УДК 004.056

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

СОВРЕМЕННОЕ СОСТОЯНИЕ БАНКОВСКОЙ СИСТЕМЫ КЫРГЫЗСКОЙ РЕСПУБЛИКИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ: ТРАНСФОРМАЦИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В данной статье исследуется современное состояние банковской системы Кыргызской Республики в условиях ускоряющейся цифровизации в стране. В работе в основе существующих данных Национального банка Кыргызской Республики проведен анализ институциональных и финансовых параметров банковского сектора КР, развитие удаленного банковского обслуживания, рост платежей посредством мобильных приложений с помощью QR-кодов, увеличение количества платежной инфраструктуры, а также улучшение интеграционных процессов на основе API. Установлено, что цифровизация банковской деятельности всегда сопровождается не только повышением доступности и скорости финансовых операций, но и увеличением вероятности информационных рисков. Подтверждено, что широкое распространение удаленных каналов взаимодействия, рост взаимодействия посредством инфраструктурных элементов и широкое развитие открытых интерфейсов усиливают уязвимость банковской системы к различным видам мошенничества, фишинга, компрометации учетных данных и иным киберугрозам. В исследовании уделено регуляторным изменениям 2025–2026 гг., в рамках которых Национальный банк Кыргызской Республики интегрировал антифрод-подходы в систему управления операционным риском. На основе этого сделан вывод о том, что информационная безопасность в банковском секторе Кыргызской Республики приобретает статус системообразующего фактора финансовой устойчивости, корпоративного управления и защиты интересов клиентов.

Ключевые слова: банковская система Кыргызской Республики, цифровизация общества, информационная безопасность, антифрод, дистанционное банковское обслуживание, QR-платежи, API, операционные риски, платежные системы

Введение

Развитие банковской системы Кыргызской Республики в 2025–2026 гг. происходит параллельно с одновременным расширением масштабов банковской деятельности и ускоренным внедрением цифровых финансовых услуг. Интенсивность цифровизации меняет особенности банковских операций, повышает использование дистанционных каналов обслуживания и способствует популярности безналичного платежного оборота. Вместе с тем это положение объективно усиливает зависимость данного сектора от устойчивости цифровой инфраструктуры, надежности межсистемных взаимодействий и уровня защищенности от угроз клиентских и внутренних информационных систем.

В таких условиях защита информации банковских систем перестает быть исключительно технологической задачей, относящейся к сфере ИТ-подразделений. Значение информационной безопасности этого сектора существенно расширяется, так как любое событие, связанное с нарушением конфиденциальности, целостности или доступности банковских систем, способно негативно повлиять не только на отдельную кредитную организацию, но и на доверие к банковской системе вообще. Поэтому проблемы киберустойчивости [7], противодействия мошенничеству и защиты цифровых каналов обслуживания должны рассматриваться как важная часть политики обеспечения финансовой стабильности экономики страны [1].

Цель исследования состоит в выявлении взаимосвязи между цифровизацией банковского сектора Кыргызской Республики и рисками информационной безопасности банковских услуг.

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

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.

1. Современное состояние банковского сектора Кыргызской Республики

Согласно официальным данным Национального банка Кыргызской Республики, по состоянию на 31 января 2026 г. в стране существовали 23 коммерческих банка и 306 их филиалов [1]. Это подтверждает факт сформированности банковского сектора как основного институционального элемента национальной финансовой системы.

Финансовые показатели банковской системы страны на конец 2025 г. также подтверждают ее высокую системную значимость. Совокупные активы банковского сектора достигли 1 211,3 млрд сомов, объем кредитного портфеля составил 507,0 млрд сомов, обязательства — 990,7 млрд сомов, депозитная база — 865,9 млрд сомов, а чистый суммарный капитал — 215,5 млрд сомов [1]. Указанные данные отражают не только масштаб банковской системы, но и ее растущую роль в перераспределении финансовых ресурсов и обслуживании хозяйственного оборота.

Особого внимания заслуживают показатели прибыльности и капитализации банковского сектора. По данным НБ КР, доходность активов по итогам 2025 г. составила 3,5 %, доходность капитала — 23,3 %, а коэффициент достаточности суммарного капитала достиг 26,4 % при нормативном минимуме 12,0 % [1]. Следовательно, банковский сектор Кыргызской Республики характеризуется не только ростом показателей, но и сравнительно высокой финансовой устойчивостью.

Именно поэтому проблемы защиты информации в банковской системе Кыргызской Республики выходят за пределы узкофункциональной банковской практики. Чем более значимым становится банковский сектор для экономики страны, тем выше системные последствия потенциальных инцидентов, связанных с кибератаками, мошенничеством, нарушением доступности сервисов или компрометацией платежной инфраструктуры. В современных условиях обеспечение информационной безопасности банковского сектора КР должна оцениваться как фактор макрофинансовой устойчивости [8].

2. Рост цифровых платежей и дистанционного банковского обслуживания

В последнее время одним из основных направлений развития банковской системы Кыргызской Республики выступает расширение дистанционных форм обслуживания. Тем более актуальное регулирование НБ КР прямо предусматривает возможность предоставления банковских и платежных услуг через широкий спектр удаленных каналов: банкоматы, платежные терминалы, интернет-банкинг, мобильный банкинг, мобильные приложения, электронные кошельки и иные формы дистанционного взаимодействия [2]. Из этого исходит, что цифровые технологии в банковской системе страны стали не вспомогательным элементом банковской деятельности, а ее полноценной инфраструктурной составляющей.

Ещё одним важнейшим фактом цифровой трансформации стало расширение использование QR-кодов. По состоянию на 1 декабря 2025 г. общее количество установленных в Кыргызской Республике QR-кодов достигло 108,8 тыс. единиц, что на 70 % больше по сравнению с аналогичным периодом предыдущего года [3]. Данный показатель отражает стремительное расширение безналичного обращения и внедрение цифровых способов оплаты в повседневных финансовых операциях.

Высокая динамика цифровой трансформации проявляется и в объеме операций. В IV квартале 2025 г. через основного оператора взаимодействия было проведено 525,1 млн

платежей на сумму 908,6 млрд сомов, из которых 27,2 млн платежей на сумму 27,2 млрд сомов пришлись на государственные услуги [3]. На основе этих данных можно сделать вывод о том, что цифровые платежные системы уже превратились в массовую инфраструктуру, обеспечивающую как коммерческие, так и социально значимые платежи.

Существенно усложняется и институциональная архитектура платежного рынка. Согласно реестру НБ КР, опубликованному 19 марта 2026 г., в Кыргызской Республике действовали 55 лицензий операторов платежных систем и 19 лицензий платежных организаций [5]. Такое положение указывает на формирование многосубъектного цифрового пространства, в котором банки взаимодействуют с процессинговыми центрами, платежными организациями, техническими посредниками и иными инфраструктурными участниками.

Следовательно, развитие цифрового взаимодействия в банковском секторе экономики Кыргызской Республике сопровождается не только количественным ростом финансовых операций, но и повышением сложности самого цифрового пространства. Чем больше каналов, участников и интеграционных связей включено в единую операционную среду, тем выше значимость вопросов безопасности и устойчивости этой среды.

3. Цифровизация как фактор усиления рисков информационной безопасности

Расширение дистанционных операций закономерно ведет к трансформации профиля рисков банковской деятельности. В традиционной модели банковского обслуживания значительная часть контроля осуществлялась в физическом пространстве банковского отделения. В цифровой модели финансовой системы значительный массив операций переносится в удаленную среду, где растет роль аутентификации клиента, информационной защиты пользовательских данных, устойчивости предлагаемых банками мобильных приложений и достаточной корректности работы удаленных точек доступа [10].

Первая группа таких рисков связана с ростом клиентских киберугроз. Известно, что массовое использование мобильного и интернет-банкинга повышает вероятность фишинга, перехвата учетных данных, несанкционированного доступа к пользовательским аккаунтам и компрометации сессий дистанционного обслуживания. НБ КР на действующем ныне этапе регулирования прямо закрепляет обязанность поставщиков дистанционных услуг информировать клиентов о правилах безопасного поведения, в том числе о недопустимости передачи третьим лицам логинов, паролей и иных идентификаторов [2]. Это свидетельствует о том, что пользователь в цифровом банкинге рассматривается как активный элемент общей системы безопасности.

Вторая группа рисков обусловлена интеграционным характером современной финансовой среды. В концепции развития открытого банкинга в Кыргызской Республике подчеркивается, что API уже широко используются участниками банковского сектора для взаимодействия с платежными системами и обмена данными между информационными системами [4]. В концепции API рассматриваются как базовый инструмент интеграции банков, платежных систем и других участников цифрового финансового рынка [4]. С точки зрения информационной безопасности говорится о том, что надежность банка все в большей степени зависит не только от защищенности его внутренних систем, но и от безопасности внешних интерфейсов, протоколов обмена, механизмов идентификации и контроля доступа.

Третья группа рисков обусловлена с усилением зависимости банковской деятельности от внешних акторов и инфраструктурных посредников. Регулирование удаленного обслуживания допускает участие операторов связи [2], а платежная среда опирается на операторов взаимодействия, процессинговые организации и иные внешние элементы инфраструктуры [3; 5]. В такой ситуации инцидент на стороне третьего участника системы способен трансформироваться в операционную проблему банка, включая перебои в предоставлении услуг, задержки платежей, нарушение доступности сервисов и снижение доверия со стороны клиентов.

Из вышеперечисленного исходит, что цифровизация банковского сектора не снижает, а, напротив, усложняет требования к информационной безопасности. Защита банковской системы в цифровой среде предполагает уже не только физическую, аппаратно-программную и организационную защиты внутренних ИТ-ресурсов, но и управление распределенной экосистемой рисков, включающей клиентов, интерфейсы интеграции, внешних контрагентов и инфраструктурные платформы.

4. Регуляторный поворот 2025–2026 гг.: от декларативной безопасности к прикладной антифрод-устойчивости

Ключевой особенностью регулирования 2025–2026 гг. стало смещение акцента от общего требования обеспечения безопасности к формированию прикладной модели кибер- и антифрод-устойчивости. Постановлением правления Национального банка от 26 сентября 2025 г. в банковское регулирование были включены специальные минимальные требования к системе противодействия внутреннему и внешнему мошенничеству [6].

Внедренная модель регулирования обеспечения информационной безопасности банковского сектора принципиально важна по следующим причинам.

Во-первых, банк обязан не просто использовать отдельные защитные инструменты, а обеспечить наличие и эффективное функционирование антифрод-системы [6].

Во-вторых, политика противодействия мошенничеству в системах удаленного и дистанционного банковского обслуживания должна утверждаться советом директоров банка [6]. Это означает, что антифрод поднимается из уровня внутренней технической процедуры на уровень корпоративного управления и стратегического контроля [9].

В-третьих, становится явным, что требования НБ КР носят выраженно прикладной характер. Антифрод-системы должны обеспечивать последовательный и непрерывный по времени мониторинг и оценку риска по каждой расходной транзакции, который осуществляется через дистанционные каналы обслуживания, невзирая на ее суммы, регулярности или истории предыдущих операций [6]. Такое положение отражает переход регулятора от формального контроля к риск-ориентированной модели, которая предполагает постоянную аналитическую оценку цифровых операций в режиме, приближенном к реальному времени.

В-четвертых, НБ КР установил требование о формировании и ведении реестра запрещенных к обслуживанию идентификаторов и атрибутов, запятнанных с мошенническими операциями. В такой реестр могут включаться номера телефонов граждан, ID, QR-коды, сервисные имена отправителей и получателей, а также иные идентификаторы, ассоциированные с мошеннической активностью [6]. Этот инструмент констатирует, что современное регулирование стремится не только реагировать на уже совершенные инциденты, но и формировать превентивные меры блокирования подозрительных операций.

Немаловажным считается и расширение ряда операций, подлежащих антифрод-контролю. Также оценке риска подлежат операции, связанные с кредитованием, QR-платежами, внутрибанковскими и межбанковскими переводами, системами «ГРОСС» и «КЛИРИНГ», международными переводами, снятием наличных, POS-операциями и переводами на кошельки виртуальных активов [6].

Такой охват подтверждает, что антифрод больше не воспринимается как некий инструмент защиты отдельных дистанционных каналов; антифрод становится элементом комплексного управления платежной и расчетной деятельностью банка.

Необходимо подчеркнуть то, что принципиально важной особенностью новой регуляторной модели выступает требование о доказуемой результативности антифрод-механизмов. При этом банк обязан использовать систему метрик, включающую долю ложноположительных срабатываний, среднее время выявления инцидента, среднее время реагирования, количество выявленных схем мошенничества и качество ведения соответствующего реестра [6]. Результаты таких аудитов должны документироваться и представляться в Национальный банк не реже одного раза в квартал [6]. Кроме того, не реже

одного раза в год банками должны проводиться стресс-тестирование, тесты на проникновение и проверка новых алгоритмов с учетом актуальных мошеннических схем [6].

В совокупности эти внедрения позволяют утверждать, что в 2025–2026 гг. в Кыргызской Республике сформировался новый подход к регулированию информационной безопасности банковской системы. Его специфика состоит в интеграции вопросов ИБ, антифрода, внутреннего контроля и операционного риска в единую систему надзора и управления устойчивостью.

Заключение

Проведенные выше виды анализа показывают, что современное состояние банковской системы Кыргызской Республики определяется сочетанием двух взаимосвязанных направлений: устойчивого финансового роста и динамики цифровой трансформации банковского сектора экономики. Банковский сектор республики обладает значительным масштабом в пределах и за пределами страны, высоким уровнем капитализации и важной ролью в экономике, что придает вопросам его устойчивости системный характер [1].

Одновременно развитие удаленного обслуживания, рост QR-платежей, распространение API-приложений и расширение числа участников платежной инфраструктуры существенно усложняют среду функционирования банков [2–5]. Интенсификация цифровизации банковского сектора страны повышает доступность населению финансовых услуг, но одновременно расширяет области информационных атак злоумышленниками и усиливает зависимость банков от поведения разношерстных клиентов, надежности интерфейсов интеграции, внешних поставщиков и качества антифрод-механизмов.

В этих условиях обеспечение информационной безопасности банковского сектора должно рассматриваться не как вспомогательные действия, а как один из базовых факторов стабильности банковской системы. Регуляторные изменения 2025–2026 гг. демонстрируют, что Национальный банк Кыргызской Республики последовательно переводит вопросы киберустойчивости и противодействия мошенничеству в плоскость корпоративного управления, операционного риска, контроля эффективности и защиты потребителей финансовых услуг [6].

Следовательно, дальнейшее развитие банковской системы Кыргызской Республики будет напрямую зависеть от возможности и наличия соответствующих программных средств у участников рынка. Это должно обеспечить не только технологическое развитие цифровых сервисов, но и устойчивость всей цифровой финансовой экосистемы.

В этой перспективе информационная безопасность становится необходимым условием сохранения доверия к банковскому сектору в условиях конкуренции банков, непрерывности платежного оборота и стабильности национальной финансовой системы и банковской системы в целом [11].

Литература

1. Национальный банк Кыргызской Республики. Официальный обзор банковской системы Кыргызской Республики по состоянию на 31 января 2026 г.
2. Национальный банк Кыргызской Республики. Положение о минимальных требованиях по предоставлению удаленного/дистанционного обслуживания в Кыргызской Республике (в актуальной редакции по состоянию на 13 февраля 2026 г.).
3. Национальный банк Кыргызской Республики. Официальные статистические данные о развитии QR-инфраструктуры и безналичных платежей по состоянию на 1 декабря 2025 г.

4. Национальный банк Кыргызской Республики. Концепция развития открытого банкинга в Кыргызской Республике.

5. Национальный банк Кыргызской Республики. Реестр лицензий операторов платежных систем и платежных организаций. Опубликовано 19 марта 2026 г.

6. Национальный банк Кыргызской Республики. Постановление правления от 26 сентября 2025 г. о минимальных требованиях к системе противодействия внутреннему и внешнему мошенничеству в банковской деятельности.

7. Алексанов, А. К.; Демчев, И. А.; Доронин А. М. и др. Безопасность карточного бизнеса: бизнес-энциклопедия. — М.: Московская финансово-промышленная академия, 2012. — С. 432.

8. Внуков, А. А. Защита информации в банковских системах : учебник для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Изд-во Юрайт, 2026. — 246 с.

9. Кудряшова О.А., Ильина А.В. Аналитическая система антифрод как комплекс мер для оценки риска финансовых транзакций // Актуальные вопросы экономической теории: развитие и применение в практике российских преобразований: материалы III Всероссийской научно-практической конференции, Казань, 28 января 2021 года. – Казань: Изд-во «Познание», 2021. – С.91–96.

10. Манапбаев, И. К. Актуальные проблемы использования ЭЦП в Кыргызстане // Вестник МУК. –2025. –№2(59). – С. 145–153.

11. Манапбаев, И. К. Роль методов ценевой и неценевой конкуренции на рынке банковских услуг на пути к индустрии 4.0 // Вестник МУК. – 2025. – №2(59). – С. 230 – 235.