

Исаева Екатерина Вячеславовна, студентка,
ФГАУ ВО СГЭУ, г. Самара

Бокарева Ксения Михайловна, студентка,
ФГАУ ВО СГЭУ, г. Самара

МОШЕННИЧЕСТВО В БАНКОВСКОМ СЕКТОРЕ: ВИДЫ И СПОСОБЫ БОРЬБЫ С НИМ

Аннотация: В статье рассматривается проблема мошенничества в банковском секторе, анализируются виды и способы борьбы с этим явлением. Особое внимание уделено статистике Центрального Банка за 2023 и первые 3 квартала 2024 года, которая демонстрирует значительный рост числа мошеннических операций

Ключевые слова: мошенничество, банковский сектор, способы борьбы с мошенничеством

Несмотря на активную борьбу российских банков с неправомерными финансовыми действиями в наше время мошенничество в банковском секторе остается значительной проблемой.

Мошенничество – это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием [1].

В современной России мошенники развиваются с той же скоростью, что и методы борьбы с ними. Актуальность данного явления подтверждена ниже с опорой на официальную статистику Центрального банка РФ (данные приведены в таблице 1).

Таблица 1

Обзор отчетности об инцидентах информационной безопасности
при переводе денежных средств Банка России (2023 и 2024 гг.)

Период	1 квартал 2023	2 квартал 2023	3 квартал 2023	2023	1 квартал 2024	2 квартал 2024	3 квартал 2024
Количество операций без согласия клиентов	252 111	279 706	288 784	1 165 990	294 414	256 936	348 593
Объем операций без согласия клиентов (тыс. руб.)	4 549 282,42	3 622 543,21	3 591 091,15	15 791 410,00	4 263 315,94	4 775 114,61	9 309 050,71

По данным Центрального банка РФ [2] в третьем квартале 2024 года российскими банками было зафиксировано 348,6 тысяч операций на общую сумму 9,3 миллиарда рублей, совершенных без согласия физических и юридических лиц, что по сравнению с третьим кварталом прошлого 2023 года больше в 2,6 раза, а относительно второго квартала 2024 года объем противоправных финансовых действий, произведенных через банки, вырос почти вдвое.



При изучении причин роста объема финансового мошенничества, несмотря на активную борьбу и ожидание снижения его уровня, были исследованы отдельные категории мошенничества и проведен сравнительный анализ данных, опубликованных Центральным Банком РФ, за 3 квартал 2024 и 3 квартал 2023 года [3] (данные приведены в таблице 2).

Таблица 2

Классификация операций, совершенных без согласия клиентов
(III квартал 2023 и 2024 года)

Способ мошенничества	Объем операций без согласия клиентов, III квартал 2023 года (тыс. руб.)	Доля в общем объеме операций без согласия клиентов, %	Объем операций без согласия клиентов, III квартал 2024 года (тыс. руб.)	Доля в общем объеме операций без согласия клиентов, %
Карты	248620	86,09	189329	54,31
Счета	17241	5,97	32180	9,23
СБП	20131	6,97	61116	17,53
Электронные кошельки	2772	0,96	858	0,25
Денежные переводы путем внесения наличных	20	0,01	65110	18,68
Всего	288784	100	348593	100

По итогам исследования, проведенному по данным таблицы 2, были сделаны следующие выводы о динамике мошенничества в банковском секторе: наблюдается сокращение объема мошенничества (на 31,78 п.п.) через карты, однако все еще это основной способ.

За год произошел резкий рост мошенничества через денежные переводы (на 18,67 п.п.).

В Центральном Банке подобное явление объясняют тем, что с 25 июля 2024 года банки начали отчитываться о мошеннических операциях по обновленной форме, поскольку вступил в силу закон о противодействии мошенническим переводам, который изменил определение операции без добровольного согласия клиента. С июля 2024 года денежный перевод, совершенный человеком вследствие обмана или злоупотребления доверием, также является мошеннической операцией [4].

Наиболее подвержены способу мошенничества, связанным с переводом наличных средств или внесением их на счет мошенников, люди выше среднего возраста. Они чаще всего откладывают деньги в наличной форме, так как их уровень доверия к банковской системе снижен, что обусловлено особенностями их поколения. «В России до сих пор большое количество людей возрастом выше среднего, которые не всегда охотно применяют пластиковые карты или смартфоны при оплате товаров и услуг», – уточнил финансовый аналитик Михаил Беляев. Еще одна из причин высокого уровня распространенности данного способа мошенничества – граждане старше среднего возраста, в частности пожилые люди, обладающие высоким уровнем доверчивости к социальной инженерии мошенников.

Наблюдается рост мошенничества через счета и СБП (на 3,26 п.п. и 10,56 п.п. соответственно), что требует отдельного внимания, поскольку помимо обновления законодательства в этих сферах банковской деятельности выросла заинтересованность населения и, соответственно, количество пользователей увеличивается. Именно умение мошенников быстро приспосабливаться к развитию современных технологий могло стать



одним из решающих факторов, влияющих на стремительный рост уровня мошенничества – новые способы организации финансов с использованием СБП, например, гораздо быстрее и легче для граждан, чем более устаревшие способы, что уменьшает время на обдумывание своих действий и облегчает процесс кражи для мошенников.

Эксперты также объясняют общий рост числа операций, совершенных без согласия клиентов, ростом популярности СБП как вида оплаты. К примеру, Евгения Лазарева, руководитель проекта Народного фронта «За права заемщиков», координатор платформы «Мошеловка» комментирует ситуацию следующим образом: «Переводы через СБП удобны и в пределах 100 тысяч рублей бесплатны. Это одна из причин приоритетного выбора, в том числе при платежах, которые жертвы совершают под воздействием методов социальной инженерии. То, что легче для потребителей, удобнее и мошенникам. Этим же можно объяснить и рост объема хищений через электронные кошельки» [5].

Аферисты также стали активнее использовать для обзвона и иные технологии – мессенджеры Telegram и WhatsApp, так как звонки в мессенджерах бесплатны, в них часто инструменты против спама и фильтры недостаточно развиты. Особенно часто эти ситуации затрагивают такие незащищенные слои населения, как пожилых людей и людей в критических жизненных ситуациях.

В статье, посвященной мошенничеству ситуация объясняется тем, что банки зачастую уделяют недостаточно внимания безопасности расчетов и защите информации в достаточной мере, а также не осуществляют должным образом мониторинг и видеонаблюдение за банкоматами [6].

Банки совместно с Правительством России активно борются с мошенничеством: вводятся различные методы информирования населения о видах мошенничества (как на наружной рекламе, так и в сети интернет и также с использованием личного контакта с гражданами), однако этого недостаточно, чтобы предотвратить действие возникающих с каждым днем новых способов финансового мошенничества. В связи с этим мы выявили несколько гипотез, которые могли бы уменьшить объем операций, выполняемых без согласия физических лиц в частности.

В связи с высокой долей мошенничества с использованием социальной инженерии и влиянием на незащищенные слои населения мы предполагаем, что работа с информационными источниками должна активно развиваться. То количество методов обеспечения информацией населения о борьбе с мошенничеством и защите персональных данных является достаточно большим, однако все еще недостаточным. Стоит сделать упор на те источники, которые пользуются большим доверием у людей пожилого возраста и у тех, кто попал в тяжелую жизненную ситуацию.

Банки самостоятельно могут информировать клиентов об основах безопасности, включая распознавание мошеннических операций и рискованных транзакций – например, при выдаче дебетовых карт или регистрации в онлайн-приложении банка.

Ещё одно из решений, способных уменьшить объем неправомερных операций с использованием инструментов банковского сектора – создание и внедрение образовательных программ для клиентов по выявлению фишинг-атак и по безопасному поведению в интернет-пространстве.

Со стороны банковской среды или государства полезным решением будет создание специальной горячей линии для клиентов, где они могли бы сообщать о подозрительных действиях сотрудникам, работающим на этой горячей линии, которые должны быть компетентны не только в предотвращении проведения этих операций, но и во взаимодействии с правоохранительными органами в целях наказания этих мошенников.



Ограничить объем переводов способно ужесточение правил перевода средств, например, внедрение лимитов на суммы переводов без дополнительной верификации по звонку из банка с уточнением цели и предостережения клиентов от рискованных действий.

Для тех видов противоправной деятельности в банковском секторе, при которых мошеннические действия проводятся без согласия и без ведома обладателя персональными данными поможет такой способ обеспечения финансовой безопасности как регулярный анализ транзакций (возможно с использованием нейросетевых моделей) для выявления аномалий и подозрительных действий в реальном времени. В непрерывном обновлении системы защиты от мошенничества учреждениям банковской сферы способно помочь возможное сотрудничество с поставщиками антивирусного программного обеспечения или иными инновационными проектами, занимающимися разработкой программного обеспечения.

Активное использование мессенджеров для обзвона вызывает необходимость разработки и внедрения программного обеспечения для мониторинга мессенджеров на предмет мошеннических действий и их предварительного предотвращения, а также защиты от спам-сообщения, включающих нежелательную рекламу и предложения мошенников.

Недостаточное внимание к безопасности расчётов и защите информации решается путём разработки и создания средств мониторинга и видеонаблюдения за банкоматами, включая системы для анализа поведения клиентов, для которых инструментом может стать работа искусственного интеллекта.

Телеком-сектору необходимо усилить работу в сфере противодействия кибермошенничеству, в частности продолжать борьбу с «серыми» сим-картами, проверять и обновлять данных об абонентах, идентифицировать рабочие телефоны сотрудников организаций, а также принимать меры и по решению возникающих проблем, и по предотвращению их возникновения.

Таким образом, по данным проведенного исследования было выявлено, что объём операций, совершенных без согласия клиентов, в 2024 году вырос, а особенно это заметно по 3 кварталу. Произошло как вследствие изменения в законодательстве, так и из-за высокого уровня приспособленности и социальных навыков у мошенников. Из способов мошеннических операций большей популярностью выделились такие категории операций как СБП и денежные переводы из-за простоты и быстроты их применения. Государство и банковский сектор продолжают активную борьбу с мошенничеством, однако в современных реалиях этого недостаточно для остановки роста объема противоправных финансовых операций. Необходимо ввести в работу новые инновационные решения, отвечающие на вызовы современности для предотвращения роста количества операций без согласия физических и юридических лиц.

Список литературы:

1. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 28.12.2024) ст. 159, п. 1
2. Противодействие мошенническим операциям: итоги III квартала // Банк России. – URL: <https://www.cbr.ru/press/event/?id=23217> (дата обращения: 30.12.2024)
3. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // Банк России. – URL: https://www.cbr.ru/statistics/ib/review_1q_2024/ (дата обращения: 30.12.2024)
4. Кошкина Ю., Чернышова Е. Объем хищений с банковских счетов россиян оказался рекордным за 4 года / Кошкина Ю., Чернышова Е. // РБК: сайт. – URL: <https://www.rbc.ru/finances/09/12/2024/6756dfb09a79477dd39360b6> (дата обращения: 30.12.2024)



5. Банковские мошенничества в 2024 году: новая реальность или продолжение тренда?
// Уралсиб. – URL: <https://journal.uralsib.ru/hse/research/7> (дата обращения: 30.12.2024)

6. Дадашов, Р. Ф. Актуальные меры противодействия интернет-мошенничества, связанного с использованием платежных карт / Р. Ф. Дадашов, Т. С. Биндюкова // Актуальные проблемы современности. – 2019. – № 1 (23). – С. 53-59

