

УДК 33 DOI: 10.14451/1.254.230

Эрозия доверия к банковским сервисам после кибератак: механизмы, последствия и стратегии восстановления

© 2026 Селюгина Светлана Викторовна

Директор факультета экономических и прикладных наук. МБИ имени Анатолия Собчака, Санкт-Петербург, Россия.

E-mail: seluygina@ibispb.ru

Ключевые слова: информационная безопасность, банки, кибервоздействия, кибератаки, кибербезопасность, доверие клиентов, утечка данных, финансовые риски, экономическая безопасность.

В данной статье исследуется феномен эрозии доверия клиентов к корпоративным информационным системам, сервисам и услугам банков, кредитных учреждений и других финансовых организаций на фоне существенного увеличения количества, совершенствования тактики и усложнения кибератак. На основе анализа статистических данных, отраслевых отчётов и конкретных инцидентов в Российской Федерации и мире представлены основные механизмы влияния киберугроз на восприятие надёжности и финансовой устойчивости банков. В работе рассматриваются прямые (финансовые убытки) и косвенные (репутационные) последствия кибератак, анализируется поведение клиентов, включая отток вкладов и смену финансовых институтов. Особое внимание уделяется усилению роли регуляторов и трансформации стратегий информационной безопасности банков, кредитных учреждений и других финансовых организаций. В рамках данного исследования формулируются возможные комплексные меры, необходимые для восстановления и поддержания доверия клиентов в условиях цифровой экономики.

Введение

Банки, кредитные учреждения и другие финансовые организации переживают глубокую цифровую трансформацию, которая, наряду с повышением операционной эффективности и удобства для клиентов, порождает новые системные уязвимости. Финансовые организации, сосредоточивающие огромные массивы ликвидных активов и конфиденциальных персональных данных, являются одной из наиболее привлекательных целей для киберпреступников [2]. В 2024 году

финансовая отрасль занимала второе место по количеству кибератак после государственного сектора [2]. По данным Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России (далее – Фин-ЦЕРТ), в 2024 году было зафиксировано порядка 750 кибератак на финансовые организации [5].

Учащение компьютерных инцидентов, сопряжённых с утечками миллионов записей персональных данных и хищениями денежных средств,

ставит под удар один из фундаментальных столпов банковской системы – доверие клиентов. Как отмечают эксперты, информационная безопасность для банков перестала быть лишь технической задачей, превратившись в элемент бизнес-стратегии и ключевой фактор конкурентного преимущества [2]. Целью данной статьи является анализ механизмов, посредством которых кибератаки подрывают доверие к корпоративным информационным системам и сервисам банковского сектора, оценка масштабов последствий и формулирование научно обоснованных подходов к построению устойчивых клиентских отношений в условиях перманентной киберугрозы.

Ландшафт киберугроз и динамика утечек данных в банковском секторе

Киберугрозы для финансового сектора отличаются разнообразием тактики и подходов, а также постоянной эволюцией. Можно выделить несколько доминирующих векторов (направлений) атак:

1. *Социальная инженерия и фишинг.* Фишинговые атаки остаются главным инструментом начального проникновения в корпоративные информационные системы и сервисы банковского сектора. В 2023 году более 80% инцидентов начинались с фишинга [3]. В 2024 году доля атак с применением методов социальной инженерии на сотрудников и клиентов составила 35% по данным ЦБ [3]. Злоумышленники создают дипфейки, используют утекшие персональные данные для персонализации атак, что многократно повышает их эффективность [6].
2. *Целевые атаки на инфраструктуру.* В их числе – эксплуатация уязвимостей (например, во вредоносное программное обеспечение для удалённого доступа), DDoS-атаки на критически важные сервисы и сложные многоэтапные атаки (Advanced Persistent Threat, APT). В 2024 году около 60% атак были направлены на компрометацию учётных данных сотрудников [3].
3. *Атаки через цепочки поставок (Supply Chain).* Проникновение в системы банка через взлом

подрядчиков, интеграторов или облачных провайдеров [2; 5]. Инцидент 2023 года с атакой программы-вымогателя на поставщика облачных услуг в США, которая вызвала сбои в работе 60 кредитных союзов, наглядно демонстрирует системные риски этого вектора [9].

Статистика утечек данных в России отражает тревожную динамику. Хотя в 2024 году количество инцидентов в финансовом секторе сократилось на 58,8% до 25 случаев, их масштаб остаётся значительным – было скомпрометировано 68 млн записей данных [10]. При этом 88% утечек стали результатом кибератак, что на 7 процентных пунктов выше показателя предыдущего года [10].

Механизмы эрозии доверия клиентов

Доверие к банку строится и формируется на основе двух ключевых убеждений: в его способности гарантировать конфиденциальность персональных и финансовых данных, а также в обеспечении бесперебойного доступа к собственным денежным средствам. Кибератаки системно разрушают оба этих убеждения.

Чувство уязвимости возникает у клиента, когда он становится прямой жертвой мошенничества в результате утечки его данных из банка, происходит прямое нарушение психологического контракта. Однако даже если прямых финансовых потерь нет, осознание того, что конфиденциальная информация (паспортные данные, телефоны, финансовые истории и пр.) оказалась в открытом доступе, порождает глубокое чувство уязвимости и предательства [2; 3]. По данным исследования InfoWatch, почти треть (29%) всех утекших в 2024 году персональных данных составляла аутентификационная информация (логины, пароли), что является прямым ключом к доступу к средствам [4].

DDoS-атаки и атаки программами-вымогателями, приводящие к отключению онлайн-банкинга, карточных сервисов или платёжных систем, наносят удар по второй составляющей доверия – ожиданию стабильности. Клиент теряет контроль над своими финансами в самый

неподходящий момент, что может иметь реальные жизненные последствия. Как отмечается в отчёте МВФ, такие сбои в предоставлении критически важных услуг могут серьёзно влиять на экономическую активность и подрывать доверие к финансовой системе в целом [9].

Непрозрачность в информировании о масштабах и причинах инцидента усугубляет репутационный кризис доверия. Недостаточная или запоздалая коммуникация со стороны банка заставляет клиентов искать информацию в медиапространстве, где доминируют негативные нарративы и слухи. Как следствие, локальный компьютерный инцидент перерастает в полномасштабный репутационный кризис, последствия которого (отток клиентов, падение стоимости бренда) многократно превышают прямые убытки от атаки [3]. Исследование МВФ подтверждает, что даже небольшие банки в США сталкивались с умеренным, но устойчивым оттоком депозитов после киберинцидентов [9].

Последствия для банков и финансовой системы

Эрозия доверия имеет измеримые макро- и микроэкономические последствия:

1. *Прямые финансовые потери.* Включают средства, похищенные в результате атаки, затраты на восстановление инфраструктуры, штрафы регуляторов и судебные издержки. По данным Центробанка РФ, ущерб от атак на финансовый сектор в 2024 году превысил 6 млрд рублей [3]. Пример AT&T, согласившейся выплатить 177 млн долл. США для урегулирования коллективных исков, демонстрирует масштаб долгосрочных юридических и компенсационных издержек [1].
2. *Отток клиентов и рост стоимости привлечения.* Потеря доверия ведёт к переходу клиентов к конкурентам, воспринимаемым как более надёжные. После утечки данных 1,5 млн клиентов один из российских банков потерял 10% депозитной базы [3]. Привлечение новых клиентов в таких условиях требует значительно больших маркетинговых затрат.
3. *Усиление регуляторного давления.* Реакцией

на растущие риски становится ужесточение требований регуляторов. В России с 30 мая 2025 года вступили в силу поправки, ужесточающие административную ответственность за нарушения в обработке персональных данных, включая оборотные штрафы. Банк России, ФСТЭК, ФСБ и Роскомнадзор формируют сложную систему требований к информационной безопасности, невыполнение которых грозит не только штрафами, но и ограничениями в деятельности.

4. *Угроза финансовой стабильности.* В макроэкономическом масштабе распространённые кибератаки могут создать системный риск. МВФ предупреждает, что серьёзный инцидент может подорвать доверие к финансовому учреждению, а в крайних случаях – спровоцировать обвальные распродажи активов или массовое изъятие вкладов (bank run), что дестабилизирует всю финансовую систему [9].

Направления восстановления и укрепления доверия

Преодоление кризиса доверия требует комплексных усилий на технологическом, организационном и коммуникационном уровнях. Ниже представлены возможные направления, необходимые для восстановления и поддержания доверия клиентов в условиях цифровой экономики:

1. Технологическая трансформация безопасности банковского сектора:
 - переход от защиты периметра к модели Zero Trust, где каждое обращение к ресурсам проверяется, независимо от его источника [2; 8];
 - повсеместное внедрение многофакторной аутентификации (MFA), основанной на биометрии или аппаратных ключах, для противодействия АТО-атакам (Account Takeover) [1; 2];
 - развёртывание Security Operations Center (SOC) с использованием технологий искусственного интеллекта для анализа миллионов событий и раннего выявления аномалий [2; 7];
 - планирование перехода на постквантовую криптографию, актуальность которой будет расти с развитием квантовых вычислений [2].

2. Культура безопасности внутри банка, кредитного учреждения или другой финансовой организации:

- регулярное проведение фишинг-тестов и киберучений, чтобы сделать персонал не «слабым звеном», а первым рубежом обороны [2; 6].
- внедрение систем DLP (Data Loss Prevention) и тщательный аудит доступа внешних поставщиков услуг [2].

3. Прозрачная коммуникация и клиентоцентричность:

- оперативное и открытое информирование клиентов о случившемся, масштабах и принимаемых мерах, сокрытие усугубляет репутационный ущерб;
- активная помощь клиентам в повышении их цифровой грамотности – советы по распознаванию фишинга, настройке безопасных паролей, использованию MFA;
- инвестиции в удобство безопасных сценариев, безопасность не должна достигаться ценой неудобства. Процессы верификации и подтверждения операций должны быть максимально удобными.

4. Повышение роли регуляторов и отраслевая кооперация:

- выработка единых стандартов, как отмечает МВФ, необходима разработка адекватной национальной стратегии кибербезопасности для финансового сектора [9];
- создание платформ для обмена информацией об угрозах (Threat Intelligence) между банками для коллективного повышения устойчивости [9];
- международное сотрудничество, поскольку киберпреступность носит трансграничный характер, для эффективного противодей-

ствия необходима координация на глобальном уровне [9].

Заключение

Кибератаки перестали быть просто технологической проблемой IT-департаментов банков. Они превратились в существенный стратегический финансовый риск, непосредственно влияющий на фундаментальную основу банковского бизнеса – доверие клиентов. Эрозия этого доверия происходит не только в момент прямого хищения финансов, но и через ощущение утраты конфиденциальности, нарушение стабильности банковских сервисов и неудовлетворительную коммуникацию в кризисных ситуациях.

Восстановление и поддержание доверия в цифровую эпоху требуют переосмысления подходов к экономической безопасности. Банкам необходимо инвестировать не только в передовые технологические решения (от AI в SOC до постквантовой криптографии), но и в формирование культуры безопасности внутри организации и в просвещение своих клиентов. Не менее важна прозрачность и готовность нести ответственность. Регуляторам же отводится ключевая роль в формировании сбалансированной нормативной среды, стимулирующей инвестиции в киберустойчивость и отраслевую кооперацию.

Только комплексный подход, интегрирующий технологии, процессы и человеческий фактор, позволит финансовым институтам превратить информационную безопасность из статьи расходов в реальное конкурентное преимущество и краеугольный камень долгосрочных доверительных отношений с клиентом. В условиях, когда угрозы продолжают эволюционировать, способность банка демонстрировать надёжность и прозрачность становится критически важным активом.

Библиографический список

1. Аналитический отчет по кибербезопасности и искусственному интеллекту: 20-26 июня 2025 года / Информационные технологии, кибербезопасность, искусственный интеллект. – URL:

<https://newsletter.radensa.ru/archives/9215> (дата обр. 19.01.2026).

2. Информационная безопасность банков: проблемы, угрозы и методы защиты / АБП2Б. – URL: <https://abp2b.com/tpost/spg94824n1-inf>

- ormatsionnaya-bezopasnost-bankov-prob#popup:infoblockbb (дата обр. 19.01.2026).
3. Киберугрозы в финансовом секторе: защита данных и транзакций / ИНФАРС. – URL: <https://infars.ru/blog/kiberugrozy-v-finansovom-sektore-zashchita-dannykh-i-tranzaktsiy> (дата обр. 19.01.2026).
 4. Количество слитых персональных данных в 2024 году выросло на треть / InfoWatch. – URL: <https://www.infowatch.ru/company/presscenter/news/kolichestvo-slitykh-personalnykh-dannykh-v-dve-tysyachi-dvadtsat-chetvertom-godu-vyroslo-na-tret> (дата обр. 19.01.2026).
 5. Обзор основных типов компьютерных атак в финансовой сфере в 2024 году / Банк России. – 2025. – URL: https://www.cbr.ru/collection/collection/file/55129/attack_2024.pdf (дата обр. 19.01.2026).
 6. Петрова Ю. Эксперты назвали главные киберугрозы для банков и их клиентов в 2025 году / Forbes. – URL: <https://www.forbes.ru/finansy/528907-eksperty-nazvali-glavnye-kiberugrozy-dla-bankov-i-ih-klientov-v-2025-godu> (дата обр. 19.01.2026).
 7. Создание эффективной системы мониторинга безопасности / РБК. – URL: <https://companies.rbc.ru/news/7jnWCMB0zq/sozдание-effektivnoj-sistemyi-monitoringa-bezopasnosti/?ysclid=mkleo6ltqa435764078> (дата обр. 20.01.2026).
 8. Тренды банковской информатизации / Tadviser. – URL: <https://www.tadviser.ru/index.php> (дата обр. 20.01.2026).
 9. Усиление киберугроз вызывает серьезные опасения по поводу финансовой стабильности / IMF. – URL: <https://www.imf.org/ru/blogs/manuals/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability> (дата обр. 19.01.2026).
 10. Утечки данных из банков России / Tadviser. – URL: https://www.tadviser.ru/index.php/Статья:Утечки_данных_из_банков_России (дата обр. 19.01.2026).