СОВРЕМЕННЫЕ МОШЕННИЧЕСКИЕ СХЕМЫ С ЭЛЕКТРОННЫМИ ПЛАТЕЖАМИ И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ ИМ

А. Р. Дудова

Саратовский национальный исследовательский государственный университет им. Н.Г. Чернышевского, Россия
E-mail: alisiadudova@mail.ru

В научной статье рассмотрены основные виды современных мошеннических операций с электронными платежами, получившие широкое распространение на территории Российской Федерации в связи с возникшей острой военно-геополитической ситуацией в мире. Представлен анализ динамики мошеннических операций в РФ. Рассмотрена проблематика разработки методов и схем противодействия современным схемам мошенничества в сфере операций с электронными платежами.

POTENTIAL OF THE MARKET IN RUSSIA IN MODERN CONDITIONS

A. R. Dudova

The scientific article examines the main types of modern fraudulent transactions with electronic payments, which have become widespread in the territory of the Russian Federation in connection with the acute military-geopolitical situation in the world. The analysis of the dynamics of fraudulent transactions in the Russian Federation is presented. The problems of developing methods and schemes to counter modern fraud schemes in the field of transactions with electronic payments are considered.

Целью данного научного исследования является комплексное изучение современных мошеннических схем, связанных с электронными платежами, а также анализ эффективных методов противодействия им. В статье также приведены рекомендации по повышению уровня безопасности как для пользователей, так и для финансовых институтов.

Под финансовым мошенничеством понимается совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения [1, 2].

Сегодня человечеству приходится сталкиваться с новыми, менее уязвимыми и тщательно разработанными вредоносными программами и махинациями, при помощи которых злоумышленники довольно быстро заполучают доступ к персональным данным клиента.

Так, в связи с непрерывным и повсеместным внедрением автоматизированных систем обработки данных из года в год увеличивается число преступлений и посягательств в сфере электронных информационных, в частности, платежных систем.

Ниже представлен анализ статистики операций без согласия клиентов в

2023 году относительно физических лиц (см. рис. 1) [3].

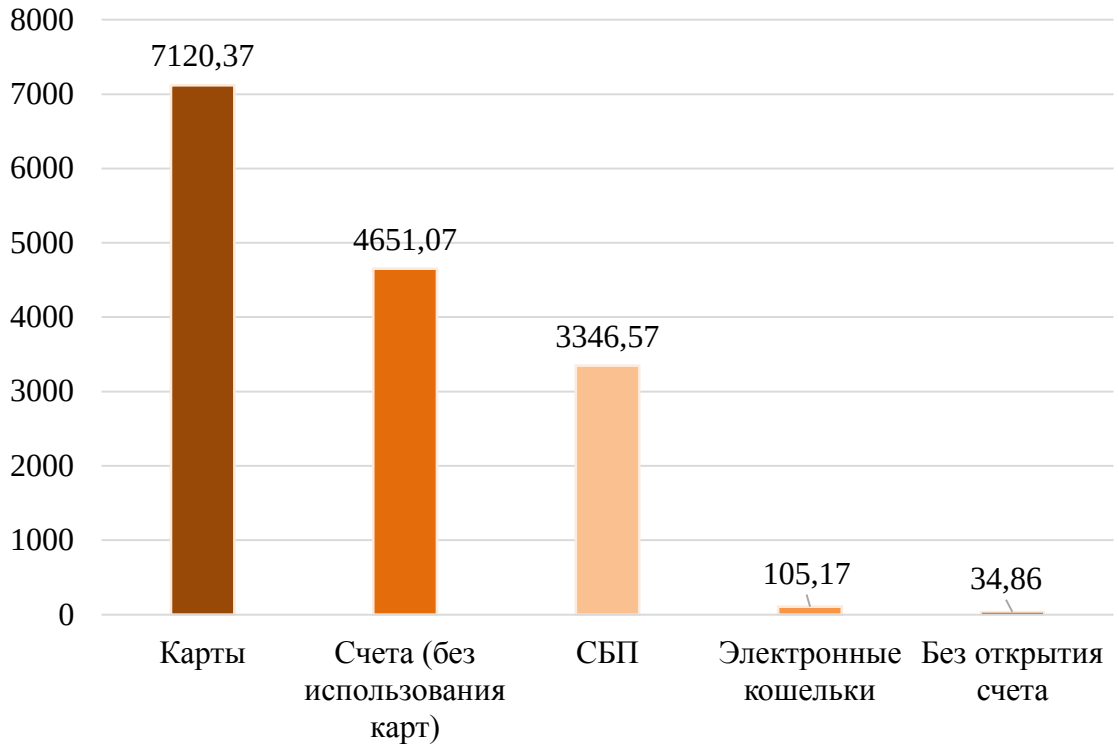

Рис. 1. Операции без согласия клиентов – физических лиц в 2023 г., млн. руб. [3]

Так, объем операций, совершенных мошенниками с использованием электронных платежных карт, оказался самым высоким среди рассматриваемых категорий в 2023 году.

В январе - марте 2024 года через СБП у россиян было украдено около 1,13 млрд. руб. По сравнению с аналогичным периодом 2023 года увеличение показателя произошло более чем в 2 раза. В то же время количество самих незаконных операций характеризуется 3-х кратным увеличением за год (см. рис. 2) [4]. Данная тенденция наблюдается, в частности, по причине роста популярности данного способа оплаты среди граждан России.

В первом квартале 2024 года россияне провели 2,5 миллиарда операций через СБП на общую сумму 10,5 триллиона рублей. Это вдвое больше по сравнению с аналогичным периодом прошлого года [4].

В период с января по март 2024 года россияне потеряли около 40 миллионов рублей через электронные кошельки, что на 40% больше, чем в первом квартале 2023 года, где сумма составила 28 миллионов рублей [4].

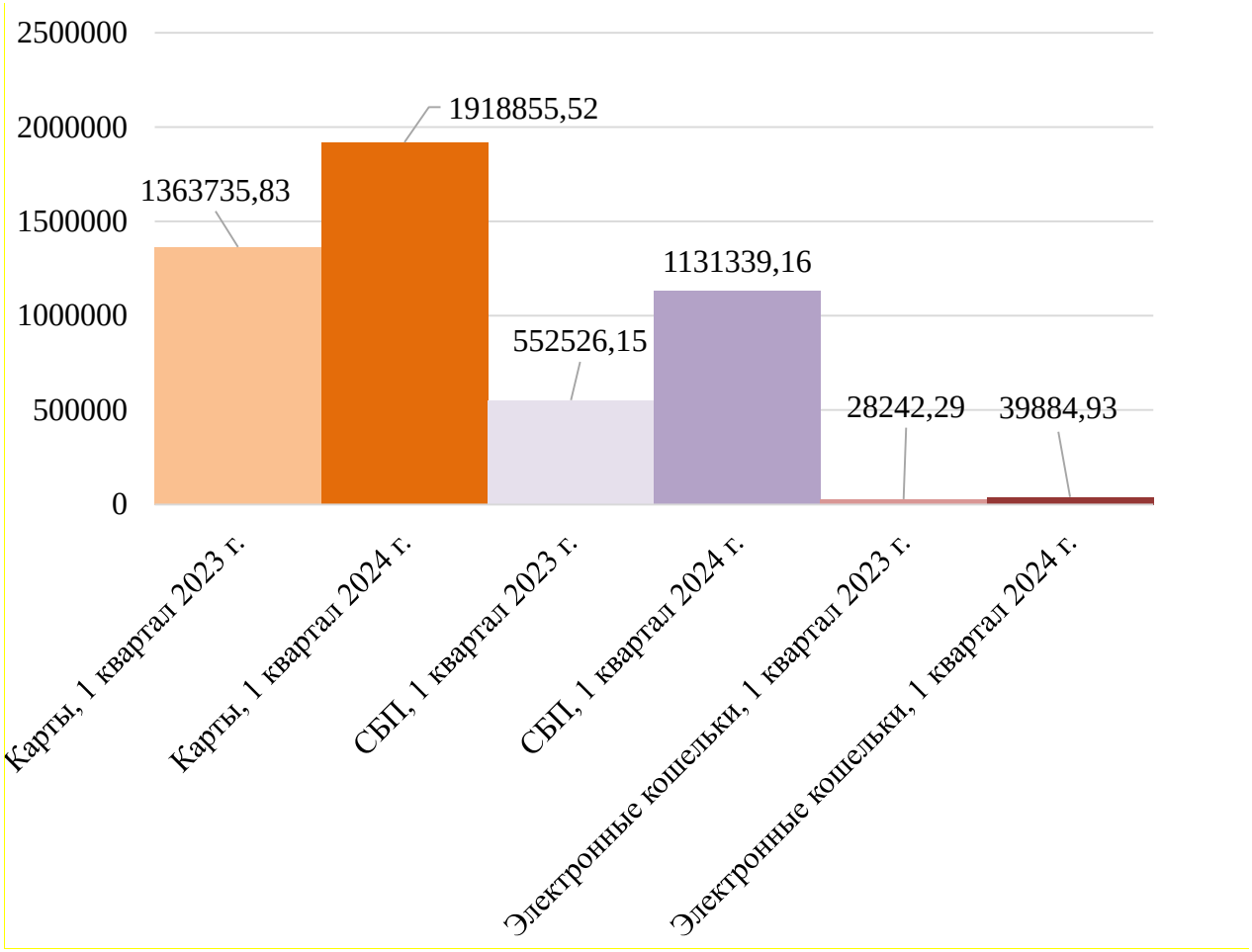

Рис. 2. Сравнительный анализ динамики объемов инцидентов
в сфере информационной безопасности ЦБ РФ в отношении физических лиц
за период 1 квартала 2023, 2024 гг., тыс. руб. [4]

Стоит отметить, что наибольший объем хищений приходится на обычные банковские карты (см. рис. 2). Рост за период 2023-2024 гг. составил более 40%. В предыдущие годы большинство незаконных операций проводилось в отношении клиентов интернет-магазинов. Сегодня же целью финансовых мошенников является доступ к дистанционным банковским сервисам и конфиденциальным данным, при помощи которых злоумышленник сможет не только снять деньги со счета, но и оформить кредит. В частности, именно поэтому больше всего потерь граждане терпят в сфере мобильного и интернет-банкинга [4].

В период с января по март 2024 года кредитные учреждения зарегистрировали почти 13,9 млн. попыток кибермошенничества с целью похищения средств у клиентов, что в пять раз превышает количество подобных случаев за аналогичный период прошлого года [4].

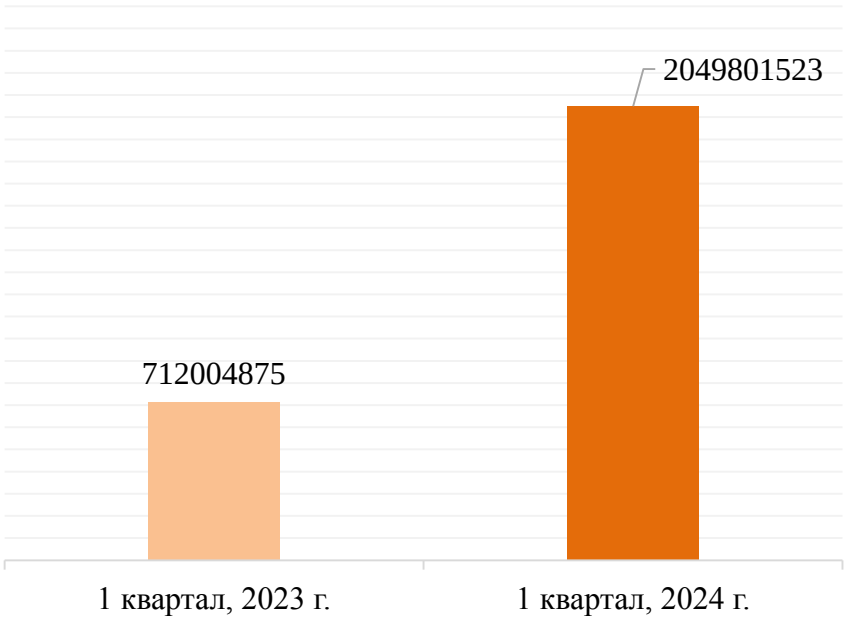

Рис. 3. Объем предотвращенных операций без согласия клиентов
за период 1 квартала 2023, 2024 гг., тыс. руб. [4]

В случае перевода средств на мошеннический счет, включенный в специальную базу данных ЦБ, финансовые организации обязаны компенсировать клиентам понесенные убытки. Данная практика стала неким стимулом для банков в сфере активного развития технологий по борьбе с мошенничеством (см. рис. 3).

Важно отметить, что наибольший объем возмещенных денежных средств характерен для операций типа «Счет» [4].

Так, благодаря оперативной работе антифрод-процедур кредитных организаций финансовым мошенникам не удалось провести более 2,7 млн. незаконных операций в 2023 году и 2, 049 млрд. ед. в 2024 г. [4].

Среди всего многообразия видов мошенничества с электронными платежами, можно выделить фишинг, скимминг, операцию «Звонок по видеосвязи для идентификации «клиентов банка» по биометрии».

Скимминг представляет собой разновидность мошеннических операций, а именно считывание с магнитной полосы карты информации. Для этого используются специализированные технические устройства или скиммеры – устройства, крепящиеся непосредственно к самому банкомату или любому принимающему слоту картоприемника [5].

Объем рынка скимминга платежных карт вырос с 3,16 млрд. долл. в 2023 году до 3,56 млрд. руб. в 2024 г. (см. рис. 4) [6].

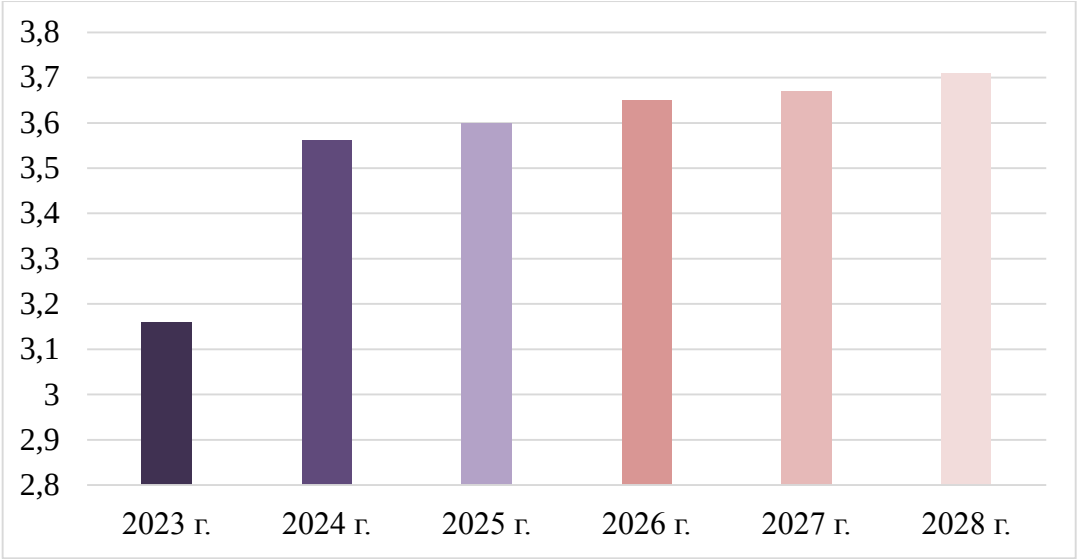

Рис. 4. Размер и возможные темпы роста глобального рынка скимминга платежных карт в 2024 г., млрд. долл. [6]

В абсолютном выражении Европа пока обгоняет Россию по скиммингу, а именно, в зарубежных странах на 1000 банкоматов приходится девятнадцать случаев скимминга, в России – до пяти. [6] Данная динамика объясняется разработкой новых специальных устройств, предназначенных для внедрения внутрь банкомата для считывания данных с чип-карт. Данный вид мошенничества получил название «Шимминг».

Еще одной разновидностью финансового мошенничества является фишинг. При помощи подделывания официальных сайтов мошенники завладевают конфиденциальной информацией, маскируясь под доверенное лицо.

Так, в первой половине 2024 года наибольшее количество фишинговых ресурсов было заблокировано для следующих брендов (см. рис. 5) [7].

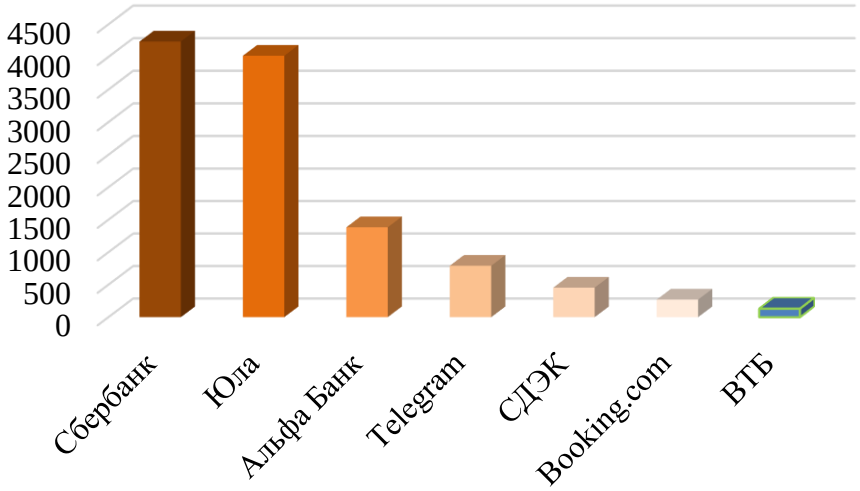

Рис. 5. Рейтинг заблокированных сайтов, 1 полугодие 2024 г., ед. [7]

График, представленный выше, отражает положительную динамику в сфере активации работы мошеннических сайтов в 2024 году.

Сегодня существует множество полезных рекомендаций от Центрального

Банка РФ. Среди них можно выделить следующие: важно не сообщать никому и никогда паспортные данные, финансовые сведения, (данные карты и владельца, CVV-код); не хранить данные карт и PIN-коды на электронных устройствах; по возможности установить антивирус на все устройства и регулярно обновлять их; завести клиентам специальную карту для онлайн-покупок, пополнять ее ровно на ту сумму, которая нужна для оплаты [8, 9].

Однако учитывая быстрые темпы роста объема мошеннических операций сегодня, одних лишь рекомендаций ЦБ РФ недостаточно. Поэтому в качестве дополнительных предложений по повышению уровня безопасности как для пользователей, так и для финансовых институтов можно добавить создание, развитие и распространение программ, курсов по повышению финансовой и юридической грамотности в образовательных учреждениях, государственном секторе, на предприятиях и в др. организациях.

Таким образом, противодействие мошенничеству с электронными платежами требует комплексного подхода, который сочетает в себе образовательные инициативы, технические меры и правовые механизмы. Только так можно повысить эффективность защиты денежных средств, конфиденциальных данных пользователей и организаций в современном цифровом пространстве.

СПИСОК ЛИТЕРАТУРЫ

1. *Кузнецов Д. С., Гусева М. Н.* Финансовое мошенничество в России: сущность, виды, проблемы противодействия // Наука и образование. 2022. № 3. [Электронный ресурс]. - URL: https://cyberleninka.ru/article/n/finansovoe-moshennichestvo-v-rossii-suschnost-vidy-problemy-protivodeystviya (дата обращения: 04.11.2024).
2. Финансовое мошенничество. [Электронный ресурс]. URL: https://kimovsk.gosuslugi.ru/netcat_files/550/3173/Finansovoe_moshennichestvo.pdf (дата обращения: 05.10.2024).
3. Обзор операций, совершенных без согласия клиентов финансовых организаций [Электронный ресурс]. URL: https://cbr.ru/analytics/ib/operations_survey/2023/ (дата обращения: 06.10.2024).
4. Банковские мошенничества в 2024 году: новая реальность или продолжение тренда? [Электронный ресурс]. URL: https://journal.uralsib.ru/hse/research/7 (дата обращения: 06.10.2024).
5. Считать и украсть: как работает скимминг банковских карт. [Электронный ресурс]. URL: https://trends.rbc.ru/trends/industry/612d019d9a79470c54677745?ysclid=m31z23tz6j258388705 (дата обращения: 16.10.2024).
6. Payment Card Skimming Global Market Report 2024. [Электронный ресурс]. URL: https://www.thebusinessresearchcompany.com/report/payment-card-skimming-global-market-report (дата обращения: 27.10.2024).
7. Статистика фишинга за первое полугодие 2024 года. [Электронный ресурс]. URL: https://ob-man.com/статистика-фишинга-за-первое-полугод/ (дата обращения: 01.11.2024).
8. Противодействие мошенническим практикам. [Электронный ресурс]. URL: https://www.cbr.ru/information_security/pmp/ (дата обращения: 03.11.2024).
9. *Григорьева Д. В., Коробов Е. А.* Проблема киберпреступности в банковском секторе российской экономики // Глобальные проблемы модернизации национальной экономики. Материалы XII Междун. науч.-практич. конф. 2023. С. 422-427.