IQRO JURNALI , IQRO JOURNAL, ИКРО ЖУРНАЛИ
ISSN:2181-4341| wordlyknowledge.uz/index.php/iqro
Volume 24. Issue 01. Oktabr, 2026

КИБЕРУГРОЗЫ В БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ (НА ПРИМЕРЕ АКБ «БАНК РАЗВИТИЯ БИЗНЕСА» — BRB)

Ибодуллаева Наргиза Нажмиддиновна
Слушатель Академии банковского дела
и финансов Республики Узбекистан.
ibodullayevanargiza2@gmail.com
https://doi.org/10.5281/zenodo.23835687

Аннотация. Исследование рассматривает угрозы информационной безопасности и механизмы защиты персональных данных в цифровом банкинге на примере публично доступных документов АКБ «Банк развития бизнеса» (BRB). Используются опубликованные в 2025–2026 гг. материалы банка, законодательство Узбекистана, международная статистика обращений о киберпреступлениях и рецензируемые исследования. Предложена воспроизводимая модель приоритизации рисков без приписывания банку неподтвержденных инцидентов.
Ключевые слова: киберугрозы, банковская деятельность, персональные данные, BRB, фишинг, риск, цифровой банкинг, ISO/IEC 27001.

Abstract. This study examines information security threats and personal data protection mechanisms in digital banking, using publicly available documents of JSCB “Business Development Bank” (BRB) as a case study. The research draws on bank materials published in 2025–2026, the legislation of the Republic of Uzbekistan, international statistics on reported cybercrime incidents, and peer-reviewed scientific studies. A reproducible risk prioritization model is proposed without attributing any unverified cybersecurity incidents to the bank.
Keywords: cyber threats, banking activities, personal data protection, BRB, phishing, risk assessment, digital banking, ISO/IEC 27001.

Введение

Цифровая трансформация банков повышает скорость и доступность платежных и кредитных услуг, одновременно увеличивая число точек доступа к персональным данным. Клиент взаимодействует с банком через мобильное приложение, веб-ресурсы, контакт-центр и внешние платежные сервисы. Уязвимость любого звена способна повлечь нарушение конфиденциальности, целостности либо доступности информации. В этой связи безопасность данных следует рассматривать как сквозной процесс управления рисками, а не как отдельную техническую функцию.

Объект исследования — публично наблюдаемая цифровая экосистема АКБ «Банк развития бизнеса»; предмет — потенциальные сценарии киберугроз и средства обеспечения конфиденциальности персональных данных. Цель состоит в разработке доказательной системы приоритетов защиты, применимой к банку с учетом доступных источников. Важное ограничение: исследование не располагает внутренними журналами событий,

результатами тестов на проникновение, числом клиентов, сведениями о подтвержденных утечках или статистикой мошенничества BRB. Поэтому приводимые оценки сценариев не являются измерением фактической защищенности банка. АКБ «Банк развития бизнеса» был преобразован из АКБ «Кишлок курилиш банк» в 2023 году; его публичный сайт содержит предложения дистанционных услуг и мобильного приложения. На сайте банка размещены правила обработки информации, а также публичные документы о проектах модернизации ИТ-инфраструктуры. Эти сведения подтверждают существование цифровых каналов и управленческих инициатив, но не позволяют установить результаты внедрения конкретных мер защиты.

Техническое задание BRB 2026 года предусматривает классификацию информации и меры предотвращения утечек (DLP), включая уровни публичных, внутренних, конфиденциальных и строго конфиденциальных данных. Это документально подтвержденное проектное требование, а не независимая проверка фактического покрытия DLP. Для научной добросовестности в настоящей работе четко разграничены публично подтвержденные факты, международные отраслевые индикаторы и авторские нормативные сценарии.

Материалы, методы и ограничения

Использован документальный анализ первичных источников: официальный сайт BRB, технические задания банка 2025–2026 годов, Закон Республики Узбекистан «О персональных данных» № ЗРУ-547, а также годовые отчеты американского Internet Crime Complaint Center (IC3) за 2024 и 2025 годы. Научный контекст сформирован по исследованиям банковских киберрисков, многоуровневой защиты и цифрового доверия (Darem et al., 2023; Shehab et al., 2024; Waliullah et al., 2025).

Для международного сравнения применены показатели IC3: в 2024 году зарегистрировано 859 532 обращения и заявленные потери свыше 16 млрд долл. США; в 2025 году — 1 008 597 обращений и почти 21 млрд долл. США. Относительное изменение числа обращений равно (1 008 597 / 859 532 − 1) × 100 = 17,34%. Показатель относится к сообщениям, полученным американским IC3, и не характеризует частоту инцидентов в BRB или банковском секторе Узбекистана.

Для сравнительного анализа использована авторская полуколичественная матрица: вероятность P и воздействие I оцениваются экспертно по шкале от 1 до 5; интегральный балл $R = P \times I$. В таблице представлены именно демонстрационные оценки, а не результаты опроса сотрудников или внутреннего аудита. После внедрения мер рассчитывается условный остаточный риск $Rr = Pr \times Ir$. Изменение $\Delta R = (R - Rr)/R \times 100\%$ характеризует сценарное снижение балла при выполнении предпосылок, но не доказанное снижение фактических потерь.

Метод имеет ограничения: шкала порядковая, произведение оценок не является денежной величиной и не заменяет количественную модель вероятности потерь. Значения нельзя использовать для утверждений о реальном уровне защиты BRB. Для эмпирической валидации необходимы обезличенные журналы SOC, результаты независимого аудита, инцидентная отчетность, параметры доступности систем и статистика обращений клиентов.

Аналитическая оценка и результаты

Согласно исследованиям, ключевые категории угроз для финансовых организаций включают социальную инженерию, вредоносное ПО, атаки на веб- и мобильные интерфейсы, компрометацию учетных записей, внутренние нарушения и риски сторонних поставщиков. В обзоре Shehab et al. (2024) подчеркивается значение сочетания технологических и организационных мер; систематический обзор Waliullah et al. (2025) связывает доверие к цифровому банкингу с многоуровневой защитой и надежностью аутентификации. Эти выводы служат основанием для выбора сценариев, но не доказывают их реализацию в BRB.

Особое значение в системе обеспечения кибербезопасности банков приобретает комплексная защита персональных данных клиентов на всех этапах их обработки: от сбора и хранения до передачи и удаления. Применительно к АКБ «Банк развития бизнеса» (BRB) перспективным направлением является совершенствование риск-ориентированного подхода, предусматривающего многофакторную аутентификацию, разграничение прав доступа сотрудников, шифрование конфиденциальной информации, непрерывный мониторинг подозрительных операций и регулярную проверку защищенности информационных систем. Дополнительное внимание необходимо уделять повышению цифровой грамотности клиентов и подготовке персонала к выявлению фишинговых сообщений и попыток социальной инженерии. При этом перечисленные меры рассматриваются как рекомендации по снижению потенциальных рисков, а не как подтверждение наличия конкретных уязвимостей или фактов нарушения информационной безопасности в BRB. Такой подход позволяет объединить технологические, организационные и правовые инструменты защиты данных, обеспечивая более устойчивое функционирование цифровых банковских сервисов.

Таблица 1

Сценарная матрица киберрисков для цифрового банка: экспертные условные баллы (не фактическая статистика BRB).

Сценарий	P	I	R	Pr	Ir	Rr / ΔR	Меры контроля
Фишинг / подмена бренда	5	4	20	3	3	9 / 55%	MFA, антифишинг, информирование
Захват учетной записи	4	5	20	2	4	8 / 60%	MFA, поведенческий мониторинг
Утечка через API / интеграции	4	5	20	2	4	8 / 60%	API-gateway, тесты, минимизация
Вымогательское ПО	4	5	20	2	4	8 / 60%	EDR, сегментация, офлайн-копии
Ошибки доступа сотрудников	4	4	16	2	3	6 / 62%	PAM, RBAC, DLP, аудит
Сбой внешнего поставщика	3	5	15	2	4	8 / 47%	Due diligence, резервирование

Сценарий	P	I	R	Pr	Ir	Rr / ΔR	Меры контроля
DDoS / недоступность сервиса	4	3	12	2	2	4 / 67%	Защита DDoS, отказоустойчивость
Утечка из резервных копий	3	5	15	1	4	4 / 73%	Шифрование, контроль ключей

Источник: составлено автором на основе NIST CSF 2.0 (2024), Shehab et al. (2024) и Darem et al. (2023). Показатели являются экспертными оценками, а не фактическими данными АКБ «БРБ».

Примечание: P — условная вероятность; I — условное воздействие; Pr и Ir — предполагаемые оценки после применения мер; ΔR — расчетное процентное изменение. Все оценки являются авторской иллюстрацией. Источники классификации угроз: Darem et al. (2023), Shehab et al. (2024), Waliullah et al. (2025).

Из таблицы следует, что максимальный исходный балл 20 получают фишинг, захват учетных записей, компрометация API и вымогательское ПО. После моделируемых мер остаточный балл этих сценариев составляет 8–9. Условная динамика не означает, что такие показатели уже достигнуты в BRB; она показывает, как управленческая команда может ранжировать инвестиции после подтверждения исходных оценок внутренними данными.

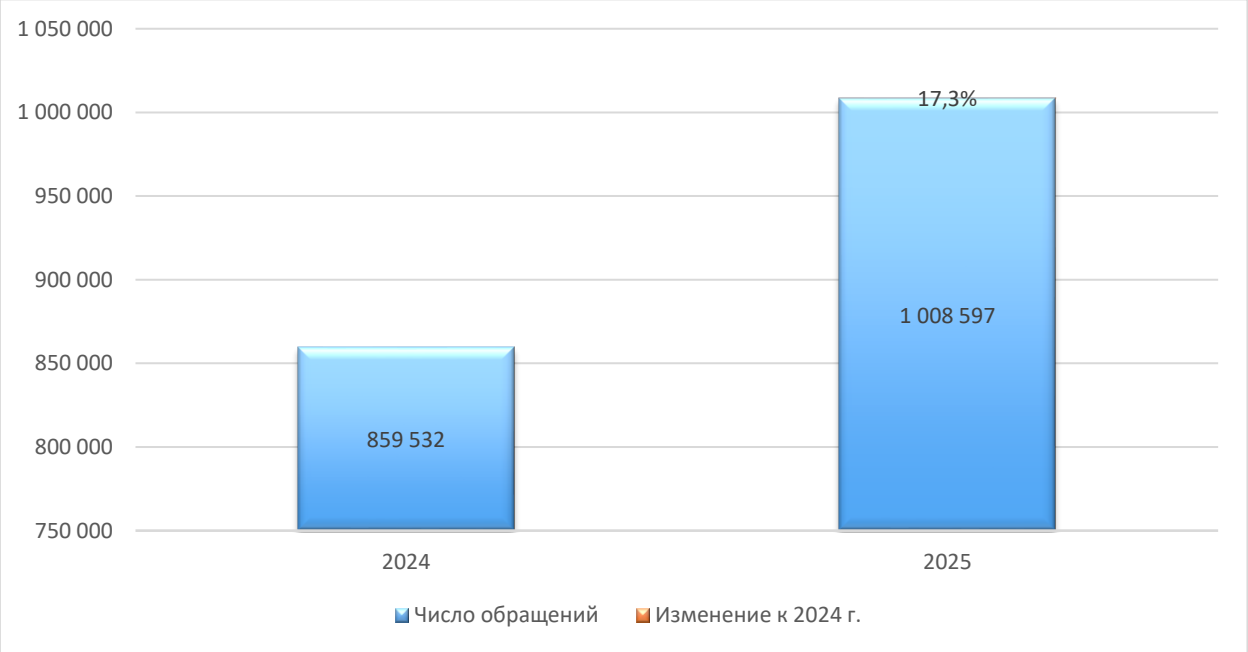


Рисунок 1. Число обращений в IC3 за 2024–2025 годы.

Источник: FBI IC3, годовые отчеты. Диаграмма характеризует США и не является статистикой атак на BRB.

Рост числа обращений IC3 на 17,34% в 2025 году иллюстрирует высокую актуальность цифрового мошенничества в международной среде. При этом рост обращений может отражать одновременно изменение распространенности преступлений, доступности каналов подачи жалоб и готовности пострадавших сообщать об инцидентах. Поэтому

прямое отождествление количества жалоб с числом успешных атак методологически некорректно.

Применительно к BRB приоритетным объектом защиты следует считать жизненный цикл персональных данных: получение сведений при идентификации клиента, их передачу по цифровым каналам, хранение, внутренний доступ, обработку подрядчиками, архивирование и удаление. Для каждого этапа необходимо определять правовое основание обработки, владельца процесса, срок хранения, минимальный состав полей и технические контрольные меры.

Закон Узбекистана «О персональных данных» № ЗРУ-547 закрепляет требования к законности обработки, конфиденциальности и защите персональных данных. Статья 27 предусматривает правовые, организационные и технические меры для защиты от неправомерной обработки, обеспечения целостности и конфиденциальности. Соблюдение закона не может быть подтверждено одним публичным документом: требуется проверка процессов, реестров обработки и фактической реализации контроля.

Для цифровых каналов банка существенны атаки на аутентификацию. Фишинговая страница или поддельное сообщение может побудить клиента раскрыть одноразовый код, а компрометация устройства — сделать недостаточной даже корректно настроенную серверную защиту. Поэтому целесообразно сочетать устойчивую многофакторную аутентификацию, подтверждение рискованных операций, анализ аномалий и ограничение числа попыток входа. Клиентские предупреждения должны содержать понятный способ проверки подлинности сообщения без перехода по присланным ссылкам.

Безопасность мобильного приложения предполагает защищенное хранение токенов, проверку целостности приложения, безопасную работу API, контроль сессий и своевременное обновление библиотек. Публичное техническое задание BRB, посвященное развитию мобильного приложения, подтверждает значение дистанционного канала для банка; однако без независимого тестирования нельзя делать вывод о наличии или отсутствии конкретных уязвимостей.

В отношении сотрудников банка важны принцип минимальных привилегий, разделение полномочий, привилегированное управление доступом и регулярная переаттестация прав. Персональные данные не должны быть доступны по умолчанию всем участникам бизнес-процесса. Особое внимание необходимо уделять выгрузкам отчетов, копиям баз данных, тестовым средам, пересылке документов и журналам технической поддержки.

Средства DLP полезны как дополнительный механизм контроля движения чувствительной информации, однако они не устраняют риски ошибочной классификации, законного массового доступа или утечки через нетипичные каналы. Для эффективности DLP требуются согласованные политики, качественная инвентаризация данных, обработка ложных срабатываний и документированные процедуры расследования.

Защита от программ-вымогателей предполагает не только антивирусные инструменты, но и изоляцию критичных сегментов, резервные копии, проверяемое восстановление, мониторинг конечных устройств и обучение персонала. Наличие резервной копии само по себе не гарантирует восстановление: необходимы тесты RTO и RPO, независимость учетных записей резервного контура и защита ключей шифрования.

Отдельную категорию составляют риски, связанные с применением искусственного интеллекта: синтетические голоса, поддельные видео, персонализированные сообщения и автоматизация социальной инженерии. Для защиты необходима верификация нестандартных распоряжений по независимому каналу, а для собственных аналитических моделей — контроль доступа к обучающим данным, оценка смещения и защита от раскрытия информации.

Научные исследования подтверждают актуальность системного подхода. Darem et al. (2023) предлагают классифицировать банковские угрозы по характеру и тяжести; Shehab et al. (2024) выделяют необходимость сочетания обмена информацией и организационных мер; Mala et al. (2025) подчеркивают роль MFA, мониторинга и обучения; Marino et al. (2025) обсуждают преимущества и ограничения машинного обучения в обнаружении угроз. Эти работы согласуются с принципом «защита на нескольких уровнях», но эффективность каждого инструмента зависит от контекста внедрения.

Для перехода от качественного обзора к измеримой системе управления рисками предлагается фиксировать пять групп показателей: охват критичных систем MFA; долю привилегированных учетных записей с регулярной переаттестацией; медианное время обнаружения и сдерживания инцидента; долю успешно протестированных восстановлений; количество подтвержденных нарушений обработки персональных данных на установленную базу операций. Показатели должны определяться единообразно по периодам, иначе сравнение может вводить в заблуждение.

Предлагаемый порядок реализации включает первичную инвентаризацию информационных активов и потоков данных, построение карты рисков, установление целевых значений, внедрение приоритетных контролей и повторное измерение результатов. Для исключения ложного эффекта необходимо учитывать изменения клиентской базы, интенсивности транзакций, полноты регистрации событий и охвата систем мониторингом.

В заключение следует отметить, что цифровизация банковской деятельности делает защиту персональных данных составной частью операционной устойчивости и доверия клиентов. Публичные материалы BRB демонстрируют внимание к вопросам информационной безопасности и проектированию соответствующих решений, однако не раскрывают достаточных данных для количественной оценки фактических инцидентов или зрелости контроля. Поэтому приоритетом остается формирование проверяемой системы измерения рисков, правомерной обработки данных, устойчивой аутентификации, мониторинга и восстановления. Представленная матрица является исследовательской моделью, подлежащей дальнейшей проверке на внутренних данных.

Список использованных источников:

1. АКБ «Банк развития бизнеса». О банке.

2. АКБ «Банк развития бизнеса». Условия и правила пользования веб-сайтом.

3. АКБ «Банк развития бизнеса». Техническое задание по подготовке СУИБ к ISO/IEC 27001:2022 (2025).

4. АКБ «Банк развития бизнеса». Приобретение услуги по модернизации ИТ-инфраструктуры (17.11.2025).

5. АКБ «Банк развития бизнеса». Техническое задание, требования к классификации данных и DLP (2026).

6. Закон Республики Узбекистан «О персональных данных» № ЗРУ-547 от 02.07.2019 (действующая редакция).

7. FBI Internet Crime Complaint Center. 2024 Internet Crime Report.

8. FBI Internet Crime Complaint Center. 2025 Internet Crime Report.

9. Darem A. A. et al. (2023). Cyber Threats Classifications and Countermeasures in Banking and Financial Sector. IEEE Access, 11, 125138–125158.