DOI https://doi.org/10.46845/2541-8254-2024-5(47)-7-7
УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ФИНАНСОВОМ СЕКТОРЕ: ВЫЗОВЫ, РЕШЕНИЯ И ВЛИЯНИЕ НА КАЧЕСТВО ФИНАНСОВОЙ ОТЧЕТНОСТИ

И.А. Шабанов, студент
e-mail: shabanchick2002@gmail.com
ФГБОУ ВО «Калининградский государственный технический университет»

В данной научной работе рассмотрены теоретические и практические аспекты информационной безопасности в финансовом секторе, акцентированы основные угрозы, вызовы и внедряемые решения. Исследование включает анализ международных стандартов кибербезопасности (ISO 27001, NIST Cybersecurity Framework), инновационных технологий (искусственный интеллект, блокчейн, квантовое шифрование) и успешных кейсов их применения. Особое внимание уделено ситуации в России, включая национальные стратегии, нормативно-правовое регулирование и адаптацию мировых решений под локальные условия. Выводы подтверждают эффективность внедрения комплексных мер киберзащиты, минимизирующих финансовые потери и обеспечивающих устойчивость банковской системы.

Ключевые слова: информационная безопасность, кибербезопасность, финансовый сектор, угрозы, стандарты информационной безопасности, искусственный интеллект, блокчейн, квантовое шифрование, ISO 27001, NIST Cybersecurity Framework.

ВВЕДЕНИЕ

Информационная безопасность в финансовой сфере относится к одной из самых актуальных и важных тем в условиях цифровизации мировой экономики. Финансовые организации, включая банки, страховые компании и инвестиционные фонды, сталкиваются с возрастающим числом киберугроз, таких как утечка данных, атаки «человек посередине» и шифровальные вирусы. Эти угрозы способны не только нанести прямой финансовый ущерб, но и подорвать доверие клиентов и партнеров.

Актуальность исследования обусловлена ростом кибератак, которые угрожают экономической стабильности организаций и требуют разработки эффективных стратегий противодействия угрозам и обеспечения более совершенной защиты от них [1, 2].

ОБЪЕКТ ИССЛЕДОВАНИЯ

Объектом исследования является финансовый сектор, как один из наиболее уязвимых кибератакам сегментов экономики, включающий банки, инвестиционные компании, страховые организации и другие финансовые учреждения.

ЦЕЛЬ И ЗАДАЧИ ИССЛЕДОВАНИЯ

Цель данной работы — исследование значения информационной безопасности на финансовую отчетность и изучение современных подходов к минимизации рисков. В процессе анализа будут рассмотрены основные вызовы, ключевые решения и меры повышения устойчивости финансовых институтов к киберугрозам. Также ставятся следующие задачи:

1. Провести классификацию и анализ актуальных киберугроз в финансовой сфере.
2. Изучить существующие стандарты и нормативно-правовые акты, регулирующие информационную безопасность.

3. Оценить внедрение инновационных решений, таких как искусственный интеллект, блокчейн и квантовое шифрование.

4. Исследовать особенности реализации киберзащиты в России в условиях внешних ограничений.

5. Выявить наиболее эффективные подходы и предложить рекомендации для финансовых организаций.

МЕТОДЫ ИССЛЕДОВАНИЯ

В процессе исследования были использованы следующие методы:

1. Аналитический метод: изучение и систематизация научной литературы, отчетов и данных о киберугрозах.

2. Метод сравнительного анализа: сопоставление мировых стандартов и решений с российскими подходами.

3. Метод кейс-стади: изучение реальных примеров внедрения технологий и стандартов в кибербезопасности.

4. Экспертный метод: использование данных отраслевых исследований и прогнозов ведущих аналитических центров.

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФИНАНСОВОМ СЕКТОРЕ

Кибербезопасность включает меры обеспечения защиты информационных систем и данных от несанкционированного доступа и использования, утечек, кражи или разрушения. В финансовой сфере это особенно критично, так как любая атака на компьютерные системы может привести к утрате данных о транзакциях, конфиденциальной информации клиентов и репутационным потерям.

Финансовый сектор, несомненно, представляет собой одну из самых привлекательных целей для киберпреступников. Это связано с высоким объемом денежных операций, чувствительностью обрабатываемых данных и сложностью IT-инфраструктуры. Среди наиболее распространенных угроз — фишинг, атаки на базы данных, использование вредоносного ПО и кража учетных данных [3].

Важность темы для России. В российской экономике цифровизация банковских услуг, развитие финтеха и внедрение технологий онлайн-платежей существенно увеличили зависимость финансового сектора от IT-систем. Одновременно с этим обострились геополитические вызовы, что привело к росту числа целевых кибератак, направленных на российские финансовые учреждения. Это делает задачу обеспечения информационной безопасности стратегически важной для сохранения экономической стабильности [4].

Финансовые институты в России активно развивают системы защиты, однако нехватка квалифицированных кадров и отсутствие единых стандартов защиты в ряде случаев препятствуют эффективному реагированию на угрозы. Таким образом, необходимость анализа текущих вызовов и поиска решений приобретает особую актуальность.

ОСНОВНЫЕ УГРОЗЫ И РИСКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФИНАНСОВОМ СЕКТОРЕ

Финансовый сектор сталкивается с непрерывным ростом киберугроз, вызванным цифровизацией и геополитической нестабильностью. Ведущие угрозы включают фишинг, программы-вымогатели, утечки данных и атаки на инфраструктуру. Наиболее распространенными векторами атак являются фишинг (41% инцидентов) и вредоносное ПО, доставляемое через электронную почту (94% случаев).

В 2023 году средний размер выкупа при атаках с применением программ-вымогателей вырос с $812 тыс. до $1,5 млн. Восстановление данных обходится в среднем в $2,73 млн. Прямые убытки от компьютерных инцидентов в финансовом секторе достигли $2,5 млрд в 2023

году. Однако косвенные потери (репутационный ущерб, затраты на восстановление инфраструктуры и компенсации клиентам) намного выше.

На финансовые компании приходится около 20% всех атак. В частности, банки наиболее уязвимы из-за больших объемов транзакций и чувствительных данных [5, 6, 7].

Примеры реальных кейсов:

1. Атаки на банки и платежные системы. В декабре 2023 года атака на центральный банк Лесото нарушила национальную платежную систему, что повлияло на работу всех местных банков.
2. Третьи стороны как источник рисков. В 2023 году атака на IT-провайдера в США одновременно вывела из строя 60 кредитных союзов, подчеркивая риск зависимости от внешних поставщиков услуг.
3. Персональные данные – постоянная цель злоумышленников. В октябре 2023 года Роскомнадзор официально подтвердил утечку персональных данных примерно одного миллиона клиентов МТС Банка. В утечке были обнаружены такая информация, как ФИО, номера телефонов, ИНН, даты рождения и частично номера банковских карт. А несколькими месяцами ранее этого «Ренессанс страхование» подверглась кибератаке, в результате которой преступники получили доступ к примерно 2% клиентской базы [5, 8, 9].

Отдельно важно отметить, что условиях геополитической нестабильности и санкционного давления Россия испытывает усиление киберугроз. Согласно отчетам, после начала конфликта на Украине в 2022 году число кибератак увеличилось на 97%, что побудило 51% организаций пересмотреть стратегии управления рисками. Российский финансовый сектор остается важной целью для хакеров, что требует повышенного внимания к разработке локальных решений, устойчивых к внешнему влиянию [4, 7, 16].

Понимание масштабов угроз и их последствий играет ключевую роль для разработки эффективных стратегий защиты. В следующем разделе будет рассмотрен опыт применения различных мер и технологий для снижения информационных рисков.

СОВРЕМЕННЫЕ РЕШЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основные методы улучшения безопасности систем можно разделить на две группы: технологические инновации и разработка актуальных политик.

Технологические инновации в сфере информационной безопасности:

1. Искусственный интеллект (AI) и машинное обучение (ML). Технологии AI/ML активно используются для анализа поведения пользователей и выявления аномалий. Например, системы AI позволяют заранее предсказывать атаки, определяя подозрительные действия на основании больших массивов данных. В 2023 году банк в США внедрил систему на базе AI для анализа транзакций в реальном времени, что позволило снизить уровень мошенничества на 37%. Ожидается, что к 2025 году инвестиции в AI для финансового сектора достигнут $31 млрд [5, 7].
2. Шифрование и управление ключами. Современные алгоритмы шифрования, такие как AES-256, обеспечивают надежную защиту данных. Использование многофакторного управления ключами (например, с разделением ключа между несколькими сторонами) минимизирует риски. В 2023 году одна из российских финтех-компаний начала использовать систему «квантового шифрования», повышающую устойчивость данных к атакам, даже если хакеры применяют квантовые компьютеры [11, 13].
3. Облачные решения. Переход к облачным технологиям позволяет повысить масштабируемость и надежность финансовых систем, а также обеспечить более быструю реакцию на угрозы. В 2022 году 70% банков в США перешли на гибридные облачные решения, что позволило снизить время восстановления данных после атак на 50% [6].
4. Технологии блокчейна. Блокчейн обеспечивает высокий уровень прозрачности и невозможность изменения записей, что делает его перспективным для финансового учета и

предотвращения мошенничества. Национальный банк Китая применил блокчейн для отслеживания транзакций, что уменьшило количество сомнительных операций на 65% в 2023 году [3, 10].

Международные стандарты и политики:

1. ISO 27001. Международный стандарт для управления информационной безопасностью. Он требует от организаций реализации комплексного подхода к киберзащите. Внедрение ISO 27001 в европейских банках привело к снижению инцидентов утечки данных на 23% [5].

2. GDPR (General Data Protection Regulation). Регламент защиты данных в ЕС устанавливает строгие требования к обработке личной информации. Нарушение GDPR в 2022 году обошлось одному из крупных банков в штраф на сумму €1,2 млн. Это подтолкнуло к пересмотру внутренней политики кибербезопасности.

3. NIST Cybersecurity Framework. Национальный институт стандартов и технологий США разработал рамку, включающую 5 ключевых направлений: идентификация, защита, обнаружение, реагирование и восстановление. Применение этой рамки позволило одному из американских банков сократить время реагирования на инциденты с 48 до 12 часов [10, 12, 14, 15].

Конечно, актуальных решений в области обеспечения кибербезопасности в финансовой сфере намного больше, как и примеров их практической реализации:

1. Применение новых мер в России по информационной защите. В условиях санкционного давления и растущих угроз в 2023 году Россия разработала национальную стратегию кибербезопасности. Банки внедряют собственные закрытые сети для предотвращения утечек данных и усиления контроля [16].

2. Эффективное реагирование на атаку. После крупной атаки на Европейский банк в 2023 году, где было украдено 1,3 млн записей клиентов, компания внедрила технологии Endpoint Detection and Response (EDR), которые снизили вероятность повторных атак на 60% [6, 7].

3. Локализация данных. Многие компании, включая российские банки, переходят на локальные серверы, что минимизирует риски утечки данных за пределы страны [16].

Таким образом, совмещение современных технологий, строгих стандартов и проактивных стратегий защиты позволяет эффективно противостоять угрозам и обеспечивать устойчивость финансового сектора.

АНАЛИЗ ВЛИЯНИЯ КИБЕРУГРОЗ НА ФИНАНСОВУЮ ОТЧЕТНОСТЬ

Кибератаки оказывают значительное воздействие на финансовую отчетность компаний. Прямые и косвенные финансовые потери, снижение доверия инвесторов и клиентов, а также необходимость выделения дополнительных средств на восстановление инфраструктуры становятся ключевыми факторами ухудшения финансовых показателей. Основные последствия влияния информационных угроз на финансовую отчетность:

1. Финансовые убытки. В среднем кибератака обходится компаниям в $4,35 млн, включая прямые затраты на устранение последствий, штрафы за утечку данных и судебные издержки. Например, в 2023 году международный банк Santander понес убытки на сумму €10 млн из-за фишинговой атаки, повлиявшей на сотни клиентских счетов.

2. Влияние на прибыль и акции. Исследования показывают, что после крупных инцидентов стоимость акций компаний снижается в среднем на 7,3% в течение месяца. Примером служит утечка данных в Equifax в 2017 году, которая обошлась компании в $1,4 млрд в виде штрафов и компенсирующих выплат.

3. Репутационные риски. Потеря доверия клиентов и партнеров приводит к снижению деловой активности. Согласно отчету IBM, 48% клиентов прекращают сотрудничество с финансовыми организациями после инцидентов утечки данных [6, 7, 10, 17, 18].

Влияние информационных угроз на российский финансовый сектор:

1. Геополитические вызовы. В 2022-2023 годах число кибератак на российские финансовые организации выросло на 97%, по данным Центра мониторинга и реагирования на компьютерные инциденты. Например, в 2023 году атака на крупный российский банк «Тинькофф» («Т-Банк») привела к утечке данных 300 тысяч клиентов. Это вызвало необходимость усиления внутреннего контроля и привлекло внимание регуляторов.

2. Расходы на кибербезопасность. Согласно отчету ЦБ РФ, российские финансовые организации увеличили расходы на защиту IT-инфраструктуры на 25% в 2023 году, что отразилось в увеличении операционных затрат и снижении прибыли.

3. Нормативные меры. Для минимизации рисков кибератак российский регулятор активно продвигает внедрение стандартов защиты данных. Например, к 2024 году обязательным станет использование систем защиты уровня ГОСТ Р 57580 [7, 16, 19].

Таким образом, кибератаки не только увеличивают прямые финансовые затраты организаций, но и подрывают их устойчивость к будущим кризисам. В условиях глобальной цифровизации финансовый сектор должен адаптировать свои стратегии управления рисками, делая акцент на внедрение инноваций и соблюдение строгих стандартов безопасности.

ЭФФЕКТИВНОСТЬ ВНЕДРЕНИЯ МЕР КИБЕРБЕЗОПАСНОСТИ В ФИНАНСОВОМ СЕКТОРЕ

Bank of America с 2019 года внедрил систему на основе машинного обучения для выявления мошеннических транзакций. В результате:

- снижение уровня мошенничества на 50% за первые два года.
- экономия более $150 млн благодаря предотвращенным атакам.

В 2022 году HSBC внедрил многофакторную аутентификацию и технологию поведенческой биометрии. Это позволило уменьшить количество случаев фишинга на 36% и сократить время реакции на инциденты с 24 до 6 часов.

В 2023 году 60% крупных финансовых организаций ЕС, сертифицированных по ISO 27001, сообщили о снижении компьютерных инцидентов на 23% в сравнении с 2022 годом.

Азиатский банк, внедривший систему EDR в 2022 году, сократил среднее время обнаружения угрозы с 35 до 6 часов, что позволило предотвратить утечку данных 2 миллионов клиентов [3, 6, 7, 15, 20, 21].

В 2023 году в России внедрение системы централизованного мониторинга киберугроз (проект ФСТЭК) помогло снизить число успешных атак на банковский сектор на 18% и обеспечить более оперативное реагирование на атаки, сокращая время устранения последствий с 48 до 12 часов.

Крупный российский банк «Сбер» реализовал систему на базе искусственного интеллекта для анализа транзакций, сократив финансовые потери от мошенничества на 22% в 2022 году и увеличив скорость проверки подозрительных транзакций на 30%.

В 2023 году российские банки увеличили расходы на кибербезопасность на 25%. Одной из мер стало внедрение платформ DLP (Data Loss Prevention), что позволило снизить утечки конфиденциальных данных на 14%. Также банки, перешедшие на локальные серверы, отметили снижение числа атак, связанных с международными хакерскими группами, на 25% [22, 23].

Говоря об общем экономическом эффекте, внедрение проактивных мер позволило финансовым организациям по всему миру сократить средние убытки от атак на 40% с 2020 по 2023 год [7].

Исходя из вышеперечисленных примеров, можно уверенно сказать, что эффективность мер кибербезопасности подтверждена на примерах как международных, так и российских организаций. Ключевым фактором остается использование современных технологий (AI, EDR, биометрия) и адаптация международных стандартов к локальным условиям. Успешный опыт применения таких решений свидетельствует о том, что комплексный подход к киберзащите минимизирует потери и повышает устойчивость финансового сектора.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

В результате исследования определены основные киберугрозы для финансового сектора, включая фишинг, атаки на программные интерфейсы и утечку данных, с подтвержденным ростом их частоты на 20% за последний год. Проведен анализ международных стандартов (ISO 27001, NIST), их адаптации в российских условиях, что укрепляет нормативную основу информационной безопасности. Выявлены и подробно рассмотрены инновационные технологии (искусственный интеллект, EDR, блокчейн), которые демонстрируют эффективность, снижая число успешных атак на 20–40%. Особое внимание уделено локализации данных и переходу на национальные решения в России, что сократило внешние угрозы на 18%. Рекомендации для финансовых организаций включают внедрение современных технологий, соблюдение стандартов и усиление внутреннего контроля, что подтверждает значимость комплексного подхода для устойчивости финансового сектора.

ЗАКЛЮЧЕНИЕ

Современный финансовый сектор активно трансформируется в условиях цифровизации, однако кибератаки на финансовые учреждения продолжают расти, их доля в общем числе инцидентов составляет около 20%. Прямые финансовые убытки от атак измеряются миллиардами долларов, не учитывая долгосрочных репутационных потерь. Анализ угроз, решений и последствий компьютерных инцидентов показывает, что внедрение инновационных технологий и нормативных стандартов существенно снижает риски для финансовых организаций. Эффективные меры, такие как использование AI, EDR и блокчейна, позволяют сократить убытки на 20–40% [20, 21].

Международные стандарты, такие как ISO 27001 и NIST Cybersecurity Framework, играют важную роль в систематизации подходов к безопасности. Однако их адаптация под локальные условия, как это сделано в России, становится важным фактором для повышения эффективности защитных механизмов [5, 6, 7].

Примеры использования искусственного интеллекта, облачных технологий и методов шифрования доказывают свою результативность. В частности, переход на локализацию данных в России снизил вероятность международных угроз на 25%, а интеграция AI позволила крупнейшим банкам снизить уровень мошенничества более чем на 20% [21].

Российский финансовый сектор столкнулся с ростом кибератак в условиях санкционного давления. Успешное внедрение национальных стратегий, включая системы централизованного мониторинга, продемонстрировало значительное снижение успешных атак (на 18%). Увеличение инвестиций в локальные разработки и переход на внутренние серверы укрепляют устойчивость к внешним угрозам [19, 22, 23].

Основные рекомендации, которые можно выделить:

1. Продолжать инвестиции в инновационные решения, такие как AI, блокчейн и облачные технологии.
2. Укреплять международное сотрудничество в области кибербезопасности для обмена опытом.
3. В России усилить контроль за выполнением национальных стандартов и развитие локальных решений.

Комплексный подход, сочетающий инновации, стандарты и государственные меры, станет ключом к обеспечению устойчивости финансового сектора перед лицом информационных угроз.

СПИСОК ЛИТЕРАТУРЫ

1. World Economic Forum. Global Risks Report 2023.
2. PwC. Global Digital Trust Insights Survey 2023.
3. SentinelOne. Cybersecurity in Finance. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-in-finance/.

4. Аналитический центр при Правительстве Российской Федерации. Цифровая экономика: вызовы и перспективы 2023.
5. IMF Blog. Rising Cyber Threats Pose Serious Concerns for Financial Stability. URL: https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability.
6. Varonis. Cybersecurity Statistics and Trends [updated 2024]. URL: https://www.varonis.com/blog/cybersecurity-statistics.
7. Cobalt. Top Cybersecurity Statistics for 2024. URL: https://www.cobalt.io/blog/cybersecurity-statistics-2024.
8. Kaspersky Lab. The State of Cybersecurity in 2023.
9. AARU Digital Commons. Securing Financial Data Storage: A Review of Cybersecurity Challenges and Solutions. URL: https://digitalcommons.aaru.edu.jo/cgi/viewcontent.cgi?article=3459&context=amis.
10. McKinsey & Company. The Cyber Clock is Ticking: Derisking Emerging Technologies in Financial Services. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services.
11. Международная конференция по информационной безопасности, 2023. Using Blockchain and Quantum Encryption in Finance.
12. ISACA. The Future of Cybersecurity in Financial Institutions.
13. IBM Security. Top Data Protection Methods in Financial Services.
14. NIST. Cybersecurity Framework. URL: https://www.nist.gov/cyberframework.
15. ResearchGate. Securing Financial Data Storage: A Review of Cybersecurity Challenges and Solutions. URL: https://www.researchgate.net/publication/379431574_Securing_financial_data_storage_A_review_of_cybersecurity_challenges_and_solutions.
16. Центробанк Российской Федерации. Отчет по информационной безопасности в финансовом секторе за 2023 год.
17. Cybersecurity Ventures. Cybercrime Report 2023.
18. IBM Security Report. The Cost of a Data Breach, 2023.
19. Федеральная служба по техническому и экспортному контролю (ФСТЭК). Положение о защите информации в финансовом секторе, 2023.
20. Microsoft Azure. Artificial Intelligence in Financial Services: Enhancing Cybersecurity.
21. Deloitte. The Financial Services Cybersecurity Trends 2023.
22. Министерство цифрового развития, связи и массовых коммуникаций РФ. Отчет о реализации национальной программы «Цифровая экономика», 2023.
23. Центробанк Российской Федерации. Отчет о состоянии информационной безопасности в 2023 году.

INFORMATION SECURITY IN THE FINANCIAL SECTOR: CHALLENGES, SOLUTIONS AND IMPACT ON THE QUALITY OF FINANCIAL STATEMENTS

I.A. Shabanov, student
e-mail: shabanchick2002@gmail.com
Kaliningrad State University

In this scientific work, the theoretical and practical aspects of information security in the financial sector are considered, the main threats, challenges and implemented solutions are emphasized. The research includes an analysis of international cybersecurity standards (ISO 27001, NIST Cybersecurity Framework), innovative technologies (artificial intelligence, blockchain, quantum encryption) and successful cases of their application. Special attention is paid to the situation in Russia,

including national strategies, regulatory regulation and adaptation of global solutions to local conditions. The findings confirm the effectiveness of the implementation of comprehensive cyber protection measures that minimize financial losses and ensure the stability of the banking system.

Key words: information security, cybersecurity, financial sector, threats, information security standards, artificial intelligence, blockchain, quantum encryption, ISO 27001, NIST Cybersecurity Framework