МОШЕННИЧЕСТВО ПРИ ПЕРЕВОДЕ БЕЗНАЛИЧНЫХ РАСЧЕТОВ И ЕГО ПРЕДУПРЕЖДЕНИЕ

Жалилов Шахзоджон Эркин угли
Гайбуллаев Абубакир Улугбек угли
Самаркандский институт экономики и сервиса
Факультет среднего и высшего образования
Банковское дело и аудиторский факультет, студента

Холмирзаев Элбек Бахтиёрович

Преподаватель Самаркандского института
экономики и сервиса

Doi: https://doi.org/10.5281/zenodo.20351167

Аннотация: В статье исследуются современные формы мошенничества при осуществлении безналичных расчетов, а также механизмы их предупреждения в банковской системе Республики Узбекистан. Рассматриваются основные схемы незаконного завладения денежными средствами через мобильные приложения, интернет-банкинг и дистанционные платежные сервисы. Особое внимание уделено влиянию цифровизации финансового сектора на рост киберпреступности, анализируются причины увеличения количества мошеннических операций и недостатки системы защиты электронных платежей. В работе изучен отечественный и зарубежный опыт противодействия финансовому мошенничеству, выявлены проблемы правового и организационного характера. На основе проведенного анализа предложены направления совершенствования системы безопасности безналичных расчетов и повышения финансовой грамотности населения.

Ключевые слова: безналичные расчеты, банковское мошенничество, киберпреступность, дистанционные платежи, финансовая безопасность, коммерческие банки, цифровые технологии, интернет-банкинг, электронные платежи, Узбекистан.

FRAUD IN CASHLESS TRANSACTIONS AND ITS PREVENTION

Abstract: This article examines modern forms of fraud in cashless payments, as well as mechanisms for their prevention in the banking system of the Republic of Uzbekistan. It examines the main schemes for the illegal appropriation of funds through mobile applications, online banking, and remote payment services. Particular attention is paid to the impact of digitalization of the financial sector on the growth of cybercrime, and the reasons for the increase in fraudulent transactions and the shortcomings of the electronic payment security system are analyzed. This paper examines domestic and international practices in combating financial fraud, identifying legal and organizational challenges. Based on this analysis, it proposes ways to improve the security of cashless payments and increase financial literacy.

Keywords: cashless payments, banking fraud, cybercrime, remote payments, financial security, commercial banks, digital technologies, online banking, electronic payments, Uzbekistan.

Введение. В последние годы система безналичных расчетов в Узбекистане развивается особенно быстро. Расширение цифровых банковских услуг, рост популярности мобильных приложений и увеличение количества онлайн-платежей значительно упростили финансовые операции населения. Вместе с этим усилилась и проблема мошенничества в сфере электронных переводов. Еще несколько лет назад основная часть финансовых преступлений была связана с наличными денежными средствами, однако сейчас ситуация изменилась. Кибермошенники начали активно использовать цифровые каналы для незаконного получения доступа к банковским счетам

граждан. Иногда кажется, что развитие технологий происходит быстрее, чем адаптация системы безопасности к новым угрозам. По данным Центрального банка Республики Узбекистан, количество пользователей мобильного банкинга в 2024 году превысило 38 миллионов. Это почти в два раза больше по сравнению с 2020 годом. Одновременно увеличилось число обращений граждан, связанных с незаконными списаниями денежных средств и мошенническими переводами. Особенно часто преступники используют методы социальной инженерии. Людей убеждают самостоятельно сообщать конфиденциальные данные, коды подтверждения и пароли. Интересно, что жертвами становятся не только пожилые люди, но и молодежь, активно использующая цифровые сервисы. В некоторых случаях мошенники действуют настолько профессионально, что пользователи даже не подозревают о преступлении до момента списания средств. Проблема приобретает не только экономический, но и социальный характер. Потеря денежных средств подрывает доверие населения к банковской системе и цифровым технологиям в целом.

Методология. Исследование основано на анализе статистических данных банковского сектора Республики Узбекистан, материалов Центрального банка, публикаций отечественных и зарубежных ученых, а также информации правоохранительных органов по вопросам финансового мошенничества. В работе использованы методы сравнительного анализа, логического обобщения, системного подхода и статистического исследования. Особое внимание уделялось изучению динамики развития безналичных платежей и росту преступлений в цифровой среде за период 2020–2025 годов. Были проанализированы наиболее распространенные схемы мошенничества, применяемые при переводе денежных средств через мобильные приложения и интернет-банкинг. Для оценки эффективности существующих механизмов защиты использовались сравнительные показатели количества мошеннических операций, скорости реагирования банков и уровня цифровой безопасности. Кроме того, в исследовании изучался зарубежный опыт противодействия финансовому мошенничеству. Анализ показал, что в развитых странах основной акцент делается не только на технической защите, но и на профилактике. Это достаточно важный момент. Иногда банки концентрируются исключительно на совершенствовании программного обеспечения, забывая о человеческом факторе. Между тем большая часть мошеннических операций совершается именно из-за невнимательности пользователей. В исследовании также применялся метод наблюдения за изменением поведения клиентов в условиях цифровизации банковского обслуживания. Отдельно были рассмотрены законодательные меры, регулирующие безопасность электронных платежей в Узбекистане.

Результаты исследования. Проведенное исследование показало, что мошенничество при безналичных расчетах в Узбекистане за последние пять лет значительно трансформировалось. Если ранее преобладали простые схемы с использованием поддельных банковских карт, то сейчас основная часть преступлений связана с мобильными приложениями и дистанционными переводами денежных средств. По данным МВД Республики Узбекистан, в 2024 году количество зарегистрированных киберпреступлений выросло почти на 42% по сравнению с 2022 годом. Особенно быстро увеличилось число случаев, связанных с незаконным доступом к банковским приложениям. Преступники активно используют телефонные звонки от имени сотрудников банка, поддельные сайты, фальшивые ссылки и сообщения в мессенджерах. Иногда схема выглядит настолько убедительно, что человек сам переводит деньги мошенникам. Интересно, что большая часть преступлений совершается не путем взлома банковских систем, а через психологическое воздействие на клиентов. Это говорит о высокой эффективности методов социальной инженерии. Кроме того, было установлено, что наиболее уязвимой категорией пользователей являются граждане, недавно начавшие пользоваться цифровыми банковскими сервисами. Многие из них недостаточно осведомлены о правилах финансовой безопасности. В отдельных случаях мошенники используют данные, полученные через социальные сети. Они изучают информацию о человеке и выстраивают более убедительную схему общения. [1]

Исследование показало, что коммерческие банки Узбекистана постепенно усиливают меры

защиты безналичных расчетов. В последние годы были внедрены дополнительные механизмы аутентификации, системы автоматического мониторинга подозрительных операций и биометрическая идентификация клиентов. Некоторые банки начали использовать искусственный интеллект для анализа поведения пользователей. Например, система способна выявлять необычные финансовые операции и временно блокировать перевод до подтверждения личности клиента. Это позволило сократить количество мошеннических операций. Однако полностью решить проблему пока не удается. Причина заключается в постоянном изменении методов мошенничества. [2]

Как только банки усиливают один уровень защиты, преступники начинают искать новые способы обхода системы. Иногда создается впечатление своеобразной гонки технологий. В 2023 году ряд крупных банков Узбекистана увеличил расходы на кибербезопасность более чем на 25%. Это довольно серьезный показатель. Он демонстрирует, насколько важной стала проблема финансовой безопасности в современных условиях. Вместе с тем небольшие коммерческие банки не всегда располагают достаточными ресурсами для внедрения сложных систем защиты. Это создает дополнительные риски.

Одним из наиболее распространенных видов мошенничества остается фишинг. Пользователю отправляется ссылка, внешне похожая на официальный банковский сайт. После ввода логина и пароля преступники получают доступ к счету клиента. Подобные схемы особенно активно распространились в период пандемии COVID-19, когда количество онлайн-платежей резко увеличилось. [3]

В Узбекистане рост электронных переводов в 2021 году составил более 30%. Вместе с этим выросло и количество мошеннических операций. Некоторые эксперты связывают это с недостаточной цифровой грамотностью населения. Действительно, многие пользователи не проверяют адрес сайта, не обращают внимания на подозрительные сообщения и легко сообщают персональные данные. Проблема осложняется тем, что мошенники часто используют номера телефонов, визуально похожие на официальные банковские контакты. Иногда граждане теряют крупные суммы буквально за несколько минут. Особенно тяжело такие ситуации воспринимаются людьми, использующими банковские приложения для хранения семейных накоплений. Финансовый ущерб сопровождается психологическим стрессом и утратой доверия к цифровым сервисам. [4]

Исследование также выявило недостатки существующей системы информирования населения о финансовых рисках. Несмотря на регулярные предупреждения со стороны банков, многие пользователи продолжают игнорировать правила безопасности. Некоторые клиенты даже передают коды подтверждения посторонним лицам, считая, что общаются с сотрудником банка. Это свидетельствует о необходимости более активной профилактической работы. Возможно, проблема заключается не только в недостатке информации, но и в форме её подачи. Стандартные предупреждения часто воспринимаются формально. Между тем реальные примеры и социальные видеоролики воздействуют значительно эффективнее. В ряде стран банки регулярно проводят специальные кампании по финансовой безопасности, используя телевидение, социальные сети и образовательные платформы. В Узбекистане подобная практика также начинает развиваться. Некоторые банки уже публикуют видеоматериалы о мошеннических схемах и способах защиты данных. Однако охват аудитории пока остается недостаточным. Особенно это касается регионов, где уровень цифровой грамотности ниже, чем в крупных городах. [5]

Обсуждение. Полученные результаты показывают, что проблема мошенничества при безналичных расчетах имеет комплексный характер. Она затрагивает не только техническую сторону банковской деятельности, но и вопросы психологии, права и информационной безопасности. Нельзя утверждать, что увеличение количества мошеннических операций связано исключительно с недостатками банковской системы. Существенную роль играет человеческий фактор. Многие пользователи не воспринимают цифровые угрозы серьезно. Иногда люди уверены,

что мошенники могут обмануть кого угодно, кроме них самих. На практике ситуация оказывается противоположной. Преступники активно используют доверчивость, спешку и недостаток финансовой грамотности граждан. Особенно опасно то, что методы мошенничества становятся всё более персонализированными.

Преступники изучают информацию о клиентах через социальные сети, телефонные базы и открытые источники. Это позволяет им выстраивать убедительные сценарии общения. Банковская система вынуждена постоянно адаптироваться к новым угрозам. При этом развитие цифровых технологий одновременно создает и новые возможности, и новые риски. Полный отказ от дистанционных сервисов уже невозможен. Современная экономика требует быстроты и удобства финансовых операций. Поэтому основной задачей становится повышение уровня безопасности безналичных расчетов. [5]

Отдельного внимания заслуживает зарубежный опыт предупреждения финансового мошенничества. В ряде европейских стран активно используются системы многоуровневой идентификации клиентов, а также механизмы мгновенного реагирования на подозрительные переводы. Некоторые банки применяют временную задержку операций при выявлении нестандартной активности. В определенных случаях это позволяет предотвратить незаконное списание средств. В Узбекистане подобные механизмы пока внедрены не во всех банках. Кроме того, зарубежная практика показывает высокую эффективность совместной работы банков, правоохранительных органов и телекоммуникационных компаний. Без такого взаимодействия борьба с цифровым мошенничеством становится менее результативной. Интересно, что многие страны делают акцент именно на профилактике преступлений, а не только на расследовании уже совершенных случаев. Это вполне объяснимо. Возврат похищенных средств далеко не всегда возможен, особенно если деньги быстро переводятся через несколько счетов или выводятся за пределы страны. Предупреждение мошенничества оказывается значительно эффективнее последующего расследования.

Заключение. Проведенное исследование позволяет сделать вывод о том, что мошенничество при переводе безналичных расчетов стало одной из наиболее актуальных проблем современного банковского сектора. Развитие цифровых технологий и расширение дистанционных финансовых услуг существенно повысили удобство проведения платежей, однако одновременно создали новые возможности для киберпреступников. Наиболее распространенными формами мошенничества являются фишинг, социальная инженерия, поддельные банковские сайты и незаконный доступ к мобильным приложениям.

Исследование показало, что коммерческие банки Узбекистана постепенно усиливают меры защиты электронных платежей. Внедряются системы многофакторной аутентификации, автоматического мониторинга операций и биометрической идентификации клиентов. Вместе с этим сохраняются проблемы, связанные с недостаточной финансовой грамотностью населения и ограниченными возможностями отдельных банков в сфере кибербезопасности.

Особое значение приобретает профилактика финансового мошенничества. Повышение уровня информированности граждан, развитие культуры цифровой безопасности и совершенствование взаимодействия банков с государственными структурами способны существенно снизить количество мошеннических операций. В перспективе эффективность системы предупреждения преступлений в сфере безналичных расчетов будет во многом зависеть от скорости адаптации банковской системы к новым цифровым угрозам.

Список литературы

1. Шарипова Нигина Джоракуловна, Джураев Искандар. Совершенствование организационных механизмов трансформационных процессов в коммерческих банках // Ethiopian International Journal of Multidisciplinary Research. – 2024. – Т. 11. – № 04. – С. 66–68.

2. Sharipova Nigina Jorakulovna, Maksudov Orif Shakirovich. The Importance of Monetary Reforms // Ethiopian International Journal of Multidisciplinary Research. – 2023. – Vol. 10. – No. 12. – P. 880–883.
3. Шарипова Н.Д. Зарубежный опыт развития банковской системы. – Самарканд: Samarkand Institute of Economics and Service, 2023. – Zenodo.
4. Шарипова Н.Д., Акобиров А.П. Дальнейшее совершенствование предоставления дистанционных банковских услуг коммерческими банками // SCHOLAR. – 2023. – № 35. – С. 66–73.
5. Центральный банк Республики Узбекистан. Годовой отчет за 2024 год. – Ташкент, 2025.
6. Закон Республики Узбекистан «О платежах и платежных системах». – Ташкент, 2019.
7. Мирзиёев Ш.М. Стратегия развития Нового Узбекистана на 2022–2026 годы. – Ташкент: Узбекистон, 2022.
8. Лаврушин О.И. Банковское дело. – Москва: КНОРУС, 2021. – 448 с.
9. Mishkin F. The Economics of Money, Banking and Financial Markets. – London: Pearson Education, 2021. – 816 p.
10. Rose P.S. Commercial Bank Management. – New York: McGraw-Hill Education, 2020. – 742 p.