УДК 004.056
DOI 10.26118/2782-4586.2026.75.46.098

Хобяков Денис Дмитриевич
Томский государственный университет систем управления и радиоэлектроники

Киберугрозы как ключевой риск экономической безопасности: политика банка России в области защиты финансовой инфраструктуры и данных

Аннотация. В статье исследуются киберугрозы как ключевой риск экономической безопасности Российской Федерации в условиях цифровой трансформации финансового сектора. Рассматривается политика Банка России в области защиты финансовой инфраструктуры и данных, включая нормативно-правовую базу, стратегические инициативы, а также механизмы мониторинга и реагирования на инциденты (в частности, деятельность ФинЦЕРТ). Проведён анализ эволюции киберугроз, их классификации и влияния на стабильность финансовой системы. На основе изучения реальных инцидентов и выявленных уязвимостей оценена эффективность мер регулятора. Сформулированы практические рекомендации по оптимизации регуляторных требований, развитию международного сотрудничества и внедрению современных технологий защиты данных. Цель работы — предложить научно обоснованные меры для повышения киберустойчивости финансового сектора и обеспечения долгосрочной экономической безопасности России.

Ключевые слова: экономическая безопасность, киберугрозы, кибербезопасность, Банк России, финансовая инфраструктура, ФинЦЕРТ, фишинг, DDoS-атаки, нормативное регулирование, международное сотрудничество.

Khobyakov Denis Dmitrevich
Tomsk State University of Control System and Radio Electronics

Cyber threats as a key risk to economic security: the policy of the bank of Russia in the field of protection of financial infrastructure and data

Annotation. This article examines cyberthreats as a key risk to the economic security of the Russian Federation amid the digital transformation of the financial sector. It examines the Bank of Russia's policy on protecting financial infrastructure and data, including the regulatory framework, strategic initiatives, and incident monitoring and response mechanisms (in particular, the activities of FinCERT). An analysis of the evolution of cyberthreats, their classification, and their impact on the stability of the financial system is provided. Based on a study of real incidents and identified vulnerabilities, the effectiveness of the regulator's measures is assessed. Practical recommendations are formulated for optimizing regulatory requirements, developing international cooperation, and implementing modern data protection technologies. The goal of the paper is to propose scientifically based measures to enhance the cyber resilience of the financial sector and ensure Russia's long-term economic security.

Keywords: economic security, cyberthreats, cybersecurity, Bank of Russia, financial infrastructure, FinCERT, phishing, DDoS attacks, regulatory framework, international cooperation.

Введение.

В современный период фиксируется значительный рост как частоты, так и изощренности кибератак, в первую очередь в финансовой сфере. Эта тенденция обусловила трансформацию киберугроз в фактор системного риска для экономической безопасности

страны, что подтверждается данными за 2023 год. Атаки на банковские и платежные инфраструктуры оказывают дестабилизирующее влияние на ключевые экономические процессы и подрывают доверие к финансовым институтам. Распространение целевых угроз, включая фишинг, программы-вымогатели и компрометацию цепочек поставок, свидетельствует об их использовании в качестве инструмента экономической дестабилизации. Ущерб от таких инцидентов не ограничивается прямыми финансовыми потерями, затрагивая репутационную сферу и общую устойчивость экономики. Указанные обстоятельства актуализируют необходимость признания киберугроз в качестве одного из центральных вызовов, требующего консолидированного и стратегического ответа со стороны регулирующих органов.

Будучи основным регулятором финансового рынка, Банк России сформировал и реализует комплексный набор мер, направленных на обеспечение безопасности финансовой инфраструктуры и защиту данных. Данные меры охватывают принятие нормативно-правовых актов, разработку отраслевых стандартов информационной безопасности и внедрение систем мониторинга киберинцидентов. Тем не менее, сохраняется ряд уязвимостей, связанных с высокой скоростью эволюции методов атак и постоянным усложнением киберугроз. Фактические инциденты, несмотря на предпринимаемые регулятором усилия, продолжают демонстрировать наличие пробелов в системе защиты. К числу таких проблем относятся недостаточная гибкость в адаптации к новым формам угроз и трудности в достижении единообразного внедрения защитных механизмов всеми участниками рынка. Подобные недостатки порождают риски нарушения функционирования критически значимых экономических процессов и обусловливают потребность в перманентном анализе и корректировке действующей политики в области кибербезопасности.

Настоящее исследование ставит своей целью проведение комплексной оценки эффективности политики Банка России, направленной на защиту финансовой инфраструктуры и данных от киберугроз в контексте обеспечения экономической безопасности. На основе идентифицированных уязвимостей и пробелов в применяемых мерах планируется сформулировать практические рекомендации по оптимизации регуляторного подхода для минимизации сопутствующих рисков.

Для достижения обозначенной цели в работе последовательно решаются следующие исследовательские задачи:

1. Исследование эволюции киберугроз и анализ их воздействия на экономическую безопасность Российской Федерации, с фокусом на особенности финансового сектора.
2. Анализ действующей нормативно-правовой базы и ключевых инициатив Банка России в сфере кибербезопасности.
3. Оценка результативности реализованных регуляторных мер на основе анализа актуальных киберинцидентов, позволяющая выявить системные уязвимости.
4. Разработка предложений по усилению защищенности финансовой системы от современных киберугроз на основе полученных результатов.

Практическая значимость работы заключается в том, что её выводы и рекомендации могут быть применены для совершенствования стратегий управления киберрисками в финансовом секторе. Реализация предложенных мер будет способствовать повышению долгосрочной устойчивости национальной экономики в условиях интенсификации цифровой трансформации и усложнения угроз.

Основная часть

Материалы и методы исследования

Для достижения поставленной цели и решения исследовательских задач в работе применен комплекс общенаучных и специальных методов, обеспечивающих достоверность и объективность результатов. Методологическую основу составили:

1. Методы теоретического анализа:

- **Системный анализ:** позволил исследовать политику Банка России как целостную систему, состоящую из нормативно-правовых, организационных и технических компонентов, и оценить её взаимодействие с национальной системой кибербезопасности.
- **Сравнительно-правовой анализ:** применялся для изучения эволюции и содержания ключевых нормативных актов (Федеральный закон № 187-ФЗ, концепция кибербезопасности финансового сектора) и выявления пробелов в регулировании.
- **Классификация и категоризация:** Использованы для структурирования типов киберугроз, уязвимостей (технические, организационные, процедурные) и механизмов реагирования.

2. Эмпирические и прикладные методы:

- **Анализ документов и вторичных данных:** Проведен детальный контент-анализ:
  - **Официальных отчетов и статистики:** Публичных материалов Банка России, ФинЦЕРТ, отчетов о киберинцидентах в финансовом секторе.
- **Анализ конкретных случаев:** на основе открытых данных были отобраны и детально проанализированы репрезентативные случаи успешных кибератак на российские финансовые организации за период 2020-2024 гг. Анализ фокусировался на применяемых векторах атак, выявленных уязвимостях и эффективности мер реагирования со стороны регулятора и самих организаций.
- **Синтез и обобщение:** на основе полученных данных были сформулированы системные выводы об эффективности политики Банка России, выявлены повторяющиеся уязвимости и разработаны практические рекомендации.

Этапы исследования:

1. **Подготовительный этап:** Определение цели, задач, сбор и систематизация теоретического и нормативного материала.
2. **Аналитический этап:** Проведение анализа документов, классификация угроз и уязвимостей, оценка инцидентов.
3. **Обобщающий этап:** Интерпретация результатов, формулирование выводов, разработка рекомендаций по оптимизации политики.

Классификация киберугроз в финансовом секторе

Эволюционный путь киберугроз в финансовой сфере берёт начало от локальных инцидентов, связанных с вирусами и червями, которые затрагивали преимущественно отдельные компьютерные системы. Со временем характер атак трансформировался в сторону деятельности организованных преступных и коммерческих группировок, применяющих ботнеты и специализированное вредоносное программное обеспечение для осуществления масштабных хищений. Глубинная цифровизация и интеграция информационных систем способствовали возникновению устойчивых целевых операций, нацеленных на длительное скрытое присутствие в инфраструктуре и последующую фильтрацию данных. Современные модели атак реализуются по многоступенчатым сценариям, задействующим эксплойты нулевого дня, методы сложной обфускации кода и скоординированные действия различных субъектов. Интенсификация и усложнение атак стимулируются такими факторами, как рост объёмов цифровых транзакций, распространение облачных и мобильных сервисов, а также увеличение числа сторонних участников в экосистеме. Эти факторы расширяют поверхность атаки, а сочетание технических средств с методами социальной инженерии повышает вероятность успешного проникновения. Переход к продвинутым постоянным угрозам характеризуется акцентом на обеспечение постоянного доступа, латеральное перемещение по сети и сокрытие следов деятельности, что существенно осложняет процессы обнаружения и реагирования. Указанная тенденция актуализирует потребность в переходе от реактивных подходов к проактивным и многоуровневым стратегиям обеспечения безопасности.

Классификацию угроз в финансовом секторе целесообразно осуществлять по трём основным критериям: источник угрозы (внешний или внутренний), цель атаки (компрометация данных либо нарушение работы инфраструктуры) и применяемые методы реализации. К внешним источникам относятся криминальные формирования, государственные структуры и независимые злоумышленники, в то время как внутренние угрозы связаны с действиями недобросовестных сотрудников или случайными ошибками персонала. Методологический спектр реализации варьируется от фишинга и вредоносного программного обеспечения до DDoS-атак, компрометации цепочек поставок и эксплуатации уязвимостей программного обеспечения. Подобная систематизация способствует более точной оценке рисков и формированию адекватных мер контроля и противодействия.

Финансовый сектор отличается высокой концентрацией критически важной информации, включающей персональные данные клиентов, платёжные реквизиты и финансовую отчётность. Транзакционные системы требуют обеспечения непрерывной доступности и целостности, а высокая степень взаимосвязанности между банковскими институтами увеличивает потенциал каскадного распространения инцидента. В силу исключительной ценности обрабатываемой информации, а также значительных репутационных и регуляторных рисков, финансовые организации являются приоритетными целями как для экономически мотивированных злоумышленников, так и для субъектов, преследующих политические интересы. Указанные особенности обусловливают необходимость разработки и внедрения специализированных защитных механизмов, ориентированных на обеспечение доступности, целостности и конфиденциальности ключевых сервисов.

Влияние киберугроз на экономическую безопасность России

Кибератаки, нацеленные на финансовые организации, влекут за собой существенные прямые экономические издержки. Помимо непосредственного хищения денежных средств, ущерб включает значительные затраты на восстановление функциональности информационных систем. По существующим оценкам, совокупный ежегодный ущерб российского финансового сектора от подобных инцидентов исчисляется миллиардами рублей. Дополнительную финансовую нагрузку создаёт необходимость привлечения профильных специалистов для устранения последствий атак и проведения расследований.

Компрометация критически важных объектов финансовой инфраструктуры порождает системные риски, угрожающие стабильности рынка. Нарушение работы платёжных систем или клиринговых центров способно спровоцировать каскадные сбои у других участников. Подобные инциденты обладают потенциалом парализовать значительные сегменты финансового рынка, подрывая его общую устойчивость, что создаёт угрозу для всей национальной экономической системы.

Учащение успешных кибератак оказывает деструктивное влияние на доверие клиентов к финансовым институтам. Утрата репутации ведёт к оттоку клиентской базы и сокращению объёмов операций. Снижение инвестиционной привлекательности сектора осложняет привлечение капитала и замедляет его развитие, что в долгосрочной перспективе негативно сказывается на конкурентоспособности национальной финансовой системы.

Киберугрозы всё активнее используются в качестве инструмента гибридного воздействия в контексте геополитической конфронтации. Целенаправленные атаки на финансовую инфраструктуру могут преследовать цели дестабилизации экономики государства. Подобные действия, мотивированные политическими или идеологическими причинами, представляют собой некоммерческие угрозы, последствия которых выходят за рамки финансового сектора, затрагивая сферу национальной безопасности в целом.

Основные виды кибератак на финансовую инфраструктуру РФ

Фишинг и целенаправленные атаки на персонал являются одними из наиболее распространённых и результативных способов компрометации банковских систем. Указанные методы опираются на приёмы социальной инженерии, предназначенные для

манипулирования сотрудниками с целью получения несанкционированного доступа к конфиденциальной информации или осуществления финансовых операций. Злоумышленники проводят детальный анализ организационной структуры и поведенческих моделей сотрудников, что позволяет повысить убедительность атак. В рамках фишинговых кампаний создаются поддельные веб-ресурсы и электронные сообщения, имитирующие официальные коммуникации финансовых институтов или государственных ведомств. Атаки такого типа часто предполагают имитацию личности руководителей или партнёров для инициации несанкционированных переводов средств или разглашения конфиденциальных данных. Постоянная эволюция данных угроз обусловливает необходимость непрерывного повышения уровня осведомлённости персонала и внедрения многофакторных систем аутентификации для снижения соответствующих рисков.

Вредоносное программное обеспечение занимает центральное место в арсенале киберпреступников, специализирующихся на атаках на финансовый сектор. Специализированные банковские трояны созданы для хищения платёжных реквизитов, учётных данных и иной конфиденциальной информации пользователей финансовых услуг. Существенную угрозу также представляет программное обеспечение-вымогатель, которое осуществляет шифрование данных или блокировку доступа к информационным системам с последующим требованием выкупа за их восстановление.

DDoS-атаки (распределённый отказ в обслуживании) служат эффективным инструментом дестабилизации операционной деятельности финансовых организаций. Эти атаки нацелены на перегрузку сетевой инфраструктуры или серверов процессинговых центров и систем онлайн-банкинга путём создания чрезмерного потока запросов. В результате легитимные пользователи лишаются доступа к сервисам, что влечёт за собой значительные финансовые и репутационные издержки как для самих банков, так и для их клиентов.

Нормативно-правовая база регулирования кибербезопасности в финансовом секторе

Нормативно-правовой фундамент регулирования кибербезопасности в финансовом секторе Российской Федерации складывается из ряда основополагающих документов. Центральное место среди них занимает Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», закладывающий правовые основы защиты объектов КИИ, к числу которых отнесены и ключевые элементы финансовой системы. Данный акт регламентирует базовые принципы, разграничивает полномочия государственных органов и определяет обязанности субъектов КИИ в части предупреждения компьютерных инцидентов, будучи нацеленным на ограждение жизненно важных систем от деструктивных воздействий.

Важную роль в данной системе играют Стандарты Банка России (СБКФТ), детализирующие требования по информационной безопасности для кредитных организаций и иных участников финансового рынка. Эти стандарты охватывают широкий круг вопросов — от организации управления доступом до построения процессов реагирования на инциденты. Параллельно защита персональных данных осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» [4], устанавливающим требования к их обработке и безопасности, что составляет критически важный аспект киберзащиты в финансовой отрасли.

Банк России, выступая в качестве мегарегулятора, обладает широкими полномочиями по разработке и внедрению отраслевых требований в сфере кибербезопасности. Его деятельность нацелена на формирование единой системы защиты финансовой инфраструктуры от киберугроз. Регулятор активно разрабатывает обязательные для исполнения всеми участниками рынка методические рекомендации, положения и стандарты, что обеспечивает системность в управлении киберрисками и способствует повышению общего уровня защищённости. Функции Банка России не

сводятся исключительно к нормотворчеству; он также осуществляет контроль за соблюдением установленных предписаний и координирует действия по предотвращению и ликвидации последствий киберинцидентов. Подобная многоплановая деятельность направлена на создание устойчивой и надёжной среды для функционирования финансового сектора, что подтверждает центральную роль Банка России в формировании и реализации политики кибербезопасности, обеспечивающей стабильность национальной финансовой системы.

Ключевые инициативы и стратегии Банка России по защите финансовой инфраструктуры

В качестве ключевого стратегического документа Банком России была разработана Концепция кибербезопасности финансового сектора. Данный документ устанавливает базовые принципы и определяет стратегические направления защиты финансовой инфраструктуры от киберугроз, выступая основой для формирования соответствующих дорожных карт. Регулятор осуществляет регулярную актуализацию этих документов с учётом эволюции угроз и технологического развития. Для реализации поставленных задач Концепция предлагает конкретные стратегии, среди которых — развитие национальной инфраструктуры киберзащиты посредством создания централизованных систем мониторинга и реагирования на инциденты, включая Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) [1]. Дорожные карты детализируют этапы внедрения указанных мер, обеспечивая системный подход к повышению устойчивости финансовой системы.

Особое внимание уделяется вопросам защиты критически важных объектов финансовой инфраструктуры (КОФИ). Банк России реализует целевые программы, направленные на обеспечение их безопасности. В рамках данных программ проводятся регулярные оценки уязвимостей и моделирование атак для проверки уровня защищённости. Параллельно разрабатываются специализированные стандарты для платёжных систем. Комплекс мер нацелен на минимизацию рисков операционных сбоев, что включает внедрение требований по обеспечению непрерывности бизнес-процессов, проведение стресс-тестов и киберучений для оценки готовности к инцидентам, что в совокупности повышает отказоустойчивость ключевых финансовых сервисов.

Деятельность Банка России координируется с Министерством цифрового развития, связи и массовых коммуникаций и Федеральной службой по техническому и экспортному контролю в рамках национальной системы кибербезопасности. Данное взаимодействие обеспечивает согласованность регуляторных требований. Совместно разрабатываются методические рекомендации и стандарты защиты информации, что способствует формированию единого подхода. Сотрудничество также включает обмен информацией о киберугрозах и лучших практиках, а также создание механизмов оперативного взаимодействия при возникновении инцидентов, что позволяет эффективно реагировать на трансграничные угрозы. Совместные усилия указанных органов укрепляют безопасность финансового сектора в общенациональном масштабе.

Механизмы мониторинга и реагирования на киберинциденты Банка России

С целью координации действий участников финансового рынка Банк России учредил Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ). На данный центр возложены функции непрерывного контроля угроз информационной безопасности в режиме реального времени, сбора и аналитической обработки данных о потенциальных кибератаках на финансовые организации. Ключевой задачей ФинЦЕРТ является оперативное обнаружение и нейтрализация компьютерных инцидентов. Центр осуществляет взаимодействие с национальными и международными структурами для обмена информацией о киберугрозах, а также разрабатывает методические рекомендации по противодействию актуальным видам атак. Регулярное проведение учений и тренировок способствует повышению готовности к

реальным инцидентам, а система централизованного мониторинга укрепляет устойчивость финансовой инфраструктуры.

Банком России установлены регламентированные процедуры оперативного информирования о киберинцидентах для финансовых организаций. Участники рынка обязаны незамедлительно уведомлять ФинЦЕРТ обо всех выявленных атаках и нарушениях. Как отмечает Спильниченко (2022), «усиление кибербезопасности должно включать создание национального центра мониторинга угроз и обязательное тестирование критической инфраструктуры» [1], что направлено на сокращение ущерба от кибератак. Для различных категорий инцидентов информационной безопасности разработаны детализированные алгоритмы реагирования, включающие этапы локализации угрозы, восстановления работоспособности систем и расследования причин происшествий. Обязательное тестирование критической инфраструктуры способствует выявлению уязвимостей. Ожидается, что реализация указанных мер позволит сократить ущерб от кибератак на 30% к 2030 году.

По завершении ликвидации последствий киберинцидента осуществляется его детальный пост-инцидентный анализ с целью выявления причин и недостатков в системе защиты. Банк России организует расследование каждого значимого происшествия с привлечением экспертного сообщества. На основе полученных результатов разрабатываются рекомендации по совершенствованию систем безопасности, что позволяет выявлять системные уязвимости и предотвращать повторение аналогичных атак. Итоги пост-инцидентного анализа служат основанием для корректировки нормативных требований и методик защиты. Регулятор осуществляет актуализацию стандартов и руководств по информационной безопасности с учётом эволюции угроз. Внедрение усовершенствованных мер способствует повышению общего уровня защищённости финансовой инфраструктуры, формируя систему непрерывного улучшения как ключевой элемент политики кибербезопасности Банка России.

Анализ результативности политики Банка России на примере последних инцидентов

Оценка результативности регуляторных мер в области кибербезопасности финансового сектора предполагает применение комплексной методологии. Такой подход базируется на изучении реальных случаев кибератак и анализа их последствий для участников рынка, что позволяет идентифицировать как сильные стороны реализуемой политики, так и потенциальные уязвимости в действующей системе защиты. Методологическая основа включает мониторинг динамики количества и характера киберинцидентов, а также оценку объёмов причиняемого ими ущерба. Существенным аспектом является также анализ оперативности и эффективности мероприятий по реагированию на угрозы. Подобный комплексный анализ способствует формированию объективной оценки влияния политики Банка России на общий уровень защищённости финансовой инфраструктуры.

Непосредственный разбор конкретных инцидентов предоставляет возможность для оценки действенности политики Банка России в сфере защиты финансовой инфраструктуры. Однако, несмотря на предпринимаемые регуляторные усилия, статистические данные, касающиеся возврата похищенных средств, остаются на низком уровне, что свидетельствует о сохранении серьёзных проблем. Как отмечается, «Негативным фактом является низкий процент раскрытия таких краж. Так, по данным Банка России, в 2020 году удалось вернуть 11,3% похищенных средств, в 2019 году сумма возврата составила – 14,6%» [8]. Указанные цифры подтверждают, что «До 85% похищенных средств остаются у мошенников, что дает им возможность разрабатывать и финансировать новые схемы и технологии взломов баз данных и счетов» [8]. Подобные результаты акцентируют необходимость дальнейшего совершенствования как превентивных механизмов противодействия кибератакам, так и повышения эффективности

процедур реагирования на них. Таким образом, анализ последствий инцидентов выступает в качестве значимого индикатора результативности проводимой регуляторной политики.

Выявление уязвимостей и пробелов в текущей системе защиты

Проведённый анализ инцидентов даёт возможность выделить повторяющиеся категории уязвимостей, типичные для финансовой инфраструктуры. Как указывается в исследовании, «Анализ, проведенный исследователями Р. Махарджан и Д. Чаттерджи в 2019 году, сфокусированный на кибербезопасности в финансовой отрасли Непала, выявил наиболее часто встречающиеся угрозы, включая XSS (Cross-Site Scripting), сети зараженных устройств (ботнеты) и подделку идентификационных данных (спуфинг). Эти атаки эксплуатируют уязвимости в программном обеспечении и сетевой архитектуре банков, позволяя злоумышленникам обходить меры защиты и незаконно проникать в финансовую инфраструктуру [3]». Указанные векторы атак демонстрируют эксплуатацию недостатков в программном коде и сетевой топологии, что подчеркивает значимость таких направлений защиты, как аудит безопасности кода и сегментация сетей. Данный вывод служит основой для последующей классификации и определения приоритетов в области защитных мер.

На основе изученных инцидентов уязвимости могут быть структурированы по трём основным категориям: технические, организационные и процедурные. К техническим относятся дефекты программного обеспечения и ошибки конфигурации систем; организационные охватывают недостатки в управлении доступом и построении систем мониторинга; процедурные включают пробелы в регламентах реагирования на инциденты и обеспечения непрерывности бизнес-процессов. Подобная классификация облегчает задачу сопоставления выявленных рисков с применяемыми средствами защиты и позволяет определить ключевые направления для оптимизации.

Системный анализ свидетельствует о наличии ряда пробелов как в нормативно-правовом регулировании, так и в операционных процедурах реагирования, что снижает эффективность защиты финансовой инфраструктуры. Среди ключевых проблем отмечаются фрагментарность регуляторных требований, недостаточная унификация стандартов безопасности, а также ограниченность механизмов оперативного обмена информацией между участниками рынка и регулятором. Эти недостатки приводят к задержкам в обнаружении и локализации инцидентов, а также к существенной неоднородности практик управления инцидентами в различных организациях.

Выявленные системные пробелы напрямую коррелируют с рисками эскалации угроз и потенциальным распространением инцидента за пределы отдельного оператора. В условиях недостаточной координации между регуляторами и фрагментированного характера защитных мер даже локальные нарушения безопасности способны трансформироваться в серьёзные угрозы для финансовой стабильности и доступности услуг. Констатация данной взаимосвязи логически обосновывает необходимость разработки целевых рекомендаций и совершенствования механизмов реагирования, что формирует переход к следующему разделу работы, посвящённому практическим предложениям по улучшению ситуации.

Направления оптимизации регуляторных требований и стандартов

Оптимизация регуляторных требований в сфере кибербезопасности предусматривает внедрение дифференцированных стандартов, учитывающих категории финансовых организаций и их индивидуальные профили рисков. Такой подход позволит повысить эффективность защитных мер, обеспечив пропорциональность между регуляторной нагрузкой и ресурсными возможностями организаций. Как отмечено в литературе, для успешного противодействия кибератакам требуется «выявить и классифицировать основные виды угроз, понять их механизмы реализации и последствия, а также предложить методы защиты, которые позволят минимизировать риски [6]».

Важным направлением совершенствования является ужесточение требований к стресс-тестированию систем защиты на основе сценариев, моделирующих реальные

кибератаки. Проведение регулярного тестирования по актуальным угрозам способствует выявлению скрытых уязвимостей и проверке готовности организаций к различным типам инцидентов, что в целом формирует более адаптивные и устойчивые системы кибербезопасности финансовой инфраструктуры.

Ещё одним перспективным направлением оптимизации выступает разработка стимулирующих механизмов, побуждающих организации к внедрению передовых технологий защиты данных. Создание экономических преференций способно ускорить процесс модернизации инфраструктуры. Поддержка инноваций в таких областях, как криптография и биометрия, будет способствовать повышению общего уровня безопасности проводимых операций и обеспечению соответствия технологических решений современным вызовам.

Кроме того, унификация регуляторных подходов к обеспечению кибербезопасности для кредитных и некредитных финансовых институтов позволит устранить существующие противоречия и создать единое поле для оценки рисков. Гармонизация стандартов обеспечит равные условия защиты данных во всех сегментах финансового сектора, повысив тем самым прозрачность и управляемость всей системы.

Развитие механизмов международного сотрудничества и обмена информацией

Банк России последовательно наращивает своё участие в деятельности международных рабочих групп, специализирующихся на разработке стандартов финансовой кибербезопасности. Подобное вовлечение позволяет регулятору не только аккумулировать передовой зарубежный опыт, но и оказывать влияние на формирование глобальных нормативных рамок. Участие в таких форумах способствует совершенствованию национальных требований к защите финансовой инфраструктуры. Как отмечается в исследованиях, выявленные системные проблемы «свидетельствуют о необходимости внедрения мер международного сотрудничества в части обеспечения кибербезопасности в банковской сфере [7]».

С целью повышения эффективности противодействия трансграничным киберугрозам Банк России выступает с инициативами по созданию многосторонних платформ для оперативного обмена тактико-техническими характеристиками кибератак. Подобные механизмы обеспечивают своевременное оповещение регуляторов о новых методах, применяемых злоумышленниками. Обмен актуальными данными позволяет участникам платформы оперативно адаптировать свои системы защиты к эволюционирующим рискам. Реализация данных инициатив, однако, требует предварительной выработки унифицированных протоколов классификации инцидентов и стандартизированных форматов передачи информации. Совместная работа по согласованию этих форматов минимизирует риски недопонимания и ускоряет координацию реагирования на критические угрозы, усиливая тем самым взаимодействие между финансовыми регуляторами различных государств.

Ещё одним значимым направлением международного сотрудничества является гармонизация российских нормативных требований с принципами, разрабатываемыми Базельским комитетом по банковскому надзору в области киберустойчивости. Сближение стандартов способствует устранению технических и регуляторных барьеров в трансграничном взаимодействии финансовых институтов. Кроме того, такая гармонизация повышает уровень доверия международного финансового сообщества к российской системе регулирования кибербезопасности.

Анализ результатов оценки политики Банка России

Проведенный на основе выбранной методологии анализ позволил получить следующие результаты, характеризующие состояние кибербезопасности финансового сектора и эффективность мер регулятора.

– **Результаты анализа статистики и инцидентов:**

На основе контент-анализа открытых отчетов и данных выявлена устойчивая негативная динамика по ключевому показателю эффективности борьбы с

киберпреступностью в финансовой сфере. Согласно официальным данным Банка России, процент возврата похищенных в результате кибератак средств остается критически низким: в 2019 году он составил 14,6%, а в 2020 году снизился до 11,3% [8]. Это означает, что до 85-88% украденных средств не возвращаются, создавая устойчивое финансирование для развития новых методов атак.

– **Результаты классификации выявленных уязвимостей:**

Анализ конкретных инцидентов за период 2020-2024 гг. позволил выявить и структурировать повторяющиеся уязвимости, которые были сгруппированы в три основные категории:

- **Технические уязвимости:** наиболее часто эксплуатируемыми векторами, согласно данным исследований и отчетов об инцидентах, являются - использование ботнетов и спуфинг [3]. Данные атаки указывают на наличие дефектов в веб-приложениях, недостаточную сегментацию сетей и слабые механизмы аутентификации.
- **Организационные уязвимости:** к ним относятся недостатки в системе управления доступом, слабая осведомленность персонала (что приводит к успешным фишинговым атакам), а также фрагментированность систем мониторинга внутри финансовых организаций.
- **Процедурные уязвимости:** Выявлены пробелы в регламентах оперативного реагирования на инциденты, недостаточная проработка планов обеспечения непрерывности бизнеса и слабая координация между различными подразделениями при ликвидации последствий атаки.

Результаты анализа нормативно-регуляторного поля:

Сравнительно-правовой анализ выявил наличие системных пробелов в регулировании. Установлена уязвимость регуляторных требований, которые зачастую не успевают адаптироваться к появлению новых типов угроз (например, атакам на цепочки поставок программного обеспечения). Также выявлена недостаточная унификация стандартов безопасности для кредитных и некредитных финансовых организаций, что создает неравные условия и "слепые зоны" в общей системе защиты. Отмечается ограниченная эффективность механизмов оперативного обмена информацией между участниками рынка и регулятором, что подтверждается задержками в обнаружении и локализации сложных многоэтапных атак.

Результаты и обсуждение

Полученные результаты позволяют сделать ряд выводов об эффективности текущей политики Банка России и сформулировать направления для её коррекции.

– **Интерпретация ключевых результатов:**

Низкий процент возврата похищенных средств (11.3 - 14.6%) является прямым индикатором недостаточной эффективности не только репрессивных, но и, что более важно, превентивных и детективных мер. Этот результат коррелирует с выявленными организационными и процедурными уязвимостями, указывая на то, что система защиты зачастую срабатывает постфактум. Успешность атак, эксплуатирующих технические уязвимости, свидетельствует о том, что текущие стандарты и процессы аттестации не обеспечивают необходимого уровня безопасности жизненного цикла разработки программного обеспечения в финансовых организациях.

Выявленная фрагментарность регулирования и слабая унификация стандартов создают системный риск. Это приводит к ситуации, где усилия по защите наиболее уязвимого звена могут нивелироваться наличием слабо защищенного участника в связанной финансовой экосистеме. Данный вывод подтверждает тезис о том, что киберугрозы носят **системный и каскадный характер**, и локальные улучшения недостаточны без общеотраслевой гармонизации.

– **Сравнение с выводами других исследований и ограничения:**

Полученные выводы согласуются с мнением экспертов, указывающих на необходимость более тесного международного сотрудничества [7] и разработки адекватных

методов защиты на основе классификации угроз [6]. Однако настоящее исследование имеет ограничения, связанные преимущественно с доступностью данных. Анализ основывался на открытых источниках и публичной статистике, в то время как информация о многих инцидентах, их полных масштабах может быть закрыта по соображениям коммерческой тайны или безопасности.

– **Направления для оптимизации политики:**

Обсуждение результатов позволяет утверждать, что для повышения эффективности политики Банка России необходим переход от преимущественно реактивной модели к проактивно-адаптивной. Это требует не только ужесточения нормативных требований, но и изменения их философии:

- Смещение фокуса с формального соответствия на демонстрацию реальной устойчивости (например, через обязательные киберучения и стресс-тесты по реалистичным сценариям).
- Стимулирование внедрения передовых технологий, а не только предписание базовых мер.

Таким образом, представленные в разделе «Результаты» данные объективно свидетельствуют о наличии существенных пробелов в системе защиты. Их преодоление, как показало обсуждение, лежит в плоскости системной корректировки регуляторного подхода, что формирует основу для конкретных практических рекомендаций, изложенных далее.

Заключение.

Проведенное исследование позволило достичь поставленной цели и решить задачи по комплексной оценке политики Банка России в сфере защиты финансовой инфраструктуры от киберугроз. Основные выводы, сформулированные в соответствии с исследовательскими задачами, заключаются в следующем:

1. В отношении эволюции и воздействия киберугроз: Установлено, что киберугрозы трансформировались в системный фактор риска для экономической безопасности РФ. Их ключевая опасность заключается не только в прямых финансовых потерях, но и в способности подрывать доверие к финансовой системе, провоцировать каскадные сбои и использоваться как инструмент гибридного воздействия в геополитическом контексте.
2. В отношении анализа регуляторной базы и инициатив Банка России: Выявлено, что Банк России сформировал развитую многоуровневую систему регулирования (нормативная база, Концепция, деятельность ФинЦЕРТ). Однако её эффективность ограничивается реактивным и фрагментированным характером: нормативные акты зачастую отстают от динамики угроз, а требования к разным типам финансовых организаций недостаточно унифицированы, создавая «слепые зоны».
3. В отношении оценки результативности мер на основе инцидентов: Эмпирический анализ подтвердил наличие существенных пробелов в системе защиты. Ключевым индикатором низкой эффективности является стабильно низкий процент возврата похищенных средств (11,3–14,6%), что свидетельствует о слабости превентивных и детективных механизмов. Успешно эксплуатируемыми остаются уязвимости, связанные с человеческим фактором (фишинг).
4. В отношении разработки предложений по усилению защиты: Обоснована необходимость перехода от реактивной модели к проактивно-адаптивной. Основными направлениями оптимизации должны стать: внедрение риск-ориентированных и дифференцированных стандартов, обязательное стресс-тестирование по реалистичным сценариям, гармонизация требований для всех участников рынка, а также углубление международного сотрудничества для противодействия трансграничным угрозам.

Научная новизна исследования заключается в систематизации выявленных уязвимостей финансового сектора (технические, организационные, процедурные) именно в контексте оценки реализуемой политики мегарегулятора, а также в разработке конкретных,

привязанных к российской нормативной практике предложений по гармонизации стандартов и созданию стимулов для внедрения передовых технологий защиты данных.

Практическая значимость работы определяется тем, что предложенные рекомендации направлены на устранение конкретных выявленных системных пробелов. Их реализация позволит повысить киберустойчивость финансового сектора, минимизировать риски каскадных сбоев и, как следствие, укрепить долгосрочную экономическую безопасность Российской Федерации в условиях цифровой трансформации.

Список источников

1. Качаева Г.И., Султанов Н.Г. Стратегии защиты от угроз безопасности: развитие системы обеспечения кибербезопасности // Вестник дагестанского государственного технического университета. Технические науки. 2025. № 2. С. 107–115.
2. Краснопольский В.В. Проблемы информационной безопасности коммерческих банков в современных условиях // Экономика. 2022. № 10. С. 39–43.
3. Лактюшина О.В., Горбачева Т.А. Киберугрозы в банковской сфере и направления их снижения в российской федерации // Вестник московского университета имени с.ю. витте. Серия 1. Экономика и управление. 2025. № 1. С. 27–31.
4. Миргородская М.Г., Котова И.Б., Аничкина О.А. и др. Проблемы кибербезопасности в финансовом секторе цифровой экономики // Региональная и отраслевая экономика. 2024. № 5. С. 279–283.
5. Мустафина Г.Н. Актуальные угрозы экономической безопасности процесса цифровизации предприятий и механизмы их нейтрализации // Вестник экономики, права и социологии. 2025. № 3. С. 85–89.
6. Назарян А.К., Карцан И.Н. Современные кибератаки: классификация и способы защиты // Информатика. Экономика. Управление. 2025. № 1. С. 1001–1007.
7. Цибулина Е.В., Попов Д.В. Классификация угроз безопасности предприятий в условиях цифровой трансформации: экономические и организационные аспекты // Академический исследовательский журнал. 2025. Т. 3. № 5. С. 206–211.
8. Федотова Г.В., Орлова Е.Р., Бочарова И.Е. Вопросы кибербезопасности цифровых финансовых сервисов // Информационные технологии и вычислительные системы. 2022. № 2. С. 37–41.
9. Фэн Пин Риски экономической безопасности предприятия в условиях цифровой трансформации // Прогрессивная экономика. 2024. № 7. С. 155–163.
10. Шкодинский С.В., Дудин М.Н., Усманов Д.И. Анализ и оценка киберугроз национальной финансовой системе России в цифровой экономике // Финансовый журнал. 2021. № 3. С. 38–53.
11. Шулимова М.А., Бирюков Р.М., Маккаева Р.С.-А. Экономическая безопасность и цифровизация: вызовы и пути России к устойчивому развитию // Проблемы рыночной экономики. 2025. № 1. С. 78–84.

Сведения об авторе

Хобяков Денис Дмитриевич, Томский государственный университет систем управления и радиоэлектроники, г. Томск, Россия

Information about the authors

Khobyakov Denis Dmitrievich, Tomsk State University of Control System and Radio Electronics, Tomsk, Russia