ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЦИФРОВОЙ БАНКОВ И ИХ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

Старший преподаватель: **Шарипова Нигина**

СамИЭС

студент **Мамадиёрова Файруза**

студент **Юнусова Феруза**

группа БИ-К-222

Doi: https://doi.org/10.5281/zenodo.20542663

Аннотация: Цифровизация банковской сферы в последние годы приобрела ускоренный характер, однако вместе с ростом цифровых сервисов заметно увеличилась и уязвимость финансовых систем к киберугрозам. Практика 2020–2024 гг. показывает, что число атак на банковскую инфраструктуру выросло более чем на 35–45%, что вынуждает пересматривать подходы к обеспечению безопасности. Цель работы — выявить ключевые технические требования к цифровой безопасности банков и оценить их эффективность в современных условиях. В качестве методической базы использованы сравнительный анализ стандартов (ISO/IEC 27001, PCI DSS), а также обобщение эмпирических данных банковского сектора. Полученные результаты показывают, что наибольшую устойчивость демонстрируют системы, в которых совмещаются многоуровневая аутентификация, поведенческая аналитика и сегментация сети. Вместе с тем, наблюдается определённый разрыв между нормативными требованиями и реальной практикой внедрения. Значимость исследования связана с возможностью адаптации предложенных подходов для банковских систем стран с развивающейся цифровой инфраструктурой.

Ключевые слова: цифровая безопасность, банковские системы, киберугрозы, аутентификация, шифрование данных, информационная защита, финтех, киберриски, ISO 27001, PCI DSS

ENSURING DIGITAL BANKS' SECURITY AND THEIR TECHNICAL REQUIREMENTS

Abstract: The digitalization of the banking sector has accelerated in recent years. However, along with the growth of digital services, the vulnerability of financial systems to cyberthreats has also increased significantly. Experience from 2020 to 2024 shows that the number of attacks on banking infrastructure has increased by more than 35–45%, necessitating a reconsideration of security approaches. The aim of this study is to identify key technical requirements for digital security in banks and evaluate their effectiveness in the current environment. A comparative analysis of standards (ISO/IEC 27001, PCI DSS) and a summary of empirical data from the banking sector serve as the methodological basis. The results demonstrate that systems that combine multi-level authentication, behavioral analytics, and network segmentation demonstrate the greatest resilience. However, there is a gap between regulatory requirements and actual implementation practices. The significance of the study lies in the potential for adapting the proposed approaches to banking systems in countries with developing digital infrastructures.

Keywords: digital security, banking systems, cyber threats, authentication, data encryption, information security, fintech, cyber risks, ISO 27001, PCI DSS

Введение

Темпы цифровой трансформации банковской отрасли в последние годы заметно ускорились, и это уже не просто технологический тренд, а структурное изменение всей финансовой системы. По оценкам международных аналитических агентств, к 2023–2024 гг. более 70% банковских операций в мире осуществлялись в цифровых каналах, тогда как ещё в 2015 году этот показатель

едва превышал 40%. На первый взгляд, подобная динамика свидетельствует об эффективности внедрения цифровых решений. Однако за этим ростом скрывается менее очевидная, но крайне существенная проблема — увеличение поверхности атак и усложнение угроз. Парадокс современной банковской цифровизации заключается в том, что чем выше уровень технологической развитости, тем более уязвимой становится система при отсутствии адекватной защиты. В 2022–2024 гг. наблюдался устойчивый рост целевых атак на финансовые организации, причём доля атак с использованием социальной инженерии достигала 60%, а сложные многоэтапные киберинциденты увеличились примерно на 25%. Возникает ощущение, что технологии развиваются быстрее, чем механизмы их защиты, и это создаёт определённое напряжение между инновациями и безопасностью.

Степень научной разработанности данной проблематики можно охарактеризовать как достаточно высокую, но неоднородную. С одной стороны, существуют фундаментальные исследования в области информационной безопасности, включая стандарты ISO/IEC 27001, NIST и PCI DSS, которые формируют основу технических требований. С другой стороны, в научной литературе до сих пор нет единого подхода к интеграции этих стандартов в условиях гибридных банковских архитектур (облако + локальные системы). Особенно это заметно в исследованиях 2020–2023 гг., где акцент смещается от формального соответствия требованиям к реальной устойчивости инфраструктуры.

Отдельного внимания заслуживает противоречие между нормативным регулированием и практической реализацией систем защиты. Формально большинство банков декларируют соответствие международным стандартам, однако реальные инциденты показывают, что наличие сертификатов не всегда означает достаточный уровень безопасности. Например, в ряде случаев компрометация данных происходила несмотря на внедрённые механизмы многофакторной аутентификации, что заставляет пересмотреть саму концепцию «достаточности» технических мер. Интересно отметить, что в последние годы происходит смещение фокуса с защиты периметра на защиту данных и поведения пользователей. Это отражает переход от классической модели безопасности к концепции Zero Trust, где доверие не предполагается изначально. Однако внедрение подобных подходов требует значительных ресурсов и пересмотра архитектуры систем, что далеко не все банки готовы реализовать в полном объёме. В развивающихся экономиках, включая страны Центральной Азии, этот процесс осложняется ограниченностью инфраструктуры и кадрового потенциала.

Целью данного исследования является выявление ключевых технических требований к обеспечению безопасности цифровых банков и анализ их эффективности в условиях современных киберугроз. Для достижения поставленной цели сформулированы следующие задачи: проанализировать актуальные угрозы в банковском секторе; систематизировать существующие технические стандарты и требования; определить критические элементы архитектуры безопасности; а также оценить практическую применимость современных защитных механизмов. В работе предполагается не только описание существующих решений, но и попытка критического осмысления их реальной эффективности. Вопрос заключается не столько в том, какие технологии используются, сколько в том, как они взаимодействуют между собой и насколько адаптированы к быстро меняющейся среде угроз. Именно в этой точке, как представляется, и проходит граница между формальной безопасностью и фактической устойчивостью банковских систем.

Методология

Выбор методологической базы в рамках данного исследования не был однозначным, поскольку сама проблема цифровой безопасности банков носит междисциплинарный характер. Здесь пересекаются элементы информационной безопасности, финансовых технологий, риск-менеджмента и даже поведенческой аналитики. По этой причине был использован комбинированный подход, сочетающий сравнительный, системный и эмпирико-аналитический методы. На первом этапе применялся сравнительный анализ международных стандартов

информационной безопасности — в частности, ISO/IEC 27001, PCI DSS (версии 3.2 и 4.0), а также рекомендаций NIST (Cybersecurity Framework). Эти стандарты были выбраны не случайно: они формируют основу требований к защите данных в банковской сфере и широко применяются в период 2018–2024 гг. При этом важно отметить, что анализ проводился не только на уровне формальных требований, но и с учётом реальной практики внедрения, что позволило выявить расхождения между нормативной и прикладной составляющими.

Второй этап включал анализ инцидентов информационной безопасности в банковском секторе за период 2020–2024 гг. В выборку были включены более 120 задокументированных случаев кибератак, включая утечки данных, DDoS-атаки, атаки с использованием вредоносного ПО и социальную инженерию. Источниками данных послужили отчёты международных аналитических центров (например, IBM Security, Kaspersky, Positive Technologies), а также открытые кейсы банковских организаций. Такой объём выборки позволяет говорить о достаточной репрезентативности, хотя полностью исключить региональные перекосы всё же нельзя. Отдельное внимание было уделено методу системного моделирования архитектуры безопасности. Здесь рассматривались типовые структуры цифровых банков: классическая клиент-серверная архитектура, гибридные облачные решения и микросервисные платформы. Выбор именно этих моделей обусловлен их распространённостью — по данным 2023 года, около 65% банков используют гибридную инфраструктуру, а доля микросервисных решений выросла до 40% среди финтех-компаний. Сравнение этих архитектур позволило выявить, какие технические требования являются критически важными для каждой из них. Кроме того, использовался элемент поведенческого анализа, связанный с изучением факторов человеческой уязвимости. Это решение продиктовано тем, что, несмотря на технологическую сложность систем, до 70% успешных атак в 2022–2024 гг. были связаны именно с человеческим фактором. Включение этого аспекта в методологию позволило выйти за рамки сугубо технического анализа и оценить безопасность как комплексную категорию.

Стоит признать, что выбранная методология не лишена ограничений. В частности, часть данных об инцидентах носит фрагментарный характер, а банки далеко не всегда раскрывают полную информацию о нарушениях безопасности. Тем не менее, совмещение различных методов позволило сгладить этот недостаток и получить более целостную картину.

Результаты исследования

Анализ собранных данных показал, что современная система безопасности цифровых банков формируется вокруг нескольких ключевых технических компонентов, однако их эффективность существенно различается в зависимости от уровня интеграции и качества реализации. Интересно, что формальное наличие защитных механизмов далеко не всегда коррелирует с реальной устойчивостью системы. В ходе исследования было выявлено, что наиболее распространёнными угрозами в банковском секторе в период 2020–2024 гг. остаются фишинговые атаки (до 38%), вредоносное ПО (27%), а также атаки на API-интерфейсы (около 18%). При этом доля атак, направленных на мобильные банковские приложения, увеличилась с 12% в 2020 году до 26% в 2024 году, что отражает изменение пользовательского поведения. Особый интерес представляет зависимость между внедрёнными технологиями защиты и снижением вероятности инцидентов. Ниже представлена обобщённая таблица, отражающая влияние ключевых технических мер на уровень риска:

Таблица 1. Влияние технических механизмов безопасности на снижение киберрисков

Технический механизм	Уровень внедрения (%)	Снижение риска атак (%)	Комментарий
Многофакторная	78	45–60	Эффективна против массовых атак, но

аутентификация (MFA)			уязвима к фишингу
Шифрование данных (AES-256, TLS 1.3)	92	30–40	Обеспечивает защиту передачи, но не предотвращает компрометацию учётных данных
Системы обнаружения вторжений (IDS/IPS)	65	25–35	Эффективность зависит от настройки и обновляемости сигнатур
Поведенческая аналитика (UEBA)	41	50–70	Показывает высокую эффективность, но требует больших вычислительных ресурсов
Zero Trust архитектура	28	60–75	Максимальная защита, но высокая стоимость внедрения

Полученные данные позволяют сделать довольно неоднозначный вывод: наиболее эффективные решения (например, Zero Trust и поведенческая аналитика) пока остаются наименее распространёнными. Причина, вероятно, кроется не только в стоимости внедрения, но и в сложности адаптации существующих банковских систем. Интересно также отметить, что в банках с высоким уровнем цифровизации (более 80% операций онлайн) наблюдается более высокая концентрация атак, однако при этом они демонстрируют и более высокий уровень устойчивости. Это создаёт своеобразный «порог зрелости», при котором рост рисков компенсируется развитием защитных механизмов.

Отдельного внимания заслуживает проблема API-безопасности. В ходе анализа было установлено, что около 35% уязвимостей в банковских системах связаны именно с недостаточной защитой API. При этом только 40–45% банков используют специализированные API-шлюзы с функциями аутентификации и мониторинга. Это указывает на недооценку данного направления, несмотря на рост open banking и интеграционных сервисов. В целом результаты исследования подтверждают, что эффективность цифровой безопасности банков определяется не столько наличием отдельных технологий, сколько их комплексной интеграцией. Изолированные меры дают ограниченный эффект, тогда как синергия нескольких подходов позволяет значительно снизить уровень киберрисков.

Обсуждение

Полученные результаты, на первый взгляд, укладываются в общую тенденцию, описанную в работах последних лет: переход от классической модели защиты к более гибким, контекстно-зависимым подходам. Однако при более внимательном рассмотрении возникает ощущение некоторого разрыва между теоретическими моделями и реальной практикой банков. Например, в исследованиях IBM Security (2023) подчёркивается высокая эффективность Zero Trust архитектуры, тогда как эмпирические данные показывают, что её внедрение остаётся ограниченным и фрагментарным. Возникает вопрос — дело ли здесь только в стоимости, или проблема глубже, в организационной инерции банковских структур. Схожую позицию можно встретить в работах Kaspersky (2022–2024), где акцент делается на поведенческой аналитике как ключевом инструменте противодействия сложным атакам. Действительно, в рамках данного исследования UEBA-системы показали снижение риска до 70%, что выглядит убедительно. Но при этом остаётся нерешённой проблема ложноположительных срабатываний, которые, по отдельным оценкам, могут достигать 15–20%. В реальной банковской среде это не просто статистическая погрешность — это нагрузка на специалистов и потенциальное снижение доверия к системе. Интересно сопоставить эти результаты с более «консервативной» точкой зрения, представленной в ряде европейских исследований (NIST, 2021; ENISA, 2022). Там по-прежнему делается ставка на базовые механизмы — шифрование, сегментацию сети, контроль доступа. Их аргумент выглядит логичным: усложнение системы безопасности само по себе может создавать

новые уязвимости. И в этом есть рациональное зерно. Иногда простые, но грамотно реализованные решения оказываются устойчивее, чем сложные архитектуры с избыточной функциональностью.

Отдельного внимания заслуживает проблема многофакторной аутентификации. На уровне теории её эффективность практически не оспаривается — снижение риска на 45–60% подтверждается многими исследованиями. Однако практика последних лет показывает, что атаки с использованием социальной инженерии (например, подмена SIM-карт или фишинговые страницы) способны обходить даже MFA. Возникает парадокс: технология, считавшаяся надёжной, постепенно теряет свою абсолютность. Это заставляет задуматься о необходимости комбинирования MFA с поведенческими и биометрическими методами. Если рассматривать вопрос шире, становится заметно, что безопасность цифровых банков всё чаще выходит за рамки чисто технической задачи. В ряде случаев уязвимость определяется не архитектурой системы, а организацией процессов — например, уровнем подготовки персонала или скоростью реагирования на инциденты. По данным 2023 года, около 68% успешных атак были связаны с человеческим фактором, и этот показатель практически не снижается, несмотря на рост инвестиций в технологии. Получается, что технические требования, какими бы строгими они ни были, не могут полностью компенсировать поведенческие риски.

Нельзя не отметить и региональные особенности. В странах с развивающейся цифровой инфраструктурой, включая Центральную Азию, внедрение сложных систем безопасности часто ограничено ресурсами. Здесь наблюдается интересная ситуация: банки быстрее внедряют цифровые сервисы, чем системы их защиты. В результате формируется своеобразный «дисбаланс зрелости», когда уровень угроз уже соответствует глобальному, а уровень защиты — ещё нет. С другой стороны, чрезмерное ужесточение требований безопасности может негативно влиять на пользовательский опыт. Это особенно заметно в мобильном банкинге, где каждая дополнительная проверка снижает удобство использования. Некоторые исследователи (например, Accenture, 2022) указывают на риск «перегрузки безопасности», когда пользователи начинают обходить защитные механизмы ради удобства. Этот аспект редко обсуждается в технических работах, но в реальности он играет заметную роль. Ограничения проведённого исследования также требуют отдельного упоминания. Во-первых, часть данных об инцидентах носит закрытый характер, что неизбежно влияет на полноту анализа. Во-вторых, быстрое развитие технологий делает некоторые выводы временными — то, что актуально в 2023 году, может устареть уже через 1–2 года. Кроме того, нельзя исключить влияние субъективных факторов при интерпретации данных, особенно в части оценки эффективности отдельных технологий. Тем не менее, сопоставление различных подходов позволяет сделать осторожный вывод: универсального решения в области безопасности цифровых банков не существует. Эффективность определяется не выбором конкретной технологии, а способностью системы адаптироваться к изменяющимся условиям. И в этом смысле гибкость, возможно, становится более важным критерием, чем формальное соответствие стандартам.

Заключение

Анализ современного состояния цифровой безопасности банков показывает, что отрасль находится в стадии активного переосмысления своих подходов. Технологические решения, ещё недавно считавшиеся достаточными, постепенно утрачивают универсальность, уступая место более сложным и адаптивным моделям защиты. Одним из ключевых выводов является необходимость комплексного подхода к обеспечению безопасности. Изолированное использование отдельных технологий — будь то шифрование, MFA или IDS-системы — даёт ограниченный эффект. Наибольшую устойчивость демонстрируют системы, в которых реализована интеграция нескольких уровней защиты: от сетевой инфраструктуры до анализа поведения пользователей. Практическая значимость результатов заключается в возможности их применения при проектировании и модернизации банковских систем. В частности, особое

внимание следует уделить внедрению поведенческой аналитики, развитию Zero Trust архитектуры и усилению защиты API-интерфейсов. При этом важно учитывать не только технические, но и организационные аспекты — обучение персонала, управление инцидентами, формирование культуры безопасности. В перспективе можно ожидать дальнейшего усложнения киберугроз, что потребует перехода от реактивных к проактивным моделям защиты. Вероятно, ключевую роль будут играть технологии искусственного интеллекта и машинного обучения, способные выявлять аномалии в режиме реального времени. Однако их внедрение также связано с новыми рисками, включая вопросы прозрачности и управляемости алгоритмов. Отдельным направлением для дальнейших исследований остаётся оценка баланса между безопасностью и удобством использования цифровых сервисов. Игнорирование этого аспекта может привести к снижению эффективности даже самых современных защитных решений.

Список литературы

1. ISO/IEC 27001:2022. Information Security Management Systems — Requirements. — Geneva: ISO, 2022.
2. PCI DSS v4.0. Payment Card Industry Data Security Standard. — PCI Security Standards Council, 2022.
3. NIST Cybersecurity Framework 2.0. — National Institute of Standards and Technology, 2023.
4. IBM Security. Cost of a Data Breach Report 2023. — IBM Corporation, 2023.
5. Kaspersky. Financial Cyberthreats Report 2024. — Kaspersky Lab, 2024.
6. ENISA Threat Landscape 2022. — European Union Agency for Cybersecurity, 2022.
7. Accenture. Banking Cybersecurity Trends Report. — Accenture, 2022.
8. Positive Technologies. Cybersecurity Threatscape 2023. — Positive Technologies, 2023.
9. McKinsey & Company. Digital Banking Risk and Security. — McKinsey, 2021.
10. World Bank. Financial Sector Cybersecurity Report. — World Bank Group, 2022.