УДК 336.1

Е. К. Воронкова

ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова», Москва, e-mail: Voronkova.EK@rea.ru

М. А. Валишвили

ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова», Москва, e-mail: Valishvili.MA@rea.ru

РИСКИ ФИНАНСОВОГО ДОВЕРИЯ: АТРИБУТЫ ФИНАНСОВОГО МОШЕННИЧЕСТВА И ЛИЧНОЙ ФИНАНСОВОЙ БЕЗОПАСНОСТИ

Ключевые слова: финансовое мошенничество, риски, дипфейк технологии, личная финансовая безопасность, Банк России.

Во всем мире наблюдается рост количества и модификация форм финансовых посягательств в сфере персональных финансов. Финансовое мошенничество является угрозой финансовому благополучию граждан. Цель исследования – сформировать системное представление о рисках финансового мошенничества в сфере персональных финансов, обосновать актуальность противодействия финансовым преступлениям против граждан, раскрыть основные механизмы выявления и преодоления несанкционированной деятельности в финансовой сфере, используемые государственными и негосударственными структурами. В процессе работы использованы аналитические, логические, эмпирические методы исследования. Для выявления российской специфики финансовых махинаций авторы обращались к национальным нормативным актам, документам и базам данных Банка России, российских системно значимых банков, Аналитического центра НАФИ, некоторых других отечественных и зарубежных институтов. В статье рассмотрены вопросы финансового мошенничества, направленного на хищение личных финансовых средств, представлен анализ масштабов банковских операций без согласия клиентов, объемов хищения денежных средств граждан, способов совершения финансовых махинаций, ключевой инструментарий, используемый финансовыми институтами для снижения рисков финансового мошенничества, сформулированы правила личной финансовой безопасности, определены некоторые направления преодоления угроз финансового мошенничества.

E. K. Voronkova

Plekhanov Russian Economic University, Москва, e-mail: Voronkova.EK@rea.ru

M. A. Valishvili

Plekhanov Russian Economic University, Москва, e-mail: Valishvili.MA@rea.ru

RISKS OF FINANCIAL TRUST: ATTRIBUTES OF FINANCIAL FRAUD AND PERSONAL FINANCIAL SECURITY

Keywords: financial fraud, risks, personal finance, deepfake technology, personal financial security, Bank of Russia.

The number and modification of forms of financial attacks in the sphere of personal finances are growing all over the world. Financial fraud is a threat to the financial well-being of citizens. The purpose of the study is to form a systemic understanding of the risks of financial fraud in the sphere of personal finances, to substantiate the relevance of counteracting financial crimes against citizens, to reveal the main mechanisms for identifying and overcoming unauthorized activities in the financial sphere used by state and non-state structures. In the course of the work, analytical, logical, empirical research methods were used. To identify the Russian specifics of financial fraud, the authors referred to national regulations, documents and databases of the Bank of Russia, Russian systemically important banks, the NAFI Analytical Center, and some other domestic and foreign institutions. The article examines the issues of financial fraud aimed at theft of personal financial resources, presents an analysis of the scale of banking operations without the consent of clients, the volume of theft of citizens' funds, methods of committing financial fraud, the key tools used by financial institutions to reduce the risks of financial fraud, formulates the rules of personal financial security, and identifies some areas for overcoming the threats of financial fraud.

Введение

Распространение финтехсервисов становится причиной возрастания уязвимости личных финансов к мошенническим действиям. Финансовое мошенничество наносит большой ущерб национальной экономике, оказывая негативное влияние на поведение рыночных субъектов, сдерживает развитие предпринимательской деятельности, инвестиционных процессов. Финансовые преступления являются источниками операционных рисков банков и ведут к прямым финансовым потерям финансовых организаций, ухудшают их деловую репутацию. По мнению авторов, выявление и анализ причин, последствий, признаков нацеленного на граждан хищения финансовых средств, формулировка предложений по управлению рисками финансового мошенничества в сфере персональных финансов являются актуальными направлениями исследований не только с точки зрения повышения финансовой грамотности, как непременного условия защищенности населения от финансовых мошенников, но и в аспекте формирования государственных, корпоративных и личных стратегий финансовой безопасности.

Научно-практическая значимость настоящей работы заключается в комплексном рассмотрении проблемы финансового мошенничества с целью учета изложенных положений при совершенствовании системы управления рисками финансового мошенничества.

В ходе исследования был сделан акцент на рассмотрении трендов финансового мошенничества и противодействия ему именно в сегменте личных финансов.

Цель исследования – сформировать системное представление о рисках финансового мошенничества в сфере персональных финансов, обосновать актуальность противодействия финансовым преступлениям против граждан, раскрыть основные механизмы выявления и преодоления несанкционированной деятельности в финансовой сфере, используемые государственными и негосударственными структурами.

Материалы и методы исследования

При проведении исследования использовался метод контент-анализа научных отечественных и зарубежных разработок, материалов официальных сайтов финансовых учреждений, в которых представлена современная терминологическая база в соответствующем аспекте, рассматриваются факторы распространения финансового мошенничества и его влияние на общество, отмечается важность понимания особенностей мошенничества в финансовой сфере, обосновывается необходимость постоянного совершенствования инструментов и методов предупреждения финансового мошенничества. Концептуально отечественные и зарубежные исследователи единодушны в том, что финансовое мошенничество является значительной проблемой, которая требует создания целостной стратегии противодействия, непрерывного изучения мошеннических схем и потенциала новых технологий.

Результаты исследования и их обсуждение

Мошеннические схемы с денежными средствами граждан распространяются с каждым годом. Существует множество видов финансового мошенничества, основа которых – психологическое воздействие на человека. Используя методы социальной инженерии, преступники вводят граждан в заблуждение, похищают деньги или персональные данные жертвы, позволяющие им проводить несанкционированные финансовые операции. Проблема финансового мошенничества имеет международный характер и затронула все государства мира независимо от уровня развития. В США ущерб от мошенничества в 2023 году вырос на 14% по сравнению с предыдущим годом и составил более 10 млрд долл., из которых почти 2,7 млрд долл. пришлись на утечку персональных данных. Потери от мошенничеств с платежами в ЕС в 2022 году составили 4,3 млрд евро, а за полгода 2023 года – 2 млрд евро [1].

В России ответственность за мошеннические действия установлена Уголовным кодексом РФ. И, хотя термина «финансовое мошенничество» уголовное законодательство не содержит, оно подпадает под статью 159 УК РФ, которая определяет его как «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием» и предусматривает наказание за мошенничество в виде штрафа, обязательных и исправительных работ, ареста или лишения свободы на срок до десяти лет в зависимости от тяжести и последствий преступления [2].

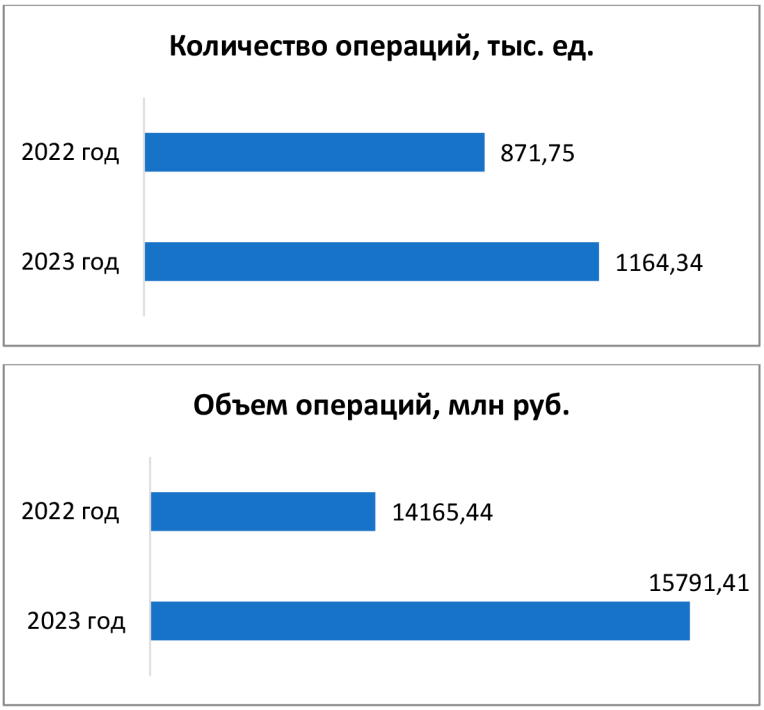

Рис. 1. Динамика количества и объема операций по хищению финансовых средств и граждан Российской Федерации [4]

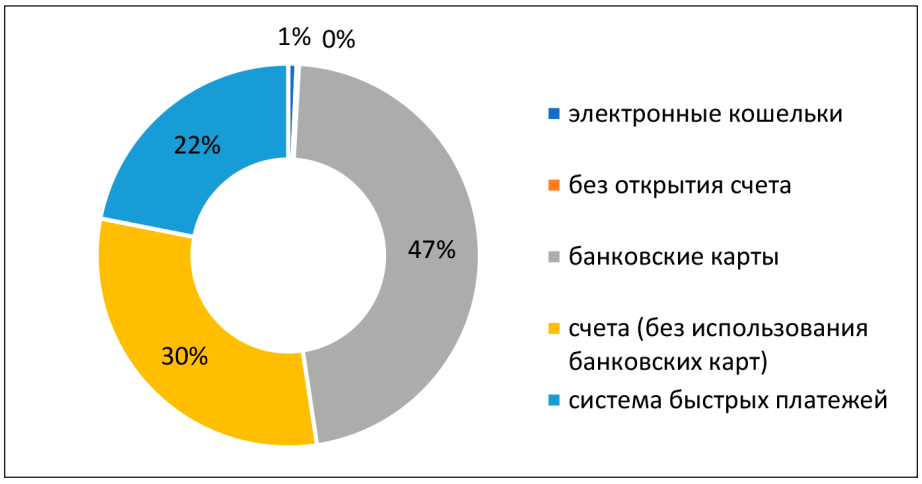

Рис. 2. Структура объема хищений денежных средств у населения России по видам платежных инструментов в 2023 году [4]

Кроме того, по этой статье суд может применить дополнительные меры воздействия, такие как конфискация имущества, запрет на занимание определенных должностей или занятие определенной деятельностью.

Министерство финансов РФ под финансовым мошенничеством понимает «совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения».

Ежегодно с банковских счетов россиян мошенники крадут до 16 млрд руб. При этом вернуть получается менее 15% от украденного. С 2019 года по 2023 год объем банковских операций без согласия клиентов вырос почти втрое. Только в 2023 году по отношению к россиянам совершен 1 164 340 финансовых преступлений мошеннического характера, что в стоимостном выражении составило 15,3 млрд руб. (рис. 1) [3,4].

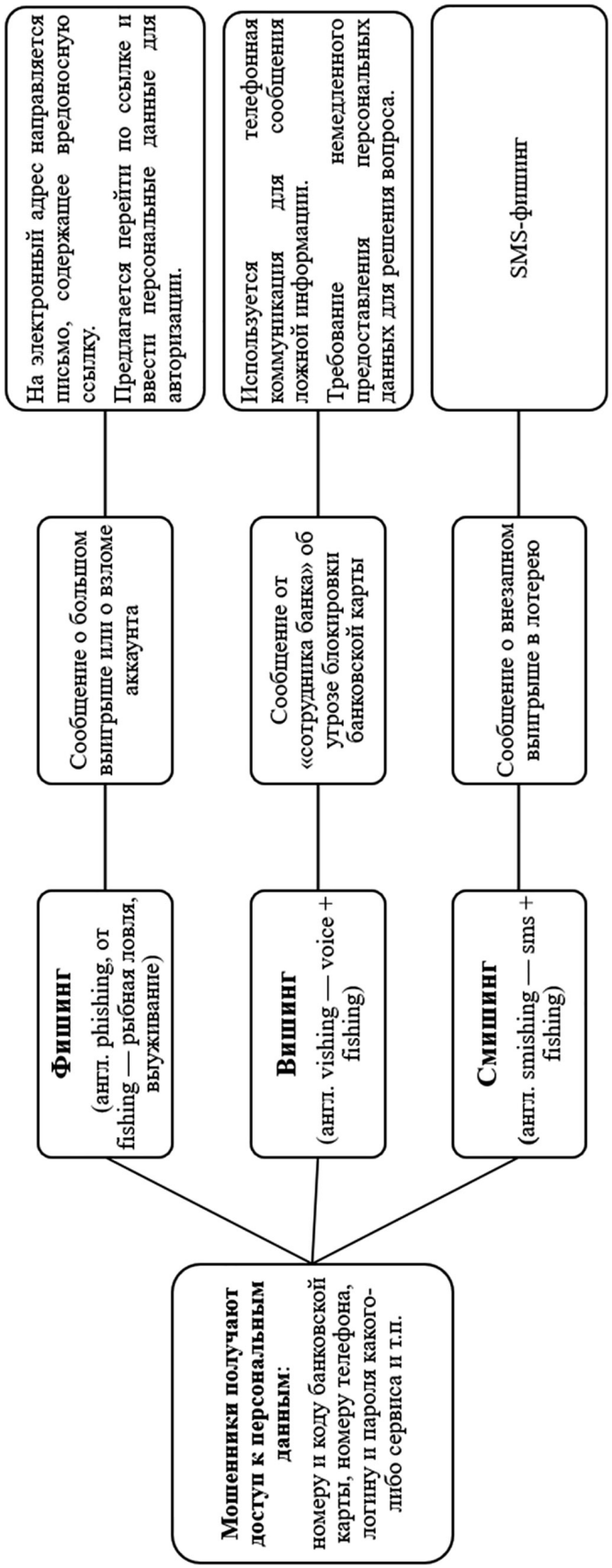

Рис. 3. Виды финансового мошенничества

В виду массовости и доступности сильно подвержен операционному риску рынок банковских карт. Поэтому вполне логично, что самыми значительными являются мошеннические операции с использованием банковских карт (46,7% от общего объема хищений) – почти 985 000 операций на сумму больше 7 млрд руб. по итогам 2023 года (рис. 2) [4].

Финансовые мошенники, осуществляя свою незаконную деятельность, могут представляться сотрудниками банка, правоохранительных органов, социальных служб, операторами мобильной связи. Под разными предлогами они пытаются получить доступ к чужим финансовым ресурсам или персональным данным жертвы. Наиболее «популярны» среди мошенников такие способы воздействия на человеческие эмоции, как фишинг, вишинг, смишинг (рис. 3).

Анализ современных технологий хищения денежных средств граждан позволил сформулировать характерные черты финансового мошенничества. Мошенники используют актуальные общественные тренды, действуют максимально настойчиво, требуют быстрого принятия решений, запрашивают персональные данные потенциальной жертвы по телефону или иными удаленными способами, обещают существенную выгоду. Телефонные звонки всегда поступают с незнакомых и подменных номеров.

В целом финансовое мошенничество в зависимости от схемы воздействия на личность можно классифицировать следующим образом: прямое выманивание денег, шантаж или банковское мошенничество.

Мошенники активно используют новации в финансовой сфере. Примером может быть проводимая Банком России модернизация банкнот номиналом 100 руб. и 5000 руб. Используя низкую осведомленность граждан о том, что в действительности приложение «Банкноты Банка России» не позволяет отличать подлинные банкноты от фальшивых, злоумышленники развернули компанию по «проверке подлинности» наличных денег, в том числе новых купюр, через якобы «официальное приложение Банка России». Гражданину направляется ссылка на поддельное приложение, лишь визуально похожее на официальное. А после скачивания жертвой приложения мошенники ее телефон и счета становятся доступными для мошенников, и они получают возможность похитить с них деньги.

Факты финансового мошенничества связаны и с появлением цифрового рубля. Цифровой рубль пока проходит тестовый этап, планов по замене наличных и безналичных денег новой формой валюты пока нет, а все сведения о новой цифровой форме российской валюты размещаются только на официальных ресурсах регуляторов или российских банков. Игнорируя это, и невзирая на то, что по российскому законодательству, граждане имеют право самостоятельно принимать решение, в какой форме им удобно получать государственные пособия и выплаты, на фоне проведения Банком России мероприятий по популяризации новой цифровой валюты, преступники рассылают населению сообщения об обязательном переводе пенсионных и социальных выплат в цифровые рубли с фишинговыми ссылками.

Отдельное направление финансового мошенничества состоит в применении искусственного интеллекта (ИИ). Использование мошенниками ИИ, крупных языковых моделей и криптовалют в сочетании с бизнес-моделями фишинга и программ-вымогателей привело к усложнению мошеннических схем.

В России злоумышленники для хищения денег стали чаще использовать такой тип ИИ, как дипфейк-технологии (deepfake). Дипфейк – это метод создания поддельного медиаконтента (аудио, изображения или видео), с помощью алгоритмов глубокого обучения. Финансовые мошенники с помощью нейросети генерируют образ человека и рассылают его друзьям или родным через мессенджеры или социальные сети. В некоторых случаях мошенники создают дипфейки работодателей, сотрудников государственных органов, известных личностей из той сферы деятельности, в которой трудится их потенциальная жертва. В коротком фальшивом видеоролике виртуальный герой, голос которого иногда сложно отличить от голоса прототипа, рассказывает якобы о своей проблеме (болезнь, ДТП, увольнение) и просит перевести деньги на указанный счет.

Банком России сформирована система противодействия финансовому мошенничеству, создана база данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, доступ к которой имеют операторы по переводу денежных средств, услуг платежной инфраструктуры, платежных систем. Регулятор координирует деятельность по блокировке

несанкционированных переводов денежных средств в своей платежной системе, останавливает работу фишинговых ресурсов и ресурсов, распространяющих вредоносное программное обеспечение, телефонных номеров и SMS-рассылок, используемых в мошеннических целях, повышает финансовую грамотность населения.

Основой для первых позитивных изменений в борьбе с финансовым мошенничеством стали принятые в 2014 году новеллы в российском законодательстве о национальной платежной системе, которые заставили банки активнее вести мониторинг эффективности защиты от неправомерного доступа к сетям и информационным массивам, обновлять методы и средства информационной безопасности.

В 2018 г. для упрощения, повышения оперативности и защищенности процесса информационного обмена Банком России была создана автоматизированная система обработки инцидентов – АСОИ Финцерт – Центр взаимодействия и реагирования Департамента информационной безопасности, специальное структурное подразделение Банка России (CERT – computer emergency response team, группа реагирования на компьютерные инциденты). Деятельность АСОИ Финцерт препятствует распространению угроз в финансовой сфере, способствует минимизации потерь финансовых организаций и их клиентов от рисков финансового мошенничества. Участники информационного обмена обращаются в АСОИ Финцерт в случае выявленных ими опасностей и совершенных на них атак для получения рекомендаций по противодействию этим рискам [5].

С целью минимизации рисков финансового мошенничества Банк России постоянно развивает законодательство, расширяет перечень признаков финансового мошенничества. Среди последних наиболее заметных изменений, направленных на повышение защиты людей от действий злоумышленников, – Закон о новых мерах банков по борьбе с мошенническими переводами, введенный 25 июля 2024 года. Согласно этому акту, коммерческие банки обязаны оперативно приостанавливать переводы при наличии информации о случаях и попытках мошеннических операций получателем денег, предупреждать клиентов о том, что платеж может быть предназначен злоумышленникам, отключать доступ к дистанционному обслуживанию клиентам, занимающимся выводом и обналичиванием похищенных денег. В этом же документе уточнено определение операции без добровольного согласия клиента, как денежного перевода, совершенного человеком вследствие обмана или злоупотребления доверием [6].

Разработкой мер по снижению рисков финансовых мошеннических операций для своих клиентов занимаются и коммерческие банки. Они осуществляют мониторинг, размещают памятки о безопасном использовании карт, внедряют технологии, ограничивающие возможности мошенников перехватить номер платежной карты и списать средства в свою пользу и т.п.

В 2020 году в российской банковской практике появились уникальные технологические антифрод-решения на базе технологий машинного обучения и ИИ, разработанные совместно с партнерами – крупнейшими операторами мобильной связи, совместимые с внутренними системами безопасности финансовых организаций. Пионерами указанных инноваций стали АО «Тинькофф» и СберПАО «Сбербанк России». К настоящему времени в соответствии с рекомендациями регулятора достигнуть необходимого уровня аутентификации и верификации пользователей и частных платежей практически все российские банки имеют специализированное программное обеспечение для борьбы с рисками финансового мошенничества. Характерно, что многие финансовые организации для повышения уровня информационной и финансовой безопасности создают собственные системы противодействия мошенничеству.

Успехи в борьбе с фродстерами весьма заметны. В 3 кв. 2024 года было предотвращено хищений на 4,9 млн руб., что втрое больше, чем за аналогичный период прошлого года. Более, чем на две трети сократилось число выявленных телефонных номеров, задействованных финансовыми мошенниками, снижается количество компьютерных атак (рис. 4) [7].

Основные каноны по снижению рисков личного финансового мошенничества с использованием искусственного интеллекта заключаются в необходимости обеспечить защиту аккаунтов и социальных сетей, используя настройки приватности, по возможности с подключением двухфакторной идентификации, спам-защиту от нежелательных звонков и т.п.

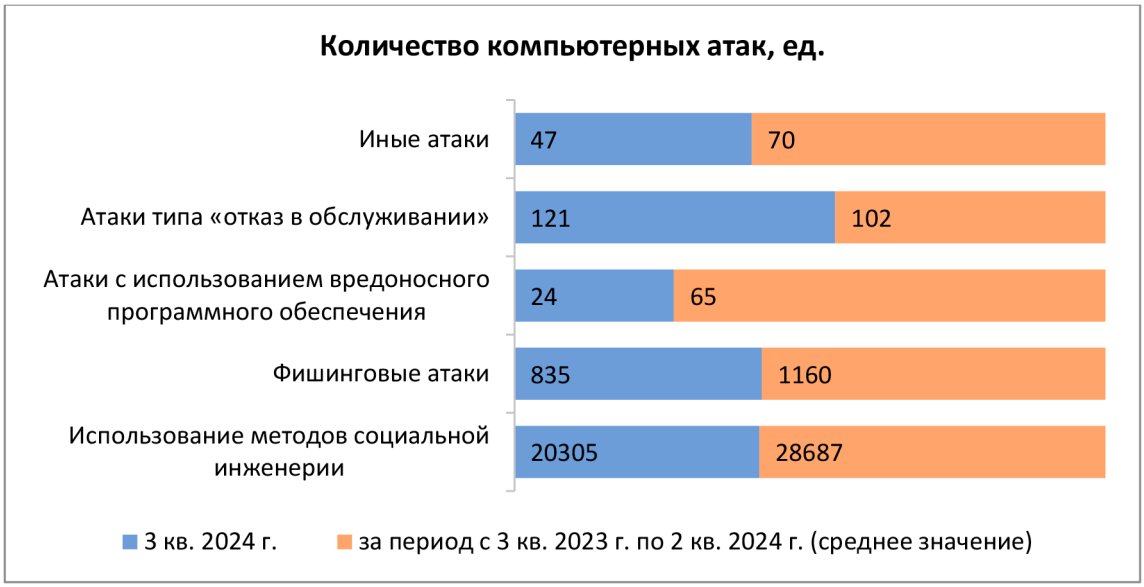

Рис. 4. Динамика изменения компьютерных атак в финансовой сфере [7]

Эффективность решения задачи снижения рисков финансового мошенничества критически зависит от уровня финансового образования и просвещения. Система безопасности в состоянии помочь только тому человеку, который осознанно следует правилам личной финансовой безопасности: не совершает операций с банковской картой или с банковским счетом под диктовку незнакомцев по телефону или посредством иных видов связи, не принимает скоропалительных финансовых решений, избавляется от ссылок в письмах или сообщениях с неизвестных адресов, проверяет подлинность и защищенность сайтов при оплате или переводах, не передает платежные данные, пароли и коды подтверждений третьим лицам. В связи с этим исключительную важность приобретает деятельность по реализации Стратегии повышения финансовой грамотности и формирования финансовой культуры до 2030 года [8].

Заключение

Выполненное исследование наглядно показывает, что глобальное распространение информационных технологий и сети Интернет, цифровизация финансовых инструментов повышают уязвимость финансовых систем к мошенническим посягательствам.

Несмотря на то, что развиваются системы управления рисками финансового мошенничества сохраняют актуальность постоянный мониторинг трансформаций мошеннических схем и активности мошенников (числа несанкционированных операций, понесенного ущерба и др.).

Требуется активно продолжать разработки новых скриптов для общения с клиентами. Показатели мошенничества по банковским картам при строгой аутентификации клиентов относительно более низкие.

В современных условиях должна усиливаться роль государства, регулятора и финансовых организаций, как основных проводников устоев финансового просвещения граждан. При этом новейшие технологии следует рассматривать не только, как факторы риска роста финансового мошенничества, но и как возможности борьбы с этой опасностью.

Библиографический список

1. Анатомия аферы: финансовое мошенничество всё больше приобретает трансграничный характер // Национальный банковский журнал. 2024. Июль-август. [Электронный ресурс]. URL: https://nbj.ru/publs/anatomiya_afery_finansovoe_moshennichestvo/66708/ (дата обращения: 25.10.2024).

2. «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ (ред. от 30.11.2024). Ст. 159. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/8012ecdf64b7c9cfd62e90d7f55f9b5b7b72b755/ (дата обращения: 25.10.2024).

3. Официальный сайт Банка России. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год. 13 февраля 2024 года. [Электронный ресурс]. URL: https://www.cbr.ru/Collection/Collection/File/32189/Review_of_transactions_2019.pdf (дата обращения: 25.10.2024).

4. Официальный сайт Банка России. Обзор операций, совершенных без согласия клиентов финансовых организаций. [Электронный ресурс]. URL: https://cbr.ru/analytics/ib/operations_survey/2023/ (дата обращения: 25.10.2024).

5. Официальный сайт Банка России. Информационная безопасность. ФинЦЕРТ. [Электронный ресурс]. URL: https://www.cbr.ru/information_security/fincert/ (дата обращения: 25.10.2024).

6. Официальный сайт Банка России. Граждан защитят по-новому от мошеннических переводов. [Электронный ресурс]. URL: https://www.cbr.ru/press/event/?id=18865 (дата обращения: 25.10.2024).

7. Официальный сайт Банка России. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. [Электронный ресурс]. URL: https://cbr.ru/press/event/?id=23217 (дата обращения: 25.10.2024).

8. Стратегия повышения финансовой грамотности и формирования финансовой культуры до 2030 года. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_460597/ (дата обращения: 25.10.2024).