSCLBO.

9. Шерстюк В.П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения информационной безопасности // Информационное общество. – 1999. – № 5. – С. 3–-5. – EDN HRNTDF.
10. Кольева Н.С., Брюханов П.В., Колесов Д.Д. Обеспечение информационной безопасности в бизнесе // Цифровая трансформация общества и информационная безопасность: Материалы II Всероссийской научно-практической конференции, Екатеринбург, 19 мая 2023 года / Отв. за выпуск А.Ю. Коковихин, отв. редактор М.А. Панов. – Екатеринбург: Уральский государственный экономический университет, 2023. – С. 80–84. – EDN ESTZTV.
11. Николаева, М. О. Информационная безопасность: современная картина проблемы информационной безопасности и защиты информации / М. О. Николаева // Мониторинг. Образование. Безопасность. – 2023. – № 1(1). – С. 51–57. – EDN IOIQDI.
12. Чапис М.А. Информационная безопасность государства как правовой порядок обеспечения национальной безопасности в информационной сфере // Наукосфера. – 2024. – № 6-1. – С. 551–557. – DOI 10.5281/zenodo.11638587. – EDN JKTRGZ.
13. Полыхань К.О. Проблемы и особенности состояния информационной безопасности в соответствии с доктриной информационной безопасности Российской Федерации // Устойчивое развитие науки и образования. – 2019. – № 5. – С. 154–160. – EDN XNBSUW.
14. Алейникова Д.И. Системы управления информационной безопасностью и событиями информационной безопасности // Технические средства защиты информации: материалы XXIII Международной научно-технической конференции, Минск, 08 апреля 2025 года. – Минск: Белорусский государственный университет информатики и радиоэлектроники, 2025. – С. 51–54. – EDN KFUOQD.