

КИБЕРБЕЗОПАСНОСТЬ И ЦИФРОВАЯ ГРАМОТНОСТЬ КАК УСЛОВИЯ УСТОЙЧИВОГО РАЗВИТИЯ ЦИФРОВОГО БАНКИНГА

Аширкулов Диорбек Алишер угли

Студент 4 курса направления «Банковское дело и аудит»,

Самаркандский институт Экономики и Сервиса

Каримова Азиза Махомадризовна

Научный руководитель, д.э.н.,

Самаркандский институт Экономики и Сервиса

<https://doi.org/10.5281/zenodo.20489527>

Аннотация: В статье рассматриваются кибербезопасность и цифровая грамотность как ключевые условия устойчивого развития цифрового банкинга в Узбекистане. Особое внимание уделяется рискам, возникающим при использовании мобильного банкинга, интернет-банкинга, онлайн-платежей и P2P-переводов. Раскрываются такие угрозы, как фишинг, социальная инженерия, утечка персональных данных, поддельные приложения и несанкционированный доступ к банковским аккаунтам. Отмечается, что безопасность цифрового банкинга зависит не только от технической защиты банковских платформ, но и от поведения пользователей. Сделан вывод о необходимости комплексного подхода, включающего развитие антифрод-систем, защиту персональных данных, повышение квалификации банковского персонала и системное обучение клиентов правилам безопасного использования цифровых финансовых услуг.

Ключевые слова: цифровой банкинг, кибербезопасность, цифровая грамотность, мобильный банкинг, интернет-банкинг, онлайн-платежи, P2P-переводы, фишинг, персональные данные, антифрод-системы, Республика Узбекистан.

Annotatsiya: Maqolada O'zbekistonda raqamli bankingning barqaror rivojlanishi uchun kiberxavfsizlik va raqamli savodxonlikning ahamiyati ko'rib chiqiladi. Asosiy e'tibor mobil banking, internet-banking, onlayn to'lovlar va P2P pul o'tkazmalaridan foydalanishda yuzaga keladigan xavflarga qaratilgan. Fishing, ijtimoiy muhandislik, shaxsga doir ma'lumotlarning sizib chiqishi, soxta ilovalar va bank akkauntlariga ruxsatsiz kirish kabi tahdidlar yoritiladi. Ta'kidlanishicha, raqamli banking xavfsizligi nafaqat bank platformalarining texnik himoyasiga, balki foydalanuvchilarning xatti-harakati va raqamli savodxonligiga ham bog'liq. Xulosa sifatida antifrod tizimlarini rivojlantirish, shaxsga doir ma'lumotlarni himoya qilish, bank xodimlari malakasini oshirish va mijozlarni raqamli moliyaviy xizmatlardan xavfsiz foydalanish qoidalariga o'rgatishni o'z ichiga olgan kompleks yondashuv zarurligi qayd etiladi.

Kalit so'zlar: raqamli banking, kiberxavfsizlik, raqamli savodxonlik, mobil banking, internet-banking, onlayn to'lovlar, P2P pul o'tkazmalari, fishing, shaxsga doir ma'lumotlar, antifrod tizimlari, O'zbekiston Respublikasi.

Abstract: The article examines cybersecurity and digital literacy as key conditions for the sustainable development of digital banking in Uzbekistan. Particular attention is paid to the risks arising from the use of mobile banking, internet banking, online payments and P2P transfers. The article discusses threats such as phishing, social engineering, personal data leakage, fake applications and unauthorized access to banking accounts. It is noted that the security of digital banking depends not only on the technical protection of banking platforms, but also on users' behavior and digital literacy. The article concludes that a comprehensive

approach is necessary, including the development of anti-fraud systems, personal data protection, improving the qualifications of bank employees and systematically educating customers on the safe use of digital financial services.

Keywords: digital banking, cybersecurity, digital literacy, mobile banking, internet banking, online payments, P2P transfers, phishing, personal data, anti-fraud systems, Republic of Uzbekistan.

Введение. В условиях активного развития цифрового банкинга кибербезопасность и цифровая грамотность становятся важнейшими условиями устойчивости банковского сектора. В Узбекистане коммерческие банки всё шире внедряют мобильный банкинг, интернет-банкинг, онлайн-платежи, P2P-переводы и другие дистанционные сервисы. Центральный банк Республики Узбекистан определяет дистанционное банковское обслуживание как систему, позволяющую клиенту удалённо осуществлять платежи и управлять банковскими счетами.

Актуальность темы связана с тем, что рост цифровых банковских услуг одновременно повышает удобство для клиентов и увеличивает риски кибермошенничества. К таким рискам относятся фишинг, социальная инженерия, утечка персональных данных, поддельные приложения, несанкционированный доступ к аккаунтам и незаконные переводы. Поэтому безопасность цифрового банкинга зависит не только от технических систем банка, но и от поведения самих пользователей.

Проблема кибербезопасности признаётся на институциональном уровне. Центральный банк проводит мероприятия, направленные на повышение осведомлённости о кибербезопасности и борьбе с финансовым мошенничеством в условиях использования цифровых технологий.

Целью данной статьи является анализ роли кибербезопасности и цифровой грамотности как условий устойчивого развития цифрового банкинга в Узбекистане.

Для достижения данной цели в статье рассматриваются основные киберугрозы в цифровом банкинге, значение цифровой грамотности клиентов, роль банков и регулятора в обеспечении безопасности онлайн-операций, а также направления повышения доверия населения к цифровым финансовым услугам.

Методология. Методологическую основу исследования составляет комплексный анализ кибербезопасности и цифровой грамотности как факторов устойчивого развития цифрового банкинга в Узбекистане. В рамках статьи цифровой банкинг рассматривается как совокупность дистанционных банковских услуг, включающих мобильный банкинг, интернет-банкинг, онлайн-платежи, P2P-переводы, электронные договоры и иные цифровые финансовые сервисы.

Информационной базой исследования послужили материалы Центрального банка Республики Узбекистан, нормативно-правовые акты в сфере платёжных систем, персональных данных и кибербезопасности, аналитические отчёты международных организаций, а также научные публикации, посвящённые цифровой грамотности, финансовым технологиям и информационной безопасности в банковском секторе.

Основное внимание в статье уделяется анализу таких вопросов, как фишинг, социальная инженерия, утечка персональных данных, несанкционированный доступ к банковским аккаунтам, роль антифрод-систем, значение цифровой грамотности

клиентов и необходимость повышения компетенций банковского персонала. Такой подход позволяет определить, каким образом кибербезопасность и цифровая грамотность влияют на доверие клиентов и устойчивость цифровых банковских услуг.

Обзор литературы: В научной и аналитической литературе кибербезопасность цифрового банкинга рассматривается не только как техническая задача, но и как комплексная проблема, связанная с поведением пользователей, защитой персональных данных, качеством банковских информационных систем и уровнем цифровой грамотности населения. В отличие от традиционного банковского обслуживания, цифровой банкинг предполагает удалённое взаимодействие клиента с банком, что увеличивает значение безопасной идентификации, защиты доступа и правильного поведения пользователя при совершении онлайн-операций.

Нормативную основу исследования составляет Закон Республики Узбекистан «О кибербезопасности», который определяет общие правовые основы обеспечения кибербезопасности и подчёркивает необходимость соблюдения законодательства в данной сфере [1]. Для банковского сектора этот источник важен тем, что цифровые банковские услуги относятся к сфере повышенного риска: сбои, атаки или утечки данных могут привести не только к финансовым потерям, но и к снижению доверия населения к онлайн-сервисам.

Важное значение имеет законодательство о персональных данных. Закон Республики Узбекистан «О персональных данных» регулирует отношения, связанные с обработкой и защитой персональных данных [2]. Для цифрового банкинга это особенно актуально, поскольку банки обрабатывают паспортные данные, номера телефонов, сведения о счетах, операциях, устройствах клиента и иногда биометрическую информацию. В 2026 году были уточнены требования к хранению отдельных категорий персональных данных на территории Узбекистана, включая биометрические данные физических лиц [3]. Это показывает, что защита данных становится одним из ключевых элементов цифровой безопасности.

Материалы Центрального банка Республики Узбекистан подчёркивают практическую значимость проблемы. В 2024 году Центральный банк организовал семинар «Секреты безопасности в эпоху цифровых технологий: кибербезопасность и борьба с финансовым мошенничеством», где рассматривались вопросы информационной безопасности и кибербезопасности при использовании цифровых технологий [4]. Это подтверждает, что регулятор рассматривает кибербезопасность как необходимое условие устойчивого развития финансового сектора.

Аналитические исследования по цифровой экономике Узбекистана также выделяют цифровую грамотность и безопасность данных как важные вызовы для дальнейшей цифровизации. В отчёте UNDP о цифровой экономике Узбекистана отмечается необходимость развития цифровых навыков, предпринимательских компетенций и устойчивой цифровой среды [5]. Для банковского сектора это означает, что распространение мобильного банкинга и онлайн-платежей должно сопровождаться обучением клиентов правилам безопасного поведения в цифровой среде.

В научных публикациях по кибербезопасности банковской системы Узбекистана среди наиболее серьёзных угроз выделяются фишинг, социальная инженерия, слабые механизмы контроля доступа, уязвимости мобильного банкинга и API, а также

недостаточно развитые антифрод-системы [6]. Данные работы показывают, что безопасность цифрового банкинга зависит не только от программной защиты банка, но и от способности выявлять подозрительные операции, предотвращать мошенничество и снижать риски человеческого фактора.

Таким образом, анализ литературы показывает, что устойчивое развитие цифрового банкинга требует сочетания трёх элементов: надёжной технической защиты банковских систем, эффективного правового регулирования и высокого уровня цифровой грамотности клиентов. При отсутствии хотя бы одного из этих элементов цифровые банковские услуги могут стать источником повышенных рисков для банков, клиентов и всей финансовой системы.

Результаты анализа. Проведённый анализ показывает, что кибербезопасность и цифровая грамотность являются взаимосвязанными условиями устойчивого развития цифрового банкинга. Техническая защита банковских систем сама по себе не может полностью обеспечить безопасность онлайн-операций, если клиенты не обладают достаточными знаниями о цифровых рисках. В то же время высокая цифровая грамотность пользователей не заменяет необходимость надёжной банковской инфраструктуры, антифрод-систем, защиты персональных данных и постоянного мониторинга подозрительных операций.

Развитие мобильного банкинга, интернет-банкинга, онлайн-платежей и P2P-переводов увеличивает количество цифровых операций, совершаемых клиентами ежедневно. Это повышает удобство банковского обслуживания, но одновременно расширяет пространство для киберугроз. Наиболее распространёнными рисками являются фишинговые ссылки, поддельные сайты банков, вредоносные мобильные приложения, звонки мошенников от имени сотрудников банка, кража одноразовых SMS-кодов и попытки получить доступ к персональным данным клиента [1].

Особенно опасной угрозой является социальная инженерия. В отличие от технического взлома, она основана на психологическом воздействии на клиента. Мошенники убеждают пользователя самостоятельно сообщить пароль, код подтверждения, данные карты или перейти по поддельной ссылке. В таких случаях даже защищённая банковская система может оказаться уязвимой, поскольку операция формально подтверждается самим клиентом. Поэтому устойчивость цифрового банкинга зависит не только от IT-безопасности банков, но и от способности клиентов распознавать мошеннические схемы.

Таблица 1

Основные киберугрозы в цифровом банкинге¹

Вид угрозы	Содержание	Возможные последствия
Фишинг	Поддельные ссылки, сайты и сообщения	Кража логина, пароля, данных карты

¹ cbu.uz. Семинар «Секреты безопасности в эпоху цифровых технологий: кибербезопасность и борьба с финансовым мошенничеством».

Социальная инженерия	Обман клиента через звонки или мессенджеры	Передача кодов подтверждения мошенникам
Поддельные приложения	Установка вредоносных программ	Доступ к банковским данным клиента
Утечка персональных данных	Незаконное распространение клиентской информации	Финансовые потери и нарушение прав клиента
Несанкционированный доступ	Вход в аккаунт без согласия владельца	Незаконные переводы и списания
Слабая цифровая грамотность	Ошибки пользователя при онлайн-операциях	Повышение риска мошенничества

Важным направлением защиты цифрового банкинга является развитие антифрод-систем. Такие системы позволяют выявлять подозрительные операции, анализировать необычное поведение пользователя, блокировать потенциально опасные транзакции и предупреждать клиента о возможном мошенничестве. В условиях роста онлайн-платежей и мобильных переводов антифрод-механизмы становятся обязательной частью банковской безопасности. Однако их эффективность зависит от качества данных, скорости обработки операций и способности банка быстро реагировать на инциденты.

Отдельное значение имеет защита персональных данных. Цифровой банкинг предполагает обработку паспортных данных, номеров телефонов, банковских счетов, истории платежей, информации об устройствах клиента и в некоторых случаях биометрических данных. Утечка такой информации может использоваться мошенниками для оформления кредитов, доступа к аккаунтам или проведения незаконных операций. Поэтому банки должны обеспечивать безопасное хранение данных, ограничение доступа сотрудников к конфиденциальной информации и соблюдение требований законодательства о персональных данных [2].

Цифровая грамотность клиентов выступает не менее важным условием безопасности. Пользователь должен понимать, что нельзя передавать третьим лицам SMS-коды, PIN-коды, CVV-коды, пароли от мобильного приложения и данные банковской карты. Также важно уметь отличать официальный сайт банка от поддельного, проверять адреса ссылок, не устанавливать приложения из неизвестных источников и своевременно обращаться в банк при подозрительных операциях. Чем выше уровень цифровой грамотности населения, тем ниже вероятность успешного мошенничества.

Таблица 2

Навыки цифровой грамотности, необходимые пользователям цифрового банкинга²

Навык	Практическое значение
Проверка ссылок и сайтов	Защита от фишинга

² sbu.uz. Семинар «Секреты безопасности в эпоху цифровых технологий: кибербезопасность и борьба с финансовым мошенничеством».

Неразглашение SMS-кодов и паролей	Предотвращение несанкционированных операций
Использование официальных приложений	Снижение риска установки вредоносного ПО
Контроль уведомлений банка	Быстрое выявление подозрительных списаний
Понимание условий онлайн-операций	Снижение ошибок при платежах и переводах
Обращение в банк при угрозе	Быстрая блокировка карты или аккаунта

Роль банков в повышении цифровой грамотности клиентов должна быть более активной. Недостаточно только размещать предупреждения в мобильном приложении. Банки могут проводить информационные кампании, отправлять короткие обучающие уведомления, публиковать инструкции по безопасному использованию карт и приложений, объяснять типичные схемы мошенничества и регулярно напоминать клиентам о правилах защиты данных. Особенно важно делать такие материалы простыми и понятными для пожилых людей, жителей регионов и пользователей с низким уровнем цифровых навыков.

Кадровая подготовка банковского персонала также имеет большое значение. Сотрудники банков должны не только обслуживать клиентов, но и объяснять им правила безопасного использования цифровых сервисов. Кроме того, банкам необходимы специалисты в области кибербезопасности, анализа данных, антифрод-мониторинга и управления цифровыми рисками. Без квалифицированных кадров даже современные технологические решения могут использоваться неэффективно.

Значимую роль играет и Центральный банк Республики Узбекистан как регулятор финансового сектора. Его деятельность должна быть направлена на формирование требований к безопасности цифровых банковских услуг, мониторинг рисков, повышение устойчивости платёжной инфраструктуры и развитие финансовой грамотности населения. Проведение семинаров и информационных мероприятий по борьбе с финансовым мошенничеством показывает, что проблема кибербезопасности признаётся на институциональном уровне [7].

В то же время развитие цифрового банкинга требует баланса между удобством и безопасностью. Если система защиты будет слишком сложной, клиентам станет неудобно пользоваться мобильным банкингом. Если же процедуры будут чрезмерно упрощены, возрастут риски мошенничества. Поэтому банки должны внедрять такие решения, которые одновременно обеспечивают высокий уровень защиты и сохраняют удобство для пользователя. К таким инструментам относятся многофакторная аутентификация, биометрическая идентификация, push-уведомления, лимиты на операции, временная блокировка подозрительных переводов и персонализированные предупреждения.

Заключение. таким образом, кибербезопасность и цифровая грамотность являются необходимыми условиями устойчивого развития цифрового банкинга в Узбекистане. Расширение мобильного банкинга, интернет-банкинга, онлайн-платежей и P2P-переводов повышает удобство банковского обслуживания, однако одновременно

увеличивает риски фишинга, социальной инженерии, утечки персональных данных и несанкционированного доступа к банковским аккаунтам.

Проведённый анализ показывает, что безопасность цифрового банкинга зависит не только от технической защиты банковских платформ, но и от поведения пользователей. Даже современные антифрод-системы, многофакторная аутентификация и защищённые мобильные приложения не могут полностью исключить риски, если клиенты передают коды подтверждения, переходят по поддельным ссылкам или используют неофициальные приложения.

В связи с этим дальнейшее развитие цифрового банкинга должно сопровождаться комплексными мерами: усилением киберзащиты банковских систем, развитием антифрод-механизмов, защитой персональных данных, повышением квалификации банковского персонала и системным обучением клиентов правилам безопасного использования цифровых сервисов. Особое значение имеет формирование доверия населения к онлайн-операциям, поскольку именно доверие определяет готовность клиентов активно использовать цифровые банковские услуги.

Следовательно, устойчивость цифрового банкинга в Узбекистане будет зависеть от совместных действий банков, регулятора и пользователей. Только сочетание технологической безопасности и высокого уровня цифровой грамотности позволит снизить риски мошенничества, повысить качество дистанционного обслуживания и обеспечить дальнейшее развитие цифровой финансовой экосистемы страны.

Adabiyotlar, References, Литературы:

1. Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764
2. Закон Республики Узбекистан «О персональных данных» от 02.07.2019 г. № ЗРУ-547
3. Закон Республики Узбекистан «О внесении изменений и дополнения в Закон Республики Узбекистан “О персональных данных”» от 26.03.2026 г. № ЗРУ-1125
4. sbi.uz. Семинар «Секреты безопасности в эпоху цифровых технологий: кибербезопасность и борьба с финансовым мошенничеством».
5. Отчет UNDP «Digital Economy of Uzbekistan: The State of Digital Entrepreneurship and Artificial Intelligence», 2025.
6. Cybersecurity in Uzbekistan’s Banking System // Web of Journals. 2026.
7. Материалы Центрального банка Республики Узбекистан о «Дистанционное банковское обслуживание».
8. Лаврушин О.И. Банковское дело: учебник. — М: КНОРУС, 2020.
9. Касперский Е.В. Компьютерная безопасность: угрозы и методы защиты. — М: Эксмо, 2021.