УДК 33 DOI: 10.14451/1.236.332

Мошенничество как проблема цифровизации финансового сектора (цифровые платежи)

© 2024 **Иконников Владислав Владимирович**
Студент Финансового факультета. Финансовый университет при Правительстве РФ.
E-mail: 226421@edu.fa.ru

© 2024 **Потапцева Александра Михайловна**
Студент Финансового факультета. Финансовый университет при Правительстве РФ.
E-mail: 226268@edu.fa.ru

© 2024 **Лялькова Евгения Евгеньевна**
Кандидат экономических наук, доцент, доцент Департамента бизнес-аналитики Факультета налогов, аудита и бизнес-анализа Заместитель заведующего кафедрой Современные технологии сбора и обработки отчетности (МШБ). Финансовый Университет при Правительстве РФ.
E-mail: eelyalkova@fa.ru

Ключевые слова: цифровизация, цифровой рубль, мошенничество в интернете, онлайн-платежи, фишинг, кибербезопасность, способы борьбы с мошенничеством в финансовом секторе.

Статья посвящена исследованию возможностей цифрового рубля в борьбе с теневыми и криминальными экономическими действиями. Рассматриваются свойства цифрового рубля, которые позволяют ему предотвращать и пресекать финансовые правонарушения. Также рассмотрены риски и возможные проблемы, связанные с его применением. Изучены способы борьбы и минимизации рисков в условиях цифровизации финансового сектора. Мошенничество в эпоху цифровизации становится все более распространенным явлением. С развитием интернет-технологий и электронных платежей, преступники находят новые способы обмана людей. Одной из основных форм мошенничества является фишинг — попытка получить конфиденциальную информацию, такую как пароли или номера кредитных карт, путем подделки электронных писем или веб-сайтов. Мошенничество в условиях цифровизации становится все более актуальной проблемой.

Кибербезопасность и мошенничество в интернете

Одной из ключевых целей цифровой трансформации финансовых институтов в России и других странах является повышение уровня качества обслуживания клиентов и оптимизация операционных процессов и ускорение финансовых операций. Использование цифровых технологий позволяет улучшить взаимодействие с клиентами, предоставляя им удобные и инновационные решения. Это способствует привлечению новых клиентов и удержанию существующих, что важно для конкурентоспособности финансовых институтов.

Кроме того, цифровая трансформация финансовых институтов способствует развитию эко-

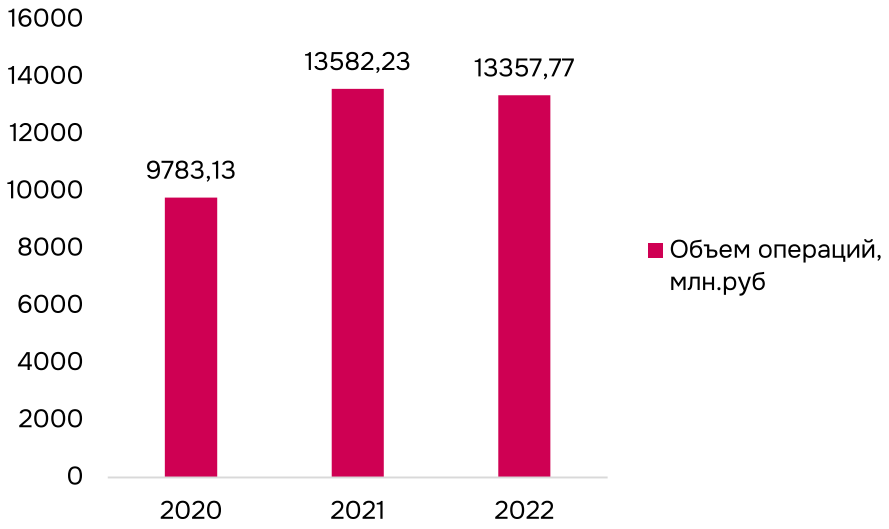

Рис. 1. Динамика операций без согласий клиента среди физических лиц.
Источник: Центральный банк РФ.

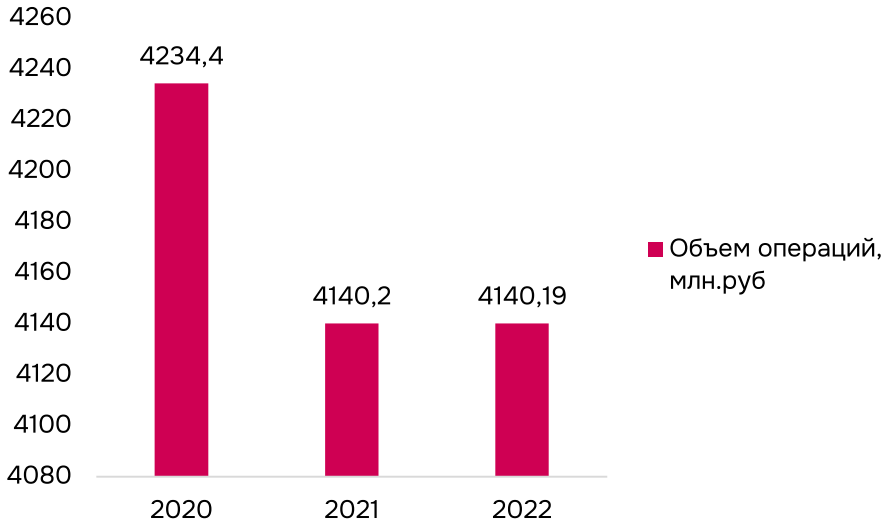

Рис. 2. Операции без согласия клиентов при оплате товаров и услуг в Интернете (CNP-транзакции).
Источник: Центральный банк РФ.

системы финансовых услуг, включая современные платежные системы, электронные кошельки, кредитные продукты и другие инновационные сервисы. Это способствует росту финансовой инклюзии и повышению доступности финансовых услуг для всех категорий населения.

Однако при внедрении цифровых технологий в финансовые институты необходимо учитывать возможные риски, связанные с кибербезопасностью, конфиденциальностью данных, а также соответствие законодательству в области финансовой деятельности. Важно развивать соответствующие механизмы защиты информации и обучать сотрудников финансовых институтов в области кибербезопасности.

Таким образом, цифровая трансформация финансовых институтов в России имеет большой потенциал для развития финансовой системы страны и повышения конкурентоспособности ее участников. Правильное внедрение и использование цифровых технологий позволит сделать финансовые услуги более доступными, удобными и безопасными для всех граждан и предприятий. Изучение процесса цифровой трансформации финансовых институтов в России представляет собой важную задачу, позволяющую рас-

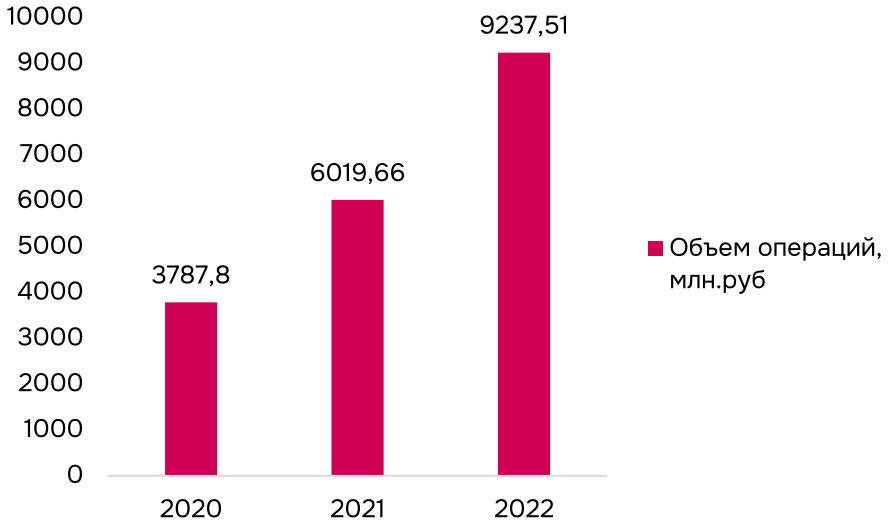

Рис. 3. Операции без согласия клиентов в дистанционном банковском обслуживании. Источник: Центральный банк РФ.

крыть потенциал для развития финансовой системы страны, выявить возможные риски и препятствия. Реализация Основных направлений 2022–2024 годов будет осуществляться Банком России во взаимодействии с государственными органами, участниками финансового рынка и иными организациями. По причине того, что сейчас цифровые технологии — это основной субъект развития не только экономической сферы, но и других основных сфер, мы подробно расскажем о случаях мошеннических деяний и их последствиях, основанных на статистике, а также способах противодействия.

В России и на мировой арене наблюдается активный процесс цифровизации различных секторов экономики, несмотря на происходящую деглобализацию и перестройку мировых рынков. Были выявлены основные факторы, причины и последствия мошеннических деяний на современный период цифровизации. Мошенничество в эпоху цифровизации и появления цифровых валют и платежей становится все более распространенным явлением. В данной статье рассматриваются причины возникновения этого явления и предлагаются способы борьбы с ним.

Одной из главных причин роста мошенничества является легкость доступа к персональным данным пользователей. С развитием технологий и увеличением числа онлайн-платежей, злоумышленники получают возможность использовать украденные данные для совершения финансовых преступлений.

Кроме того, многие пользователи не обладают достаточными знаниями о безопасности при использовании цифровых сервисов, что делает их уязвимыми перед атаками хакеров.

Для борьбы с мошенничеством необходимо принимать комплексные меры. Во-первых, компании должны усиливать защиту своих систем от взлома и кражи данных. Во-вторых, пользователям следует повышать свою осведомленность о безопасности при работе с онлайн-сервисами.

Также важно разрабатывать новые методы идентификации клиентов, такие как двухфакторная аутентификация или биометрические технологии. Это поможет предотвратить несанкционированный доступ к аккаунтам пользователей.

В целом, борьба с мошенничеством в эпоху цифровизации требует совместных усилий со стороны компаний и пользователей. Только так можно обеспечить безопасность и надежность цифровых платежей и сервисов.

Цифровизация финансовой системы Российской Федерации приносит не только позитивные

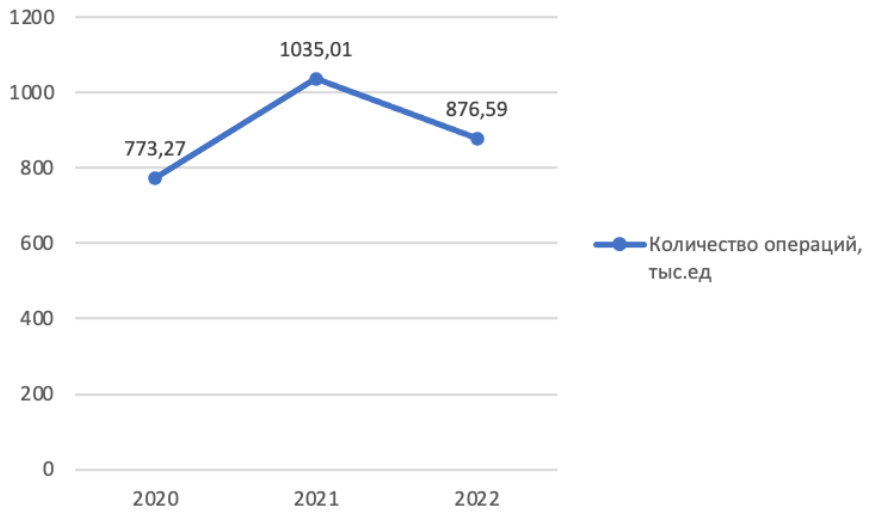

Рис. 4. Динамика совершения операций без согласия клиента.
Источник: составлено авторами на основе данных Центрального банка РФ.

результаты, но и имеет ряд негативных последствий. Это явление характерно для сложных экономических процессов. В процессе цифровизации возникают различные риски, которые необходимо своевременно идентифицировать и минимизировать.

Один из наиболее значимых социальных факторов, связанный с цифровизацией, но не связанный с мошенничеством — это увеличение числа безработных. Примером может служить сокращение рабочих мест в банковской сфере в результате внедрения цифровых технологий. Например, в октябре 2022 года Сбербанк закрыл более 500 своих отделений, что стало новым историческим рекордом.

Рассмотрим и проанализируем мошеннические схемы в условиях цифровизации.

По рисунку 1 можно увидеть, что по сравнению с 2020 годом, объем операций, проведенных без согласия физического лица, увеличился примерно на 28%.

Согласно рисунку 2, в сфере онлайн-оплаты товаров и услуг объем операций, проведенных без согласия клиентов, снизился на 3% по сравнению с 2020 годом.

На рисунке 3 изображена динамика совершения операций без согласия клиентов в дистанционном банковском обслуживании, и можно увидеть, как объем таких операций, начиная с 2020 года, равномерно увеличивается, примерно на 38% каждый год.

На рисунке 4 изображена динамика совершения операций без согласия клиента. Она заметно увеличилась в 2021 году по сравнению с 2020, но уже в 2022 году зафиксировано значительно меньшее количество таких операций.

Согласно рисунку 5, в сфере оплаты товаров и услуг в Интернете в 2021 году количество операций, совершенных без согласия клиента также значительно увеличилось, но к 2022 году снова уменьшилось и вернулось примерно к уровню 2020 года.

По рисунку 6 видно увеличение количества операций, совершенных без согласия клиента в дистанционном банковском обслуживании, которое происходит каждый год с 2020.

Таким образом, можно сделать вывод, что динамика совершения операций без согласия клиента положительна в сфере дистанционного банковского обслуживания, и объем таких операций также увеличивается. Это значит, что эта сфера наиболее подвержена атакам мошенников, и клиенты склонны попадаться на их уловки,

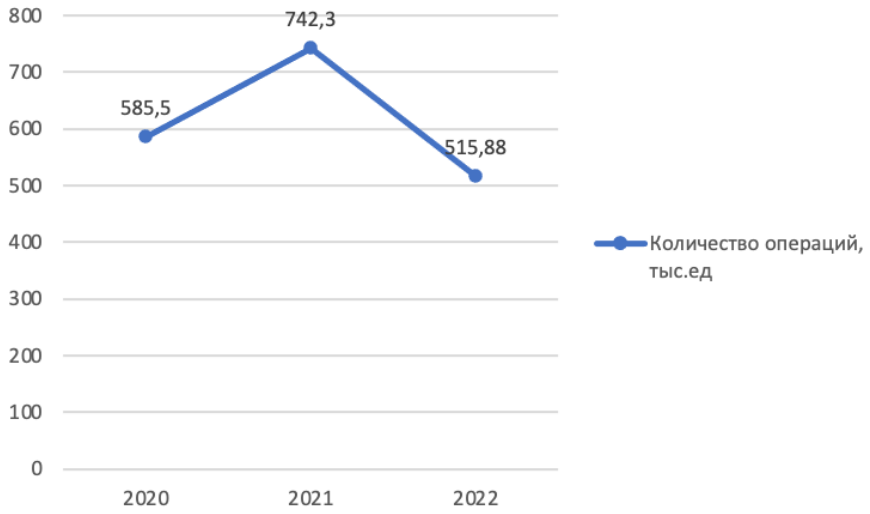

Рис. 5. Динамика совершения операций без согласия клиентов в сфере онлайн-оплаты товаров и услуг. Источник: составлено авторами на основе данных Центрального банка РФ.

поэтому увеличивается и количество самих операций, и их объем.

По данным ЦБ РФ, основным средством хищения денежных средств являются методы социальной инженерии, то есть методы манипулирования людьми с целью совершения ими каких-либо действий или получения какой-либо информации от этих людей. Этот способ упрощает получение информации или денежных средств мошенником, так как при сложности взлома систем или попыток мошенничества с помощью использования технологий, часто не удается получить нужную информацию или данные из-за защищенности информационных систем, поэтому мошенники прибегают к самому уязвимому звену — человеку. Если злоумышленник знает психологические уловки, то обмануть человека не является для него сложной задачей. Например, телефонные звонки, в которых мошенники представляются сотрудниками какого-либо банка или организации и пытаются с помощью обмана и шантажа получить доступ к данным о человеке (например, получить доступ к его банковской карточке).

Так как сотрудников в банках и других организациях много, клиенты верят таким звонкам, даже если они поступают не с официальных номеров банков или организаций. А поскольку социальные инженеры (мошенники, использующие методы социальной инженерии) способны запугать жертву, так как речь идет чаще всего об операциях с ее денежными средствами, нужные данные получаются достаточно быстро.

Таким образом, финансовое мошенничество в сфере дистанционного банковского обслуживания продолжает развиваться. Увеличилась также и средняя сумма одного хищения в 2022 году. В основном использовались методы социальной инженерии, из-за чего вырос и общий объем операций, совершенных без согласия клиента. Такую оценку приводит Банк России.

С помощью методов социальной инженерии можно украсть информацию или данные не только с целью их использования, но и с целью их уничтожения, что также является последствием мошенничества, которое тяжело потом устранить.

Существуют методы защиты от социальной инженерии, такие как обучение основам кибербезопасности (некоторые компании обучают сотрудников, также банки предупреждают своих клиентов и дают подробные инструкции, что делать, если клиент все же столкнулся с попыткой хищения его средств; предупреждения, которые можно увидеть параллельно с рекламой:

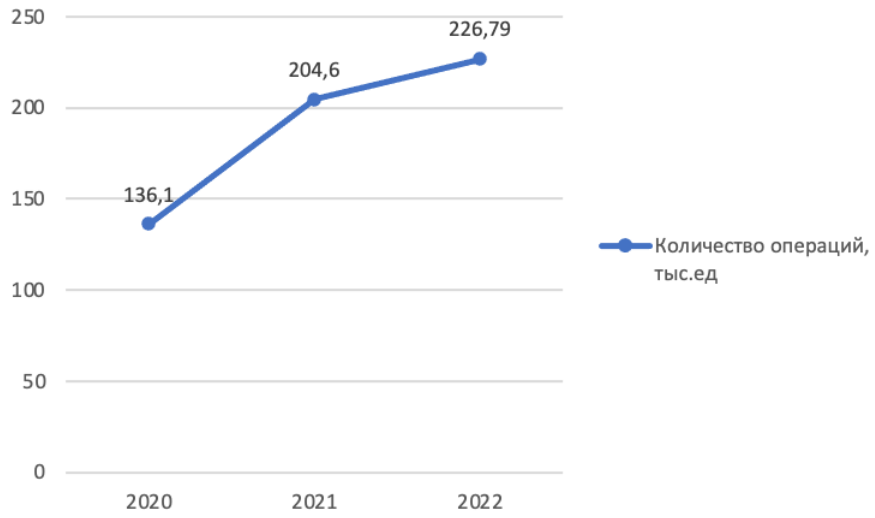

Рис. 6. Динамика совершения операций без согласия клиента в дистанционном банковском обслуживании.
Источник: составлено авторами на основе данных Центрального банка РФ.

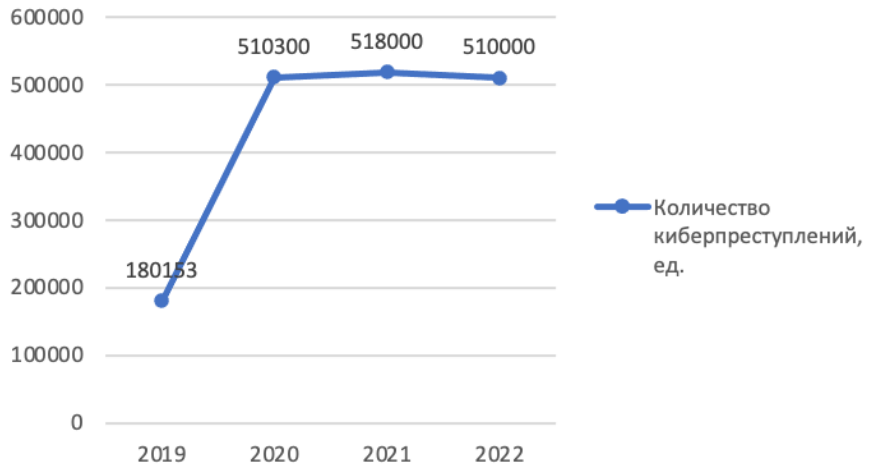

Рис. 7. Динамика киберпреступлений в России.
Источник: составлено авторами на основе данных Tadviser.

на баннерах, электронных носителях в метро, транспорте, торговых центрах и других местах массового посещения), использование средств технической защиты (использование антивирусных программ, антишпионского ПО, периодические тестирования сетей на проникновение), использование многофакторной аутентификации (дополнительные проверки личности клиента, в том числе с помощью SMS-сообщений и одноразовых кодов, биометрических данных). Также клиенты могут сами обеспечивать свою безопасность путем частой смены пароля, причем специалисты рекомендуют создавать сложные пароли, чтобы мошенникам было сложнее их угадать.

Также используется мониторинг поведения клиентов: с помощью определенных технологий анализируются операции с целью выявления подозрительных действий и вычисления злоумышленников. Сейчас для этого используется еще и искусственный интеллект.

Стоит отметить сотрудничество банков с правоохранительными органами, что также позволяет снизить риски финансового мошенничества и защитить банковскую систему от атак злоумышленников.

Рис. 8. Доля россиян, столкнувшихся с финансовым мошенничеством в 2023 году.
Источник: составлено авторами на основе данных из газеты «Известия».

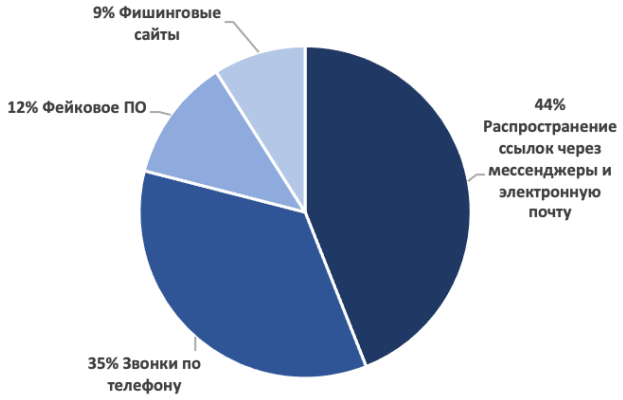

Рис. 9. Онлайн-мошенничество в 2023 году.
Источник: составлено авторами на основе данных Tadviser.

Искусственный интеллект сейчас активно используется, в том числе и для попыток мошенничества. Например, нейросеть умеет подделывать документы, в том числе и банковские чеки и выписки, и даже паспорта. Также сейчас активно развивается создание ссылок, при переходе по которым пользователи теряют свои данные о банковских картах или какую-либо персональную информацию. Телефонные звонки, которые мы упоминали ранее, иногда пишутся нейросетью или чат-ботами, и злоумышленники этим активно пользуются.

В 2017 году появилось такое понятие, как дипфейк, и сейчас оно получило еще большее распространение. Дипфейк означает подмену изображения человека или его голоса. Мошенники с его помощью подделывают голос клиента банка и оформляют на него кредит, так как сейчас активно развивается биометрия, и стало возможным оформить кредит по звонку. Таким образом, клиент банка может неожиданно для себя оказаться в должниках.

По словам Дмитрия Миклухо, старшего вице-президента — директора департамента информационной безопасности ПСБ, «принципиальной разницы в том, общаетесь ли вы с реальным злоумышленником или роботом, нет. Правила безопасности не зависят от применяемых мошенниками схем — с привлечением чат-бота или без него».

По рисунку 7 видно динамику совершения киберпреступлений в России. В 2020 году, по сравнению с 2019, количество киберпреступлений значительно выросло, примерно на 65%. С 2020 года оно остается примерно на одном уровне.

По словам Генпрокуратуры, граждане чаще стали пользоваться интернет-ресурсами и дистан-

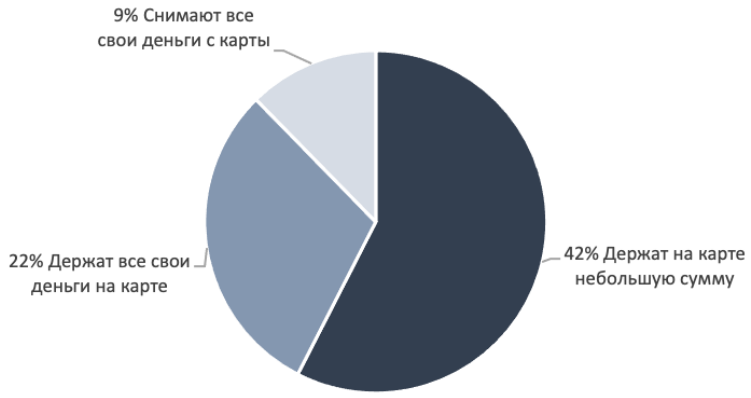

Рис. 10. Хранение россиянами денежных средств на карте.
Источник: составлено авторами на основе данных Tadviser.

ционными услугами, например, для оплаты товаров и услуг, осуществления банковских операций. Также чаще стали использоваться электронные платежи и цифровые валюты, и именно поэтому мошенничество учащается в цифровой среде.

Согласно рисунку 8, 33% россиян не сталкивались с финансовым мошенничеством в 2023 году, 67 — столкнулись. Это не означает, что все 67% стали жертвами мошенников. Они могли получать звонки с подозрительных номеров, видеть подозрительные ссылки и так далее.

После введения санкций против российских банков, многие их приложения были удалены, и их мошеннические подделки стали распространяться по разным каналам. Так, согласно рисунку 9, 44% составило распространение ссылок через мессенджеры и электронную почту, 35% составили звонки по телефону, 12% — создание фейковых ПО и 9% — создание фишинговых сайтов. Другими словами, злоумышленники, используя все те же методы социальной инженерии, убеждают клиентов банков через телефонные звонки, рассылки, сайты скачать фейковое приложение банка. Такие приложения обычно очень схожи с оригинальными, так как берется оригинальный дизайн, изображение карточек также очень похоже на настоящее.

Что касается доверия граждан банкам и их осторожности в хранении денег на картах, по рисунку 10 видно, что 42% стараются держать на карте небольшую сумму, 22% хранят все свои деньги на картах, но устанавливают суточные, недельные и месячные лимиты на переводы и проведение транзакций, для того чтобы у мошенников не было доступа к крупным суммам, 9% снимают все свои деньги с карт.

Самым оптимальным является использование лимитов или хранение небольших сумм на картах, так как при наличии лимита злоумышленник не сможет снять больше установленной пользователем суммы, а при хранении небольшой суммы на карте у него и не будет доступа к большей сумме и информации о ней.

С введением цифрового рубля может появиться новый способ мошенничества: подделка цифрового рубля. Чтобы создать фальшивый цифровой рубль, злоумышленники могут использовать известные способы: нейросеть и искусственный интеллект, и другие новые информационные технологии. Следовательно, важно создать условия и способы проверки подлинности цифровых рублей с целью уменьшения рисков мошенничества.

Что касается кибербезопасности, цифровой рубль и цифровые платежные системы могут стать объектами еще большего количества атак хакеров. Скорее всего, потребуется достаточно большое количество времени для адаптации систем и создания стабильно работающего механизма защиты цифровых рублей, платежных систем и финансовых средств граждан, которые

хранятся в безналичной форме в целом.

Заключение

В наши дни увеличивается количество атак мошенников за счет увеличения количества способов, которые можно для этого использовать. Искусственный интеллект и социальная инженерия объединяются и позволяют мошенникам быстро получать нужную информацию от клиентов банков и использовать или уничтожать ее. Цифровой рубль также может стать объектом атак хакеров, что требует еще большей осторожности граждан и организаций и еще большей защищенности финансовой системы. В связи с мошенничеством и его негативными факторами были выявлены следующие последствия:

- анонимность цифровых валют и платежей;
- рост онлайн-транзакций и электронной коммерции;
- недостаточная техническая грамотность и осведомленность о мерах безопасности;
- прогрессивность методов мошенников, использующих социальную инженерию и фишинг.

Также были выявлены такие способы борьбы с мошенничеством, как:

- усиление мер безопасности, таких как двухфакторная аутентификация и шифрование;
- повышение технической грамотности и осведомленности о мерах защиты от мошенничества;
- внедрение новых технологий для выявления и предотвращения мошенничества, таких как искусственный интеллект и машинное обучение;
- сотрудничество между правоохранительными органами, банками и технологическими компаниями для борьбы с мошеннической деятельностью;
- правовое регулирование цифровых валют и платежей для защиты прав потребителей и предотвращения отмывания денег.

Библиографический список

1. *Баранова И. В.*, *Гапон М. Н.*, *Голова Е. Е.* Цифровизация финансовых услуг как направление инновационного развития России // Вопросы инновационной экономики. — 2022. — Т. 12, № 4. — С. 2583—2598. — URL: https://elibrary.ru/item.asp?id=50211453.
2. *Беляева Е. С.*, *Костюк Н. М.* Тенденции развития цифровой экономики Российской Федерации // Стратегия формирования экосистемы цифровой экономики : Сборник материалов II Международной научно-практической конференции, Курск, 20 марта 2020 года. — Курск : Юго-Западный государственный университет, 2020. — С. 15—20. — URL: https://www.elibrary.ru/download/elibrary_43136124_14885842.pdf.
3. *Ваганова О. В.*, *Коньшина Л. А.* Развитие рынка финансовых технологий: зарубежный опыт и отечественная практика // Научный результат. Серия: Экономические исследования. — 2021. — Т. 7, № 1. — С. 80—88. — DOI: 10.18413/2409-1634-2021-7-1-0-9.
4. *Городнова Н. В.* Анализ специфики и перспектив применения цифровой валюты центральных банков // Вопросы инновационной экономики. — 2023. — Т. 13, № 3. — С. 1573—1590. — DOI: 10.18334/vinec.13.3.117168.
5. ИТ-услуги лидируют в расходах финансовых компаний. — 2023. — URL: https://banks.cnews.ru/reviews/tsifrovizatsiya_finansovogo_sektora/articles/importozameshchenie_i_vnedrenie_ii?ysclid=ltzh38akmg759787575.
6. *Кривошея Е.* Эксперты назвали главные риски внедрения цифрового рубля в России. — URL: https://www.skolkovo.ru/expert-opinions/eksperty-nazvali-glavnye-riski-vnedreniya-cifrovogo-rublya-v-rossii.
7. *Крицкая Е. В.*, *Коновалова Т. А.* Цифровое мошенничество: современные тенденции, способы защиты и превенции // Молодой ученый. — 2020. — 50 (340). — С. 258—263. — URL: https://moluch.ru/archive/340/76549.
8. *Криштаносов В. Б.* Цифровизация финансового сектора экономики: проблемы и перспективы. // Труды БГТУ. Сер. 5, Экономика и управление. — 2021. — 1 (224). — С. 17—24. — URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-finansovogo-sektora-ekonomiki-problemy-i-perspektivy?ysclid=ltzh41qwlw737148886.
9. *Лапшин И. С.* Цифровой рубль как инструмент противодействия теневой и криминальной экономической деятельности в России // Теория и практика общественного развития. — 2023. — 5 (181). — URL: https://cyberleninka.ru/article/n/tsifrovoy-rubl-kak-instrument-protivodeystviya-tenevoy-i-kriminalnoy-ekonomicheskoy-deyatelnosti-v-rossii.

10. Обзор операций, совершенных без согласия клиентов финансовых организаций / Центральный Банк Российской Федерации. — URL: https://www.cbr.ru/analytics/ib/operations_survey/2023.
11. Отчет Центрального банка. Цифровой рубль / Центральный Банк Российской Федерации. — URL: https://www.cbr.ru/StaticHtml/File/112957/Consultation_Paper_201013.pdf.
12. *Петрова Л. А.*, *Кузнецова Т. Е.* Цифровизация банковской системы: цифровая трансформация среды и бизнес-процессов // Финансовый журнал. — 2020. — Т. 12, № 3. — 91-101. https://cyberleninka.ru/article/n/tsifrovizatsiya-bankovskoy-sistemy-tsifrovaya-transformatsiya-sredy-i-biznes—protsessov/viewer.
13. Проект основных направлений цифровизации финансового рынка на период 2022–2024 годов / Центральный Банк Российской Федерации. — URL: https://cbr.ru/Content/Document/File/131360/oncfr_2022-2024.pdf.