УДК 004.056

И.К. Манапбаев imanapbaev@mail.ru
М.И. Манапбаев manasbek@list.ru
Международный университет Кыргызской Республики

ОСНОВНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКОВСКОЙ СИСТЕМЫ КЫРГЫЗСКОЙ РЕСПУБЛИКИ И ПУТИ ИХ РЕШЕНИЯ

В данной статье рассмотрены проблемы информационной безопасности банковской системы Кыргызской Республики. В работе анализированы актуальные проблемы обеспечения информационной безопасности в этой сфере в условиях масштабной цифровизации финансовых услуг. Рассматриваются ключевые киберугрозы, уязвимости платежной инфраструктуры (в частности, национальной системы «Элкарт») и регуляторные вызовы. Особое внимание уделено анализу человеческого фактора и дефициту профильных IT-специалистов.

Предложен комплексный подход к модернизации систем защиты, включающий внедрение передовых технологий шифрования, развитие риск-менеджмента и совершенствование нормативно-правовой базы. На основе актуальных данных проведен анализ существующих проблем в области обеспечения информационной безопасности банковских систем страны. В результате исследований предложены некоторые рекомендации по решению этих проблем.

Также сделан вывод о том, что комплексное обеспечение информационной безопасности банковского сектора экономики Кыргызской Республики приобретает особое значение для финансовой устойчивости страны.

Ключевые слова: банковская система КР, информационная безопасность, антифрод, дистанционное обслуживание, открытые API, цифровой сом, платежная инфраструктура, киберустойчивость

Введение

Цифровизация банковской системы Кыргызской Республики в 2025–2026 гг. заметно ускорила переход клиентов и банков к дистанционным каналам обслуживания. По состоянию на 31 января 2026 года в стране действовали 23 коммерческих банка и 306 филиалов, а суммарные активы банковского сектора на конец 2025 года составляли 1 211,3 млрд сомов; депозитная база клиентов достигла 865,9 млрд сомов, кредитный портфель – 507,0 млрд сомов [1]. Одновременно происходил быстрый рост платежной инфраструктуры: по состоянию на 1 декабря 2025 года в республике было установлено 108,8 тыс. QR-кодов, а только через систему основного оператора взаимодействия в IV квартале 2025 года прошло 525,1 млн платежей на сумму 908,6 млрд сомов [2].

Эти показатели означают не только расширение финансовой доступности, но и рост цифровой поверхности атаки. Современные риски банковской системы КР уже не ограничиваются защитой локальной банковской сети и хранилищ данных. Они охватывают мобильные приложения, интернет-банкинг, API-интеграции, платформенные решения, удаленную идентификацию, обработку персональных и биометрических данных, а также устойчивость межсистемного взаимодействия банков, платежных организаций и внешних поставщиков услуг [3-5].

Цель настоящей статьи – систематизировать основные проблемы информационной безопасности банковской системы Кыргызской Республики и предложить практические пути их решения на уровне банков, антифрод-практики, регулятора, рынка и клиентской защиты.

Объект исследования: информационная безопасность банковской системы Кыргызской Республики

Методы исследования: системный анализ, статистический анализ, сравнительно-правовой подход, анализ нормативных актов и официальных материалов Национального банка Кыргызской Республики и научных статей.

Научная новизна работы заключается в рассмотрении информационной безопасности банковской системы Кыргызской Республики не только как технической составляющей информационной защиты, но и как элемента корпоративного управления, операционной устойчивости и общей стабильности финансового рынка. Предложены пути решения этих проблем на основе существующих ресурсов.

В результате исследований авторами классифицированы основные проблемы, разработаны нормативная и риск-аналитическая рамка, карта угроз информационной безопасности банковских систем и практические рекомендации по созданию модели коллективной безопасности от кибератак.

1. Основные проблемы информационной безопасности банковской системы КР

1.1. Организационные проблемы. Для многих финансовых организаций критичным остается не отсутствие отдельных технических средств защиты, а недостаточная зрелость governance. Информационная безопасность нередко рассматривается как зона ответственности только ИТ или службы безопасности, тогда как реальный риск распределен между ИТ, бизнесом, комплаенсом, операционным риском и советом директоров. Формальный характер части внутренних документов, слабая интеграция ИБ в общее управление рисками и редкое тестирование кризисных сценариев снижают качество управленческих решений.

1.2. Правовые и регуляторные проблемы. Правовая среда банковской ИБ в КР является многослойной: она включает нормы о банковской тайне, платежной системе, операционном риске, персональных данных, кибербезопасности и при необходимости требования к критической информационной инфраструктуре. На практике сложность вызывает согласование этих режимов между собой, особенно в вопросах удаленной идентификации, электронных денег, открытых API, финансовых платформ и передачи данных внешним провайдерам [4-6, 9, 11-16].

1.3. Технические проблемы. Серьезной проблемой остается неоднородность ИТ-ландшафта: устаревшие решения сосуществуют с новыми цифровыми сервисами, а уровень сегментации сетей, зрелость логирования, корреляции событий и управления уязвимостями различаются по банкам. Дополнительные риски создают недостаточная защищенность веб-интерфейсов и мобильных приложений, слабая защита API и интеграций, DDoS-атаки, вредоносное ПО и зависимость от каналов связи, процессинга, облачных и иных внешних сервисов [8].

1.4. Проблемы дистанционного банковского обслуживания. НБ КР выделяет удаленное/дистанционное обслуживание как самостоятельную зону регулирования, что подтверждает высокий риск-профиль этой сферы [4]. Для интернет-банкинга и мобильного банкинга критичны угрозы фишинга, подмены интерфейсов, SIM-swap, перехвата сессий, компрометации пользовательского устройства и злоупотребления OTP/SMS-механизмами. При этом даже качественная защита банка не компенсирует низкий уровень защищенности клиента, если не выстроены безопасные сценарии восстановления доступа и обязательное информирование пользователя [5].

1.5. Проблемы антифрод и мониторинга операций. Антифрод нельзя сводить только к классической информационной безопасности, однако эти области тесно связаны. Компрометация учетных данных, подмена устройства, социальная инженерия и мошеннические расходные операции требуют не только защиты периметра, но и постоянной оценки каждой расходной транзакции. Нормативный контур 2025–2026 гг. показывает переход к более прикладной модели регулирования: банки должны выстраивать антифрод как полноценную систему, а не как набор статических правил [6-7].

1.6. Проблемы защиты персональных данных и банковской тайны. В банковской сфере одновременно охраняются банковская тайна, персональные данные клиентов, транзакционные данные, идентификационные сведения и в ряде случаев

биометрия. Основные риски связаны с избыточным доступом сотрудников, недостаточной минимизацией данных, слабым разграничением прав, передачей сведений подрядчикам и внутренними утечками. По мере роста открытых API и финплатформ требования к защите передаваемой информации и конфиденциальности пользовательских данных становятся еще более жесткими [9, 12, 14, 19].

1.7. Кадровые проблемы и человеческий фактор. Нехватка квалифицированных ИБ-специалистов и anti-fraud аналитиков, ошибки администрирования, внутренние злоупотребления и уязвимость сотрудников к социальной инженерии остаются одной из самых устойчивых причин инцидентов. Дополнительный фактор риска – недостаточная киберграмотность части клиентов, что особенно опасно в условиях массового дистанционного обслуживания. Действующее регулирование прямо требует информирования пользователей о безопасном поведении в цифровых каналах [5].

1.8. Проблемы непрерывности деятельности и восстановления после инцидентов. Для банков и платежной инфраструктуры критично не только предотвращение инцидента, но и способность продолжать операции и быстро восстанавливаться после сбоя. Уязвимость резервных площадок, неполноценные BCP/DRP, недостаточное резервное копирование, зависимость от дата-центров, связи, процессинга и подрядчиков повышают вероятность системных последствий. В требованиях к операторам платежных систем особое место занимают резервирование, журналирование, восстановление и бесперебойность функционирования [8].

1.9. Проблемы взаимодействия между участниками рынка. Современная платежная среда КР уже носит выраженный сетевой характер: банки, платежные организации, операторы, финплатформы и интеграторы связаны общими интерфейсами и зависимостями. Поэтому изолированный подход отдельного банка не решает системную проблему. Необходимы единые признаки high-risk операций, оперативный обмен данными о мошенничестве, стандартизированное уведомление об инцидентах и развитие модели коллективной киберустойчивости рынка.

1.10. Новые зоны риска на 2026 год. Наиболее значимыми новыми зонами риска выступают удаленная идентификация и верификация, открытый банкинг и API-экосистема, финансовые платформы/маркетплейсы, услуги, связанные с виртуальными активами, а также цифровой сом как новая форма национальной валюты [20]. НБ КР уже закрепил регулирование доступа к финансовым услугам через финплатформы на основе открытых программных интерфейсов [9], порядок предоставления услуг, связанных с виртуальными активами [10], а законодательство о Национальном банке и платежной системе вводит цифровой сом и платформу цифрового сома как новую архитектуру рисков [11, 13].

2. Нормативная и риск-аналитическая рамка

Таблица 1 – Нормативная база информационной безопасности банковской системы КР на 2026 год

Нормативный акт	Зона регулирования	Значение для банковской ИБ
Конституционный закон «О Национальном банке Кыргызской Республики»	Статус НБ КР, цифровой сом, платформа цифрового сома	Формирует институциональную основу регулирования устойчивости, защиты информации и цифровой валютной инфраструктуры
Закон «О банках и банковской деятельности»	Банковская деятельность, банковская тайна, обязанности банков	Закрепляет режим сведений, составляющих банковскую тайну, и базовые обязанности банка по защите клиентских данных
Закон «О платежной системе Кыргызской Республики»	Платежи, расчеты, переводы, участники	Определяет правовую основу цифровых платежей, межсистемного

	платежной системы	взаимодействия и требований к участникам платежной инфраструктуры
Положение о минимальных требованиях по предоставлению удаленного/дистанционного обслуживания	Интернет-/мобильный банкинг, удаленные операции, электронная подпись	Выделяет дистанционные каналы как самостоятельную зону регулирования и требует защиты каналов, учетных данных и пользовательских сценариев
Положение по управлению операционным риском в коммерческих банках	Операционный риск и антифрод	Закрепляет необходимость полноценной антифрод-системы, связанной с мониторингом инцидентов и несанкционированных операций
Положение об ИБ операторов платежных систем и платежных организаций	Уязвимости, журналирование, шифрование, защита от malware, резервирование	Используется как отраслевой ориентир для базовых контролей, особенно в части цифровых каналов, процессинга и восстановления
Положение о финплатформах/маркетплейсах с использованием открытых API	Открытый банкинг, API-экосистема, платформенные модели	Вводит требования к стандартизированным интерфейсам, защите передаваемой информации и конфиденциальности данных
Порядок предоставления услуг, связанных с виртуальными активами	Услуги ПУВА, роль банков, надзор	Определяет новый контур рисков, где сочетаются финансовые, технологические и комплаенс-требования
Закон «Об информации персонального характера»	Персональные данные, обработка, хранение, передача	Требует законной обработки данных, минимизации доступа и защиты персональной информации клиентов
Закон «О кибербезопасности Кыргызской Республики» и акты по КИИ	Национальная система кибербезопасности, критическая инфраструктура, аудит	Создает общую рамку киберустойчивости, важную для системно значимых участников финансового рынка

*Составлена авторами по официальным актам НБ КР и ЦБД Минюста КР***.**

Таблица 2 – Основные угрозы и уязвимости по каналам обслуживания

Канал/контур	Основные угрозы	Типовые уязвимости	Приоритетные меры
Интернет-банкинг	Фишинг, credential stuffing, session hijacking	Слабая MFA, уязвимые веб-сессии, небезопасное восстановление доступа	MFA, device binding, anomaly detection, hardening web-flow
Мобильный банкинг	SIM-swap, overlay-атаки, malware, захват устройства	Недостаточная mobile app security, слабый контроль устройства	RASP/App Shielding, device intelligence, step-up authentication
QR/P2P/карточные операции	Несанкционированные расходные транзакции, mule-схемы, social engineering	Слабый риск-скоринг, rule-only antifraud	Оценка каждой расходной операции, поведенческие модели, blacklists
Удаленное открытие счета/идентификация	Подмена личности, synthetic identity, deepfake-попытки	Недостаточная верификация, слабая проверка liveness и устройств	Многофакторная верификация, cross-check данных, manual review high-risk cases

API/open banking/финплатформы	Компрометация токенов, abuse интеграций, утечки данных	Слабый API gateway, плохая сегментация, избыточные права	API security, rate limit, mTLS, secrets management, zero trust
Внутренние системы банка	Insider misuse, lateral movement, ransomware	Слабая сегментация, patch gaps, избыток привилегий	PAM, EDR/XDR, сегментация, patch/vulnerability management
Подрядчики, связь, процессинг, дата-центры	Отказ сервиса, supply-chain, компрометация третьих лиц	Неполные SLA/BCP, непрозрачные зависимости	Third-party risk management, резервирование, cyber-drill, contractual controls

Составлена авторами по положениям НБ КР о дистанционном обслуживании, операционном риске и ИБ платежной инфраструктуры.

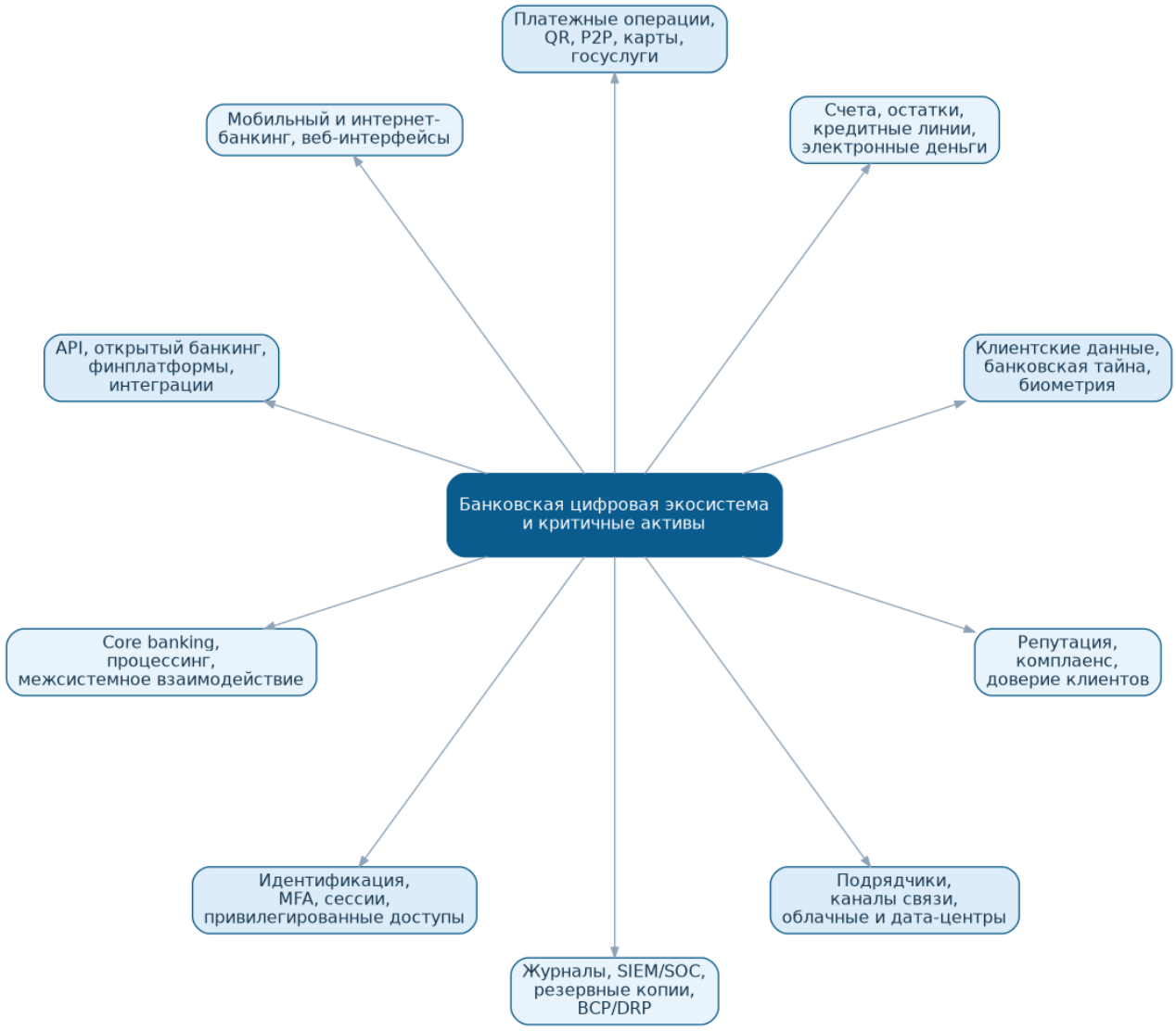

Рисунок 1 – Объекты защиты банковской цифровой экосистемы

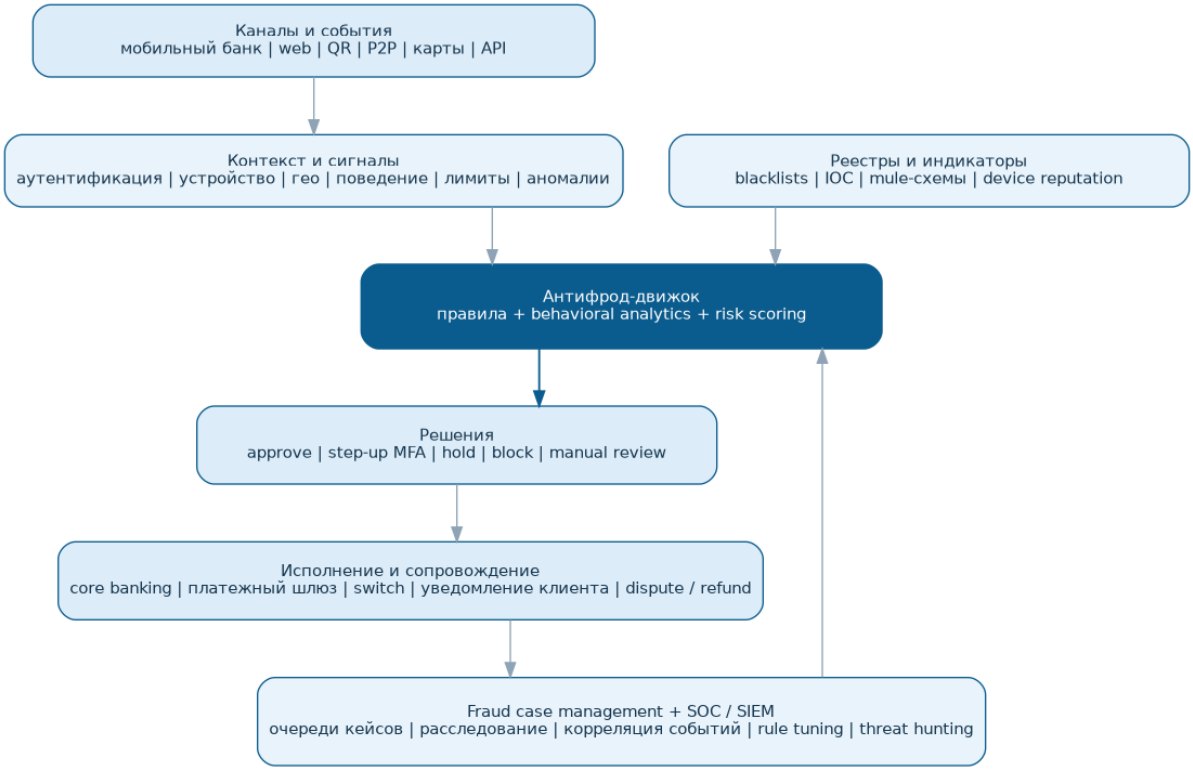

Рисунок 2 – Место антифрод-системы в архитектуре банка

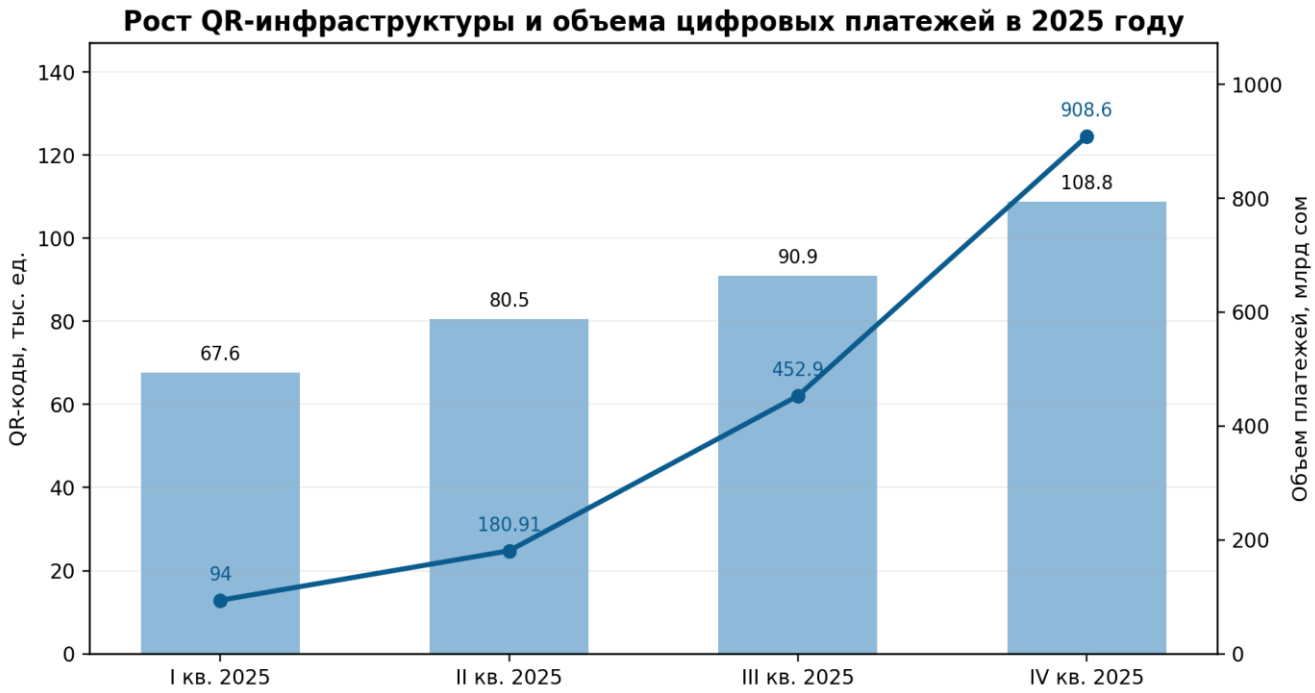

Рисунок 3 – Рост QR-инфраструктуры и объема цифровых платежей в 2025 году (по данным НБ КР за I–IV кварталы 2025 года [2-3, 17-18]).

Таблица 3 – Проблемы ИБ: организационные, правовые, технические, кадровые

Категория	Ключевые проявления	Управленческий вывод
Организационные	Формальный характер части политик, слабая роль совета директоров, фрагментация ответственности, редкое тестирование кризисных сценариев	ИБ должна стать частью enterprise risk management и повестки board-level oversight

Правовые	Пересечение банковской тайны, персональных данных, платежного регулирования, кибербезопасности, требований к API и платформам	Нужна единая интерпретация требований и harmonized compliance-by-design
Технические	Неоднородный ИТ-ландшафт, слабая сегментация, дефицит SIEM/SOC-практик, patch gaps, уязвимости мобильных и API-каналов	Приоритет – baseline controls, централизованный мониторинг и зрелое vulnerability management.
Кадровые	Дефицит ИБ- и anti-fraud специалистов, ошибки администрирования, социальная инженерия, низкая киберграмотность части клиентов	Нужны постоянное обучение, drills, phishing simulation и клиентские кампании киберграмотности

.

Таблица 4 – Проблема → причина → последствия → решение

Проблема	**Причина**	**Последствия**	**Решение**
Фрагментированное governance	ИБ не встроена в общий риск-менеджмент	Медленные решения, пробелы ответственности	Комитет по рискам, board reporting, risk-based governance
Слабая защита ДБО	Зависимость от OTP/SMS и поведения клиента	Несанкционированные операции, потери доверия	MFA, adaptive auth, device binding, secure recovery
Rule-only antifraud	Недостаток аналитики и поведенческих моделей	Высокий fraud loss или рост false positives	Behavioral analytics, per-transaction scoring, case management
Недостаточная защита данных	Избыточные доступы и передача третьим лицам	Утечки, регуляторные и репутационные риски	Data minimization, DLP, zero trust access, vendor controls
Кадровый дефицит	Нехватка экспертов и слабые тренировки	Ошибки конфигурации, успех социнженерии	Training pipeline, drills, phishing simulation
Слабый BCP/DRP	Недооценка зависимости от подрядчиков и связи	Простои, системные сбои, ущерб клиентам	Резервирование, recovery testing, supplier continuity plans
Слабая рыночная координация	Нет единого обмена индикаторами и кейсами	Повторяющиеся мошеннические паттерны по рынку	Sector sharing, high-risk indicators, cyber-drills, rapid notification

Таблица 5 – Международная практика vs вызовы банковской системы КР

Международная практика	**Ключевой вызов для КР**	**Приоритет внедрения**
Board-level cyber governance и risk ownership	ИБ часто воспринимается как функция ИТ, а не как часть корпоративного риска	Высокий
Risk-based MFA / adaptive authentication	Рост удаленных сервисов, фишинга и SIM-swap в ДБО	Высокий
Behavioral fraud analytics и per-transaction scoring	Ограниченность rule-based антифрода	Высокий
Zero trust и API security by design	Расширение open banking, API-экосистемы и финплатформ	Высокий

Sector-wide information sharing / FS-ISAC-like модели	Недостаточный межбанковский обмен индикаторами компрометации и fraud-паттернами	Средне-высокий
Operational resilience, cyber-drill, stress-test, recovery testing	Зависимость от процессинга, связи, дата-центров и подрядчиков	Высокий

Составлена авторами на основе международных подходов NIST/ISO/operational resilience и анализа вызовов рынка КР.

3. Практические рекомендации по укреплению информационной безопасности

На уровне банков. Необходимо усилить роль совета директоров и комитета по рискам, перевести ИБ в формат risk-based governance, централизовать мониторинг через SOC/SIEM, развивать threat hunting, red team, phishing simulation, зрелое управление уязвимостями, BCP/DRP, а также повсеместно применять MFA, adaptive authentication и усиленную защиту мобильных приложений.

На уровне антифрод-практики. Ключевой задачей должно стать развитие поведенческих моделей, оценка каждой расходной транзакции, единые признаки high-risk операций, централизованный fraud case management, использование внутренних и межбанковских blacklists/индикаторов компрометации, а также контроль ложноположительных срабатываний и клиентского опыта.

На уровне регулятора и рынка. Целесообразно развивать единые методические рекомендации, отраслевой обмен данными о киберинцидентах и мошенничестве, cyber-drill и stress-test для участников рынка, baseline controls для дистанционных сервисов и более строгие требования к подрядчикам, API-провайдерам и процессинговым центрам.

На уровне клиентской защиты. Постоянные кампании киберграмотности, единые предупреждения в интерфейсах приложений, безопасные сценарии восстановления доступа и усиленное подтверждение высокорисковых операций должны стать обязательной частью клиентского пути.

На уровне законодательства и стратегии. Требуется более тесное согласование банковского регулирования, законодательства о персональных данных и кибербезопасности, а также дальнейшее обновление подходов к облакам, API, финплатформам, виртуальным активам и цифровому сому.

Заключение

Цифровизация банковской системы Кыргызской Республики ускорилась, а вместе с ней выросла цифровая поверхность атаки. Ключевые проблемы ИБ лежат не только в технологиях, но и в governance, антифроде, кадрах, защите данных, клиентской культуре и непрерывности сервисов.

Период 2025—2026 гг. показывает переход НБ КР к более прикладной модели регулирования, где в единую связку входят операционный риск, антифрод, дистанционные каналы, защита данных и устойчивость платежной инфраструктуры [4-10]. Поэтому дальнейшее укрепление банковской ИБ в КР требует не точечных мер, а модели коллективной киберустойчивости рынка, при которой защита строится одновременно на уровне банка, клиента, регулятора и всего цифрового финансового контура.

Литература

1. Тенденции развития банковского сектора Кыргызской Республики (по состоянию на 31 января 2026 года). Национальный банк Кыргызской Республики, 16.03.2026. https://www.nbkr.kg/index1.jsp?item=80&lang=RUS

2. Официальные материалы НБ КР с данными о QR-инфраструктуре и платежах через основного оператора взаимодействия за IV квартал 2025 года. Национальный банк Кыргызской Республики, январь 2026 г.

https://www.nbkr.kg/DOC/11052026/000000000067188.pdf

3. Официальные материалы НБ КР с данными о QR-инфраструктуре и платежах через основного оператора взаимодействия за III квартал 2025 года. Национальный банк Кыргызской Республики, октябрь 2025 г. https://www.nbkr.kg/contout.jsp?item=2145&lang=RUS&material=128586

4. Положение о минимальных требованиях по предоставлению удаленного/дистанционного обслуживания в Кыргызской Республике (в актуальной редакции по состоянию на 2026 г.). Национальный банк Кыргызской Республики.

5. Изменения в Положение о дистанционном обслуживании, включая требования по информированию пользователей и применению электронной подписи. Национальный банк Кыргызской Республики, редакция от 21.01.2026.

6. Положение о минимальных требованиях по управлению операционным риском в коммерческих банках Кыргызской Республики (в редакции после 26.09.2025). Национальный банк Кыргызской Республики.

7. Нормы об антифроде в системе управления операционным риском и несанкционированных операциях. Национальный банк Кыргызской Республики, 2025-2026 гг.

8. Положение о требованиях по обеспечению информационной безопасности операторов платежных систем и платежных организаций. Национальный банк Кыргызской Республики, редакция от 22.05.2024.

9. Положение о регулировании доступа к финансовым услугам через финансовые платформы (маркетплейс) с использованием открытых программных интерфейсов в Кыргызской Республике. Национальный банк Кыргызской Республики, редакция от 26.12.2025.

10. Порядок предоставления услуг, связанных с виртуальными активами. Национальный банк Кыргызской Республики, 12.02.2026.

11. Конституционный закон Кыргызской Республики «О Национальном банке Кыргызской Республики» (с учетом норм о цифровом соме). ЦБД Минюста КР.

12. Закон Кыргызской Республики «О банках и банковской деятельности». ЦБД Минюста КР.

13. Закон Кыргызской Республики «О платежной системе Кыргызской Республики». ЦБД Минюста КР.

14. Закон Кыргызской Республики «Об информации персонального характера». ЦБД Минюста КР.

15. Закон Кыргызской Республики «О кибербезопасности Кыргызской Республики». ЦБД Минюста КР.

16. Требования к созданию систем кибербезопасности объектов критической информационной инфраструктуры и порядок аудита кибербезопасности. ЦБД Минюста КР.

17. ОТЧЕТ о состоянии платежной системы Кыргызской Республики за I квартал 2025 года. Национальный банк Кыргызской Республики. https://www.nbkr.kg/DOC/26092025/000000000065685.pdf

18. ОТЧЕТ о состоянии платежной системы Кыргызской Республики за II квартал 2025 года. Национальный банк Кыргызской Республики. https://nbkr.kg/DOC/27082025/000000000065444.pdf

19. Манапбаев И.К. Усовершенствование методов ценовой и неценовой конкуренции на рынке банковских услуг / Манапбаев И.К., Суркеев Б.Т. // Вестник Международного университета Кыргызстана. — 2025. — № 2-1 (59). — С. 230—234.

20. Манапбаев И.К. Современное состояние банковской системы Кыргызской Республики в условиях цифровизации: трансформация рисков информационной безопасности / Манапбаев И.К., Манапбаев М. И. // Проблемы автоматики и управления. — 2026. — № 1 (55). — С. 113—118.