



5.2.4. Финансы

Научная статья

УДК 347.73

<https://doi.org/10.37493/2307-907X.2025.6.18>

## ОСОБЕННОСТИ ФИНАНСОВОЙ БЕЗОПАСНОСТИ НАСЕЛЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Эльвира Анцасовна Русецкая<sup>1\*</sup>, Максим Владимирович Зеленов<sup>2</sup>,  
Эллина Владимировна Клочкова<sup>3</sup>, Елена Александровна Нейман<sup>4</sup>

<sup>1-4</sup> Северо-Кавказский федеральный университет (д. 1, ул. Пушкина, Ставрополь, 355017, Российская Федерация)

<sup>1</sup> [elwirasgu@mail.ru](mailto:elwirasgu@mail.ru); <https://orcid.org/0000-0002-6021-7493>

<sup>2</sup> [smax8825@gmail.com](mailto:smax8825@gmail.com); <https://orcid.org/0009-0002-5851-3346>

<sup>3</sup> [doevaellina@yandex.ru](mailto:doevaellina@yandex.ru); <https://orcid.org/0009-0005-7767-5633>

<sup>4</sup> [lenaneiman911@mail.ru](mailto:lenaneiman911@mail.ru); <https://orcid.org/0009-0003-9539-7230>

\* Автор, ответственный за переписку

**Аннотация. Введение.** Проведенный анализ научных источников по теме исследования, нормативных документов и методических материалов Центрального Банка Российской Федерации, свидетельствует о наличии устойчивой негативной динамики в сфере финансовой безопасности населения. Наблюдается системный рост как количественных показателей мошеннических операций, так и объема похищенных денежных средств. Проблема финансовой безопасности населения Российской Федерации приобретает особую актуальность в условиях роста цифровизации финансовых услуг, увеличения мошеннических операций и недостаточно высокого уровня финансовой грамотности. **Цель.** Анализ динамики фрод-операций, выявление ключевых угроз финансовой безопасности и разработка рекомендаций по их минимизации. **Материалы и методы.** Методологическую основу исследования составили работы отечественных экономистов по финансовой безопасности. Применены системный анализ нормативной базы Банка России и статистические методы изучения данных за 2022–2024 гг. Выбор методов обусловлен необходимостью комплексной оценки динамики мошеннических операций через анализ количественных показателей и качественных характеристик. **Результаты и обсуждение.** В ходе работы выявлено, что объем мошеннических операций за 2022–2024 гг. вырос на 94 %, при этом наибольший рост связан с использованием Системы быстрых платежей (СБП). Основными видами финансового мошенничества являются: телефонное мошенничество, фишинг (вид интернет-мошенничества, при котором злоумышленники пытаются выманить у жертвы личную информацию под видом официального запроса), компьютерные атаки. Установлено, что 58 % заблокированных ресурсов – фишинговые сайты, а физические лица становятся жертвами в 13 раз чаще юридических. **Заключение.** В целях минимизации мошеннических операций и снижения фрод-активности в исследовании предложен комплексный подход, сочетающий образовательные, информационные и технологические меры, способные существенно повысить уровень финансовой безопасности в долгосрочной перспективе.

**Ключевые слова:** финансовая безопасность, мошенничество, фрод-операции, финансовая грамотность, цифровая трансформация  
**Для цитирования:** Особенности финансовой безопасности населения Российской Федерации / Э. А. Русецкая, М. В. Зеленов, Э. В. Клочкова, Е. А. Нейман // Вестник Северо-Кавказского федерального университета. 2025. № 6(111). С. 170–178. <https://doi.org/10.37493/2307-907X.2025.6.18>

**Конфликт интересов:** авторы заявляют об отсутствии конфликта интересов.

Статья поступила в редакцию 06.10.2025;

одобрена после рецензирования 10.11.2025;

принята к публикации 17.11.2025.

Research article

## FEATURES OF FINANCIAL SECURITY OF THE POPULATION OF THE RUSSIAN FEDERATION

Elvira A. Rusetskaya<sup>1</sup>, Maxim V. Zelenov<sup>2</sup>, Ellina V. Klochkova<sup>3</sup>, Elena A. Neiman<sup>4</sup>

<sup>1-4</sup> North-Caucasus Federal University (1, Pushkina Str., Stavropol, 355017, Russian Federation)

<sup>1</sup> [elwirasgu@mail.ru](mailto:elwirasgu@mail.ru); <https://orcid.org/0000-0002-6021-7493>

<sup>2</sup> [smax8825@gmail.com](mailto:smax8825@gmail.com); <https://orcid.org/0009-0002-5851-3346>

<sup>3</sup> [doevaellina@yandex.ru](mailto:doevaellina@yandex.ru); <https://orcid.org/0009-0005-7767-5633>

<sup>4</sup> [lenaneiman911@mail.ru](mailto:lenaneiman911@mail.ru); <https://orcid.org/0009-0003-9539-7230>

\* Correspondence author

**Abstract. Introduction.** The analysis of scientific sources on the research topic, regulatory documents, and methodological materials of the Central Bank of the Russian Federation indicates a steady negative trend in the field of financial security for the population. There is a systematic increase in both the number of fraudulent transactions and the amount of stolen funds. The issue of financial security for the population of the Russian Federation becomes particularly relevant in the context of increasing digitalization of financial services, increasing fraudulent transactions, and a low level of financial literacy. **Goal.** The study aims to analyze the dynamics of fraud operations, identify key threats to financial security, and develop recommendations for their minimization. **Materials and methods.** The study is based on the works of Russian economists on financial security. It uses a systematic analysis of the regulatory framework of the Bank of Russia and statistical methods to study data from 2022 to 2024. The choice of methods is driven by the need for a comprehensive assessment of the dynamics of fraudulent transactions through the analysis of quantitative indicators and qualitative characteristics. **Results and discussion.** The study revealed that the volume of fraudulent transactions increased by 94% in

© Русецкая Э.А., Зеленов М.В., Клочкова Э.В., Нейман Е.А., 2025

2022-2024, with the greatest increase associated with the use of the Rapid Payment System (RPS). The main types of financial fraud include phone scams, phishing (a type of online fraud where attackers attempt to obtain personal information from victims under the guise of official requests), and computer attacks. It was found that 58% of blocked resources were phishing websites, and individuals were 13 times more likely to become victims than legal entities. **Conclusion.** In order to minimize fraudulent transactions and reduce fraud activity, the study proposes a comprehensive approach that combines educational, informational, and technological measures that can significantly improve financial security in the long term.

**Keywords:** financial security, fraud, fraud operations, financial literacy, digital transformation

**For citation:** Rusetskaya EA, Zelenov MV, Klochkova EV, Neiman EA. Features of the Financial Security of the Population of the Russian Federation. Newsletter of North-Caucasus Federal University. 2025;6(111):170-178. (In Russ.). <https://doi.org/10.37493/2307-907X.2025.6.18>

**Conflict of interest:** the authors declare that there is no conflict of interest.

The article was submitted 06.10.2025;

approved after reviewing 10.11.2025;

accepted for publication 17.11.2025.

**Введение / Introduction.** В современных экономических условиях наблюдается устойчивая тенденция к росту актуальности проблемы финансовой безопасности. Данный феномен детерминирован совокупностью факторов, среди которых особого внимания заслуживает количественный рост мошеннических операций. Указанная закономерность находится в прямой корреляции с недостаточным уровнем развития финансовой грамотности населения, качественной эволюцией методов осуществления противоправных финансовых операций, а также усложнением международной экономико-политической конъюнктуры.

Финансовая безопасность в узком смысле может быть определена как состояние защищённости экономических интересов граждан от потенциальных угроз, связанных с незаконным использованием их денежных средств. Данная категория предполагает создание условий, при которых обеспечивается как удовлетворение базовых жизненных потребностей, так и поддержание устойчивого материального благополучия.

В рамках такого подхода акцент делается на индивидуальном уровне финансовой безопасности, где ключевым объектом защиты выступают персональные экономические интересы физических лиц. При этом важнейшей характеристикой данного состояния является способность противостоять различным формам противоправных действий, направленных на незаконное присвоение или использование денежных активов граждан.

В условиях нестабильности, стремительной цифровизации финансовой сферы и изменчивой динамики финансовой грамотности населения вопросы обеспечения финансовой безопасности граждан России выходят на первый план. Особую остроту эта проблема приобретает в контексте существенных региональных различий при сохранении общенациональных тенденций.

Наблюдаемая взаимосвязь между экономической конъюнктурой, технологическим развитием финансового сектора и уровнем финансовой образованности населения формирует сложную систему многофакторных зависимостей. Эти взаимосвязи требуют глубокого научного осмысления, особенно в связи с необходимостью разработки эффективных механизмов защиты экономических интересов граждан в условиях трансформирующейся цифровой экономики [5].

Финансовая безопасность в широком смысле представляет собой систему мер, обеспечивающих защиту финансовых активов всех экономических агентов национального хозяйства, включая население, коммерческие структуры и государственные институты. Данная система направлена на предотвращение незаконного присвоения денежных ресурсов и минимизацию финансовых рисков различного характера [1,4].

Фрод (финансовое мошенничество) представляет собой противоправную деятельность, осуществляемую отдельными лицами или организованными группами с целью незаконного извлечения доходов посредством введения потерпевших в заблуждение. Такие действия характеризуются умышленным характером и направлены на получение материальной выгоды за счет обмана добросовестных участников экономических отношений.

**Материалы и методы исследований / Materials and methods of research.** Методологическую основу исследования составили работы отечественных экономистов по финансовой безопасности. Применены системный анализ нормативной базы Банка России и статистические методы изучения данных за 2022–2024 гг. Выбор методов обусловлен необходимостью комплексной оценки динамики мошеннических операций через анализ количественных показателей и качественных характеристик. Последовательность исследования включала теоретический анализ, обработку статистики ЦБ, разработку и экспертную оценку предложений по минимизации рисков.

**Результаты исследований и их обсуждение / Research results and their discussion.** Рассматривая финансовую безопасность как комплекс мероприятий по противодействию мошенническим операциям, Центральный Банк Российской Федерации выделяет виды *фрод-операций*:

- атаки с использованием телефонного мошенничества;
- атаки с использованием фишинговых сайтов;
- компьютерные инциденты и компьютерные атаки;
- финансовые пирамиды [9].

Количественные данные по операциям, произведенным без добровольного согласия клиентов, представлены в таблице 1.

Таблица 1 / Table 1

**Динамика общего объема и количества операций без добровольного согласия клиентов / Dynamics of the total volume and number of transactions without the voluntary consent of clients**

Показатель	Год			Отклонение			Темп прироста, %		
	2022	2023	2024	2023 к 2022	2024 к 2023	2024 к 2022	2023 к 2022	2024 к 2023	2024 к 2022
Объем операций, млн руб.	14 165,44	15 791,41	27 534,31	+1 625,97	+11 742,9	+13 368,86	+11,47	+74,36	+94,37
Количество операций, тыс. ед.	876,59	1 165,99	1 197,44	+289,4	+31,45	+320,85	+33,01	+2,69	36,6

\*Источник: составлено авторами по [2, 6] / Source: compiled by the authors according to [2, 6]

Согласно данным таблицы 1, за период 2022–2024 гг. наблюдается значительный рост объема мошеннических операций с 14,16 млрд руб. до 27,53 млрд руб., что свидетельствует о почти двукратном увеличении (94,4 %). При этом темпы роста количества операций отстают от динамики увеличения их объема, что указывает на возрастание средней суммы одной фрод-операции [6, 10].

Наиболее существенный прирост зафиксирован в 2024 г., когда объем мошенничества увеличился на 11,7 млрд руб. по сравнению с предыдущим периодом, составив 74 % от общего трехлетнего прироста. Основными драйверами данной негативной динамики стали двукратное расширение пользовательской базы Системы быстрых платежей (СПБ) и 40-процентный рост электронных платежей, что создало благоприятную среду для развития мошеннических схем. Эти тенденции актуализируют необходимость совершенствования механизмов финансового контроля и разработки более эффективных защитных мер [5, 10].

Однако с 25 июля 2024 г. вступил в силу Федеральный закон от 24 июля 2023 года № 369-ФЗ «О внесении изменений в Федеральный закон „О национальной платежной системе”», вводящий новые механизмы борьбы с мошенническими транзакциями. Закон уточняет определение операции без добровольного согласия клиента: под ней понимается денежный перевод, осуществленный клиентом финансового учреждения в результате обмана или злоупотребления доверием. С этой же даты финансовые учреждения начали сообщать о мошеннических операциях в обновленном формате, отражающем эти законодательные изменения, что соответственно привело к увеличению объема сообщений и количества мошеннических операций [9, 2].

Анализ данных, представленных на рисунке 1, позволяет выявить ключевые тенденции в динамике мошеннических операций по видам платежных инструментов. Наибольшее количество фрод-операций в 2023–2024 гг. зафиксировано с использованием банковских карт: 984 тыс. случаев в 2023 г. и 821 тыс. в 2024 г.

При этом наблюдается разнонаправленная динамика по другим каналам: отмечается рост операций через СБП при одновременном сокращении количества мошеннических действий с использованием электронных кошельков. Данная ситуация обусловлена решением Центрального Банка РФ от 21 февраля 2024 г. об отзыве лицензии у QIWI-Банка, который предоставлял возможность анонимных переводов без открытия счета. Это регуляторное решение существенно изменило структуру мошеннических операций в сегменте электронных платежей [2].

Наиболее распространенным методом проведения транзакций с использованием мобильного устройства без добровольного согласия является его заражение вредоносным кодом. Использование методов социальной инженерии (таких как ссылки в SMS-сообщениях, онлайн-реклама и т. д.) значительно повышает вероятность заражения мобильного устройства.

В результате злоумышленник получает возможность инициировать переводы денежных средств, в то время как уведомления о транзакциях могут не поступать владельцу мобильного устройства.

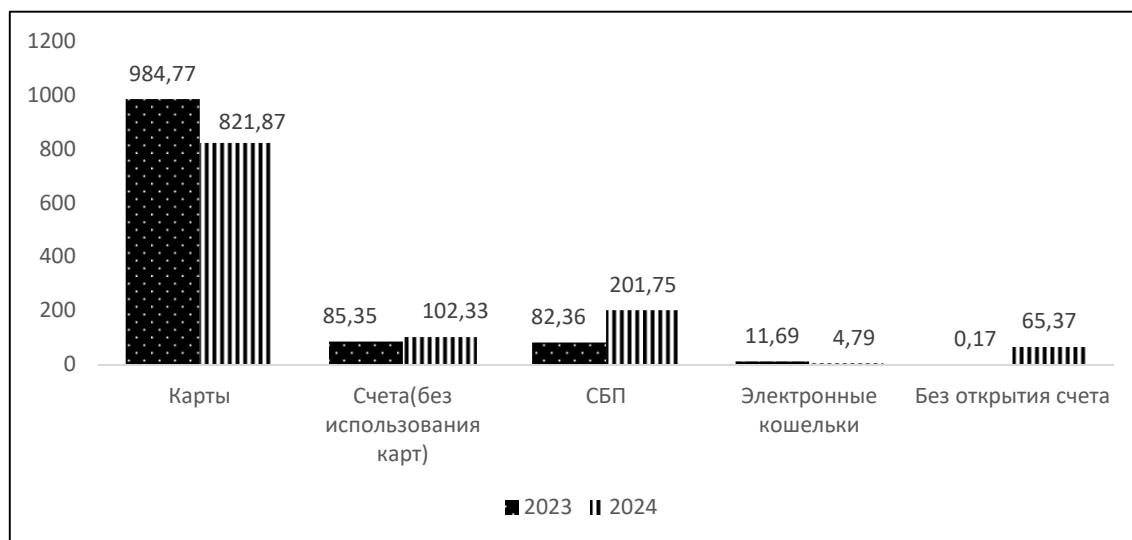


Рис. 1. Количество фрод-операций по видам за 2023–2024 гг., тыс. ед. /

Fig. 1. Number of fraudulent operations by type for 2023-2024, thousand units

\*Источник: составлено авторами по [3] / Source: compiled by the authors according to [3]

На рисунке 2 рассмотрена динамика мошеннических операций по видам платежных документов.

Данные рисунка 2 свидетельствуют, что объем мошеннических операций физических лиц превышает количество аналогичных юридических лиц более чем в 13 раз, а количество – более чем в 800 раз.



Рис. 2. Операции без согласия по видам клиентов / Fig. 2. Non-consensual transactions by client type

\*Источник: составлено авторами по [3] / Source: compiled by the authors according to [3]

При совершении фрод-операций мошенники используют различные телефонные номера. Анализ данных, представленных на рисунке 3, выявляет характерные особенности структуры мошеннических операций, совершаемых посредством телефонных звонков. Основная доля противоправных действий осуществляется с использованием стандартных мобильных номеров, что оказывает значительное психологическое давление на социально уязвимые группы населения с низким уровнем финансовой грамотности. Особую сложность для идентификации представляют случаи подмены номеров, когда злоумышленники маскируются под федеральные номера формата «8-800», имитируя официальные контакты финансовых организаций.

Следует подчеркнуть, что легитимные кредитные организации, являющиеся участниками системы страхования вкладов, в соответствии с действующим российским законодательством никогда не запрашивают конфиденциальные данные клиентов или подтверждение операций по телефону. Данный факт может служить ключевым маркером для идентификации мошеннических схем. Услож-

нение методов социальной инженерии, включая технологию подмены номеров, требует усиления защитных механизмов и повышения финансовой грамотности населения.

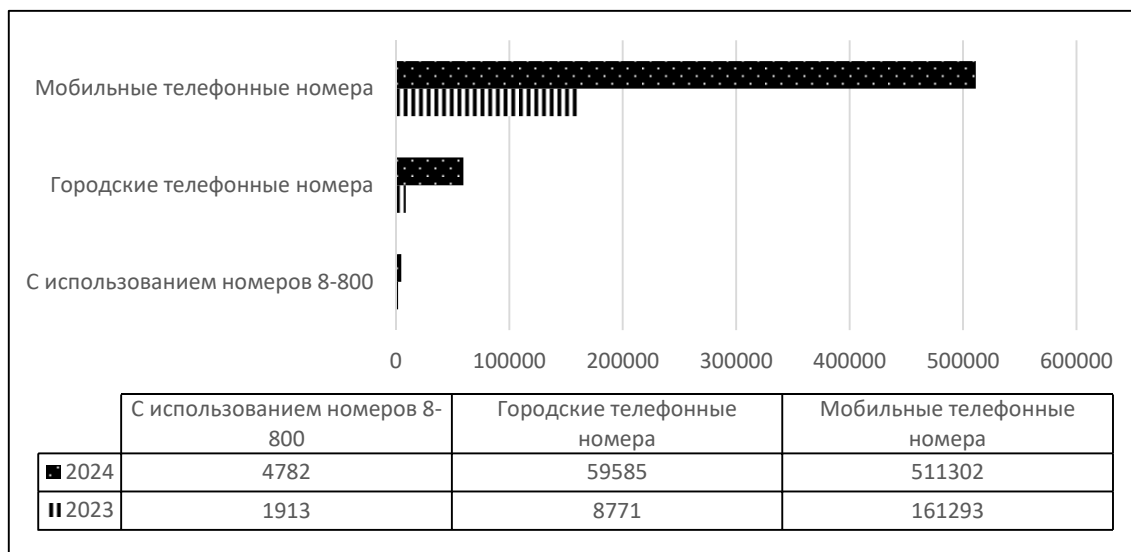


Рис. 3. Использование телефонных номеров для фрод-операций /

Fig. 3. Using phone numbers for fraudulent operations

\*Источник: составлено авторами по [3, 7] / Source: compiled by the authors according to [3, 7]

На рисунке 4 представлены основные типы ресурсов, используемые злоумышленниками в 2024 г.

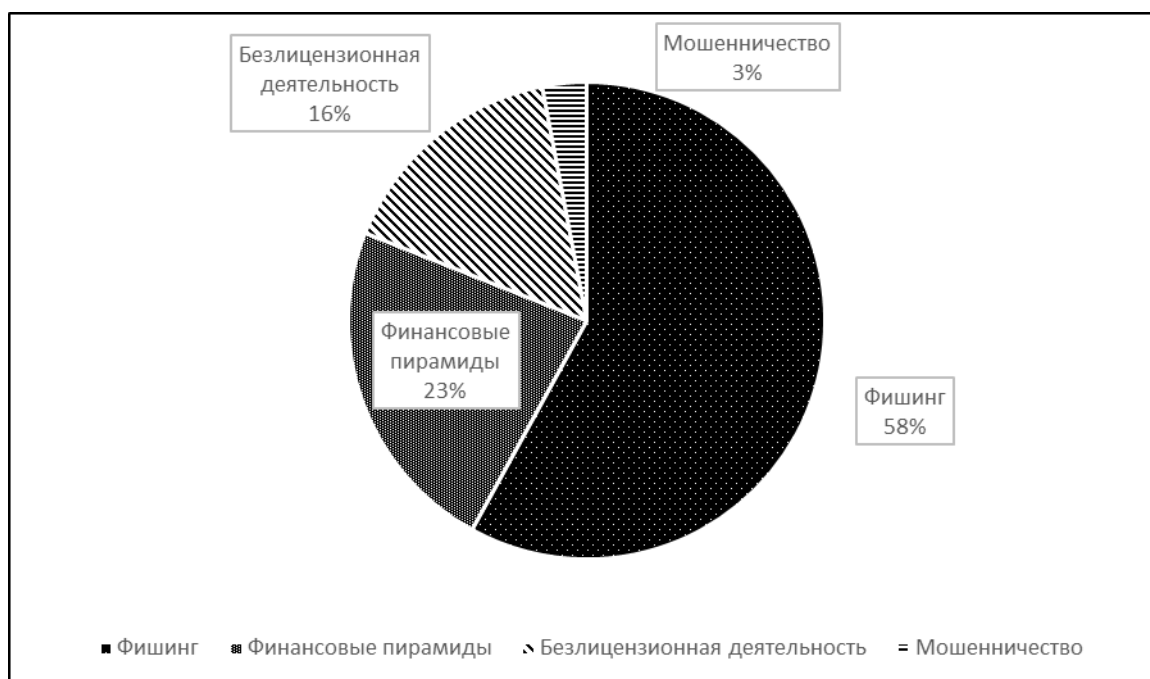


Рис. 4. Типы ресурсов, используемые злоумышленниками в 2024 г. /

Fig. 4. Types of resources used by offenders in 2024

\*Источник: составлено авторами по [3] / Source: compiled by the authors according to [3]

В 2024 г. большинство ресурсов, заблокированных по инициативе Банка России (58 %), были фишинговыми сайтами, выдававшими себя за известные банки и инвестиционные компании. Второе место (23 %) заняли финансовые пирамиды, часто замаскированные под онлайн-игры, где пользователям обещали огромную прибыль (до 1000 % годовых) от покупки внутриигровых персонажей, что приводило к потере всех вложенных средств [8].

Мошеннические веб-сайты, осуществляющие нелегальную деятельность на рынке ценных бумаг, а также выдающие себя за несуществующие кредитные и микрофинансовые организации, также оставались широко распространенными (около 16 %). Около 3 % заблокированных ресурсов были отнесены к категории «прочее мошенничество». Распространение вредоносного программного обеспечения (malware) было наименее распространенным видом мошенничества, на долю которого приходилось менее 1 % всех заблокированных ресурсов.

Стоит отметить, что, по данным Банка России, в 2023 г. кибератак на банки и финансовые компании стало меньше, чем в 2022 г., но методы у хакеров все те же: DDoS-атаки, фишинг, вредоносные программы, взлом из-за уязвимостей в софте и подбор паролей, чтобы украсть учетные записи сотрудников и клиентов. Хорошо, что многие атаки удалось вовремя остановить благодаря машиночитаемым бюллетеням от Банка России, которые каждый день предупреждают о возможных угрозах.

Начиная с 2023 г. наблюдается изменение вектора кибератак в финансовом секторе – злоумышленники стали чаще нацеливаться не непосредственно на кредитные организации, а на их IT-поставщиков и сервисных провайдеров. Основной мотивацией подобных атак остается финансовый интерес, реализуемый через криптографические атаки (шифрование данных), нарушение работоспособности информационных систем и кражу конфиденциальной информации.

Примечательно, что, по данным Банка России, несмотря на рост числа инцидентов, не было зафиксировано атак с использованием принципиально новых сложных методик. Основной уязвимостью, которой продолжали пользоваться киберпреступники, стало несвоевременное обновление программного обеспечения в финансовых организациях. Это свидетельствует о том, что базовые меры кибергигиены по-прежнему остаются критически важным элементом защиты финансового сектора.

Анализ современных киберугроз свидетельствует, что наиболее эффективным методом противодействия хакерским атакам является своевременная ликвидация уязвимостей в программном обеспечении, что соответствует методическим рекомендациям ФСТЭК России и ФинЦЕРТ Банка России. В 2023 г. Департамент информационной безопасности Банка России опубликовал серию из трех аналитических бюллетеней, содержащих детализированный разбор актуальных атак и конкретные рекомендации по обеспечению информационной безопасности.

Эмпирические данные демонстрируют характерные паттерны поведения злоумышленников при успешном преодолении систем защиты. В большинстве случаев (50 %) целью атак становится хищение конфиденциальных данных для последующей коммерциализации через теневые каналы сбыта. Значительная доля инцидентов (15 %) связана с деструктивными действиями, выражающимися в несанкционированной модификации контента веб-ресурсов. Остальные случаи (35 %) приводят к нарушению функциональности критически важных систем, что вызывает существенные перебои в обслуживании клиентов финансовых организаций.

Полученные результаты подтверждают необходимость реализации комплексного подхода к кибербезопасности, включающего не только технические меры защиты, но и постоянный мониторинг угроз, систематическое обучение персонала и строгое соблюдение регламентов обновления программного обеспечения.

Основным рекомендационным решением по минимизации мошеннических операций и приравливания их к нулю является повышение финансовой грамотности населения страны, которое можно осуществить с посредством определенных мероприятий.

Интеграция финансовой грамотности в образовательные программы представляет собой перспективное направление повышения экономической осведомленности населения. Включение данного предмета в школьную программу, а также его введение в перечень дисциплин для сдачи единого государственного экзамена (ЕГЭ) по направлениям, связанным с управлением денежными ресурсами, способствует формированию системных знаний у будущих специалистов.

Важную роль в данном процессе играет поддержка некоммерческих организаций и общественных объединений, реализующих специализированные образовательные форумы и проекты. Государственное и частное финансирование таких инициатив способствует их масштабированию и повышению эффективности.

Регулирование правовой основы подразумевает в себе модернизацию законодательства, а именно Федеральный Закон № 395-1 «О банках и банковской деятельности», гл. 1, ст. 5 «Банковские операции и другие сделки кредитной организации», а также Федеральный Закон № 161-ФЗ «О национальной платежной системе», гл. 2, ст. 5. Дополнение двух законодательств в примере осуществления перевода денежных средств в размере свыше суммы 500 000 руб. за один раз – осуществление перевода непосредственно в банковском отделении по принципу «Из рук в руки». Но стоит учесть, что возможно создание

групп юридическим лицам, официально зарегистрированным, с возможностью получения лицензии на осуществление продаж, где товар имеет стоимостную оценку свыше 500 000 руб. [1, 2, 9].

Стимулирование финансовой ответственности включает в себя создание раздела на сайте ЦБ с возможностью направления письма о выявлении мошенника, предоставлении его информации, и в случае подтверждения осуществления выплаты лицу, сообщившему о нарушении.

Таблица 2 / Table 2

**Предположительная оценка решений по минимизации мошеннических операций / Prospective assessment of solutions to minimize fraudulent transactions**

Решение	Процент минимизации
Введение образовательных программ	≈2–3 %
Проведение информационных кампаний	≈1–2 %
Поддержка инициатив	≈3–5 %
Регулирование правовой основы	≈5–20 %
Стимулирование финансовой ответственности	≈2–3 %

\*Источник: составлено авторами / Source: compiled by the authors

Таким образом, средний уровень минимизации фрод-операций составит порядка 9 %, что существенно повлияет на объем операций, проведенных без согласия клиентов.

Отметим, что для реализации всех пяти решений, необходимо соблюдать ключевые принципы успешной реализации программ повышения финансовой грамотности:

- доступность: программы должны быть доступны для всех слоев населения, независимо от возраста, образования и уровня дохода;
- актуальность: информация должна быть актуальной и соответствовать текущей экономической ситуации и финансовому рынку;
- ясность: материалы должны быть изложены простым и понятным языком, следует избегать сложных терминов и аббревиатур;
- практичность: программы должны быть ориентированы на практическое применение полученных знаний и навыков;
- регулярность: повышение финансовой грамотности должно быть непрерывным процессом, а не разовой акцией;
- партнерство: успешная реализация программ требует сотрудничества между государственными органами, финансовыми организациями, образовательными учреждениями, общественными организациями и СМИ;
- оценка эффективности: необходимо регулярно оценивать эффективность реализуемых программ и вносить коррективы исходя из полученных результатов.

**Закключение / Conclusion.** Проведенный анализ научных источников по теме исследования, нормативных документов и методических материалов Центрального Банка Российской Федерации, свидетельствует о наличии устойчивой негативной динамики в сфере финансовой безопасности населения. Наблюдается системный рост как количественных показателей мошеннических операций, так и объема похищенных денежных средств. Параллельно фиксируется качественная трансформация методов противоправной деятельности, выражающаяся в усложнении схем социальной инженерии, технологическом совершенствовании инструментов кибермошенничества и расширении каналов несанкционированного доступа к финансовым ресурсам граждан.

С каждым годом информационные технологии совершенствуются – развивается машинное (искусственное) обучение техники, что играет ключевую роль и в безопасности финансовых ресурсов, и в их опасности.

Минимизировать риск мошеннических действий злоумышленников возможно путем развития регулярных информационных компаний, основанных на принципах многоканального распространения знаний и обеспечивающих широкий охват аудитории.

Одновременно с просветительскими мерами большое значение имеет внедрение технологических решений, направленных на противодействие мошенничеству. Использование систем искусственного интеллекта для анализа транзакций и выявления подозрительных операций позволит минимизировать риски несанкционированного доступа к средствам граждан. Комплексный подход, со-

четающий образовательные, информационные и технологические меры, способен существенно повысить уровень финансовой безопасности в долгосрочной перспективе.

## СПИСОК ИСТОЧНИКОВ

1. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 № 395-1. URL: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_5842/](https://www.consultant.ru/document/cons_doc_LAW_5842/)
2. Федеральный закон «О внесении изменений в Федеральный закон «О национальной платежной системе» от 24.07.2023 № 369-ФЗ. URL: <https://www.consultant.ru/>
3. Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций. URL: [https://cbr.ru/analytics/ib/operations\\_survey/2023/](https://cbr.ru/analytics/ib/operations_survey/2023/) (дата обращения 08.07.2025)
4. Круз Д. А., Брагина Г. Н. Финансовая безопасность как форма экономической безопасности // Наука через призму времени. 2023. № 4(73). С. 28–31. URL: [https://elibrary.ru/download/elibrary\\_50735018\\_37332284.pdf](https://elibrary.ru/download/elibrary_50735018_37332284.pdf)
5. Симонова В. В. Безопасность платежной и денежно-кредитной систем как часть финансовой безопасности государства // Исследование развития экосистем в цифровой экономике: сборник научных статей. Курск, 27 марта 2024 года. Курск: ЗАО «Университетская книга», 2024. С. 336–344. <http://doi.org/10.47581/2024.FK-04.Simonova-01>. URL: [https://elibrary.ru/download/elibrary\\_65594572\\_54289681.pdf](https://elibrary.ru/download/elibrary_65594572_54289681.pdf)
6. Робертс М. В. Повышение уровня финансовой грамотности в борьбе с финансовым мошенничеством // Финансовое просвещение: XXIV Всероссийская научно-практическая онлайн-конференция по финансовому просвещению в России: сборник материалов, Москва, 24–26 сентября 2024 года. М.: Ассоциация развития финансовой грамотности, 2024. С. 179–187. URL: [https://elibrary.ru/download/elibrary\\_80491666\\_68139321.pdf](https://elibrary.ru/download/elibrary_80491666_68139321.pdf)
7. Урядова О. А. Финансовое мошенничество как следствие цифровизации рынка финансовых продуктов и услуг // Умные технологии в современном мире: материалы VI Всероссийской научно-практической конференции, Южно-Уральский государственный университет (национальный исследовательский университет), 28–29 февраля 2024 года. Челябинск: Южно-Уральский государственный университет (национальный исследовательский университет), 2024. С. 79–85. URL: [https://elibrary.ru/download/elibrary\\_66998976\\_88713967.pdf](https://elibrary.ru/download/elibrary_66998976_88713967.pdf)
8. Балабанов А. И. Формы финансового мошенничества, влияющие на финансовое благополучие граждан // Архитектура финансов: трансформация в условиях новой многополярности: Сборник материалов XIII Международной научно-практической конференции, Санкт-Петербург, 10–13 апреля 2024 года. Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2024. С. 189–194. URL: [https://elibrary.ru/download/elibrary\\_80647157\\_21473519.pdf](https://elibrary.ru/download/elibrary_80647157_21473519.pdf)
9. Зеленев М. В. Особенности финансовой безопасности населения Российской Федерации // Современные проблемы экономики и управления и пути их решения: сборник материалов XII (69-й) ежегодной научно-практической конференции преподавателей, студентов и молодых ученых Северо-Кавказского федерального университета, Ставрополь, 14–27 апреля 2025 года. Ставрополь: Северо-Кавказский федеральный университет, 2025. С. 292–294. URL: <https://www.elibrary.ru/item.asp?id=82645174>
10. Асеев О. В., Сайымова М. Д., Богданова Е. А. Применение технологии блокчейн для управление рисками информационной безопасности в электронной банковской системе // Вестник Северо-Кавказского федерального университета. 2023. № 4(97). С. 39–47. <http://doi.org/10.37493/2307-907X.2023.4.4>. URL: <https://www.elibrary.ru/item.asp?id=54523100>.

## REFERENCES

1. Federal Law «On Banks and Banking Activities» dated 02.12.1990 N 395-1. Available from: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_5842/](https://www.consultant.ru/document/cons_doc_LAW_5842/) (In Russ.).
2. Federal Law «On Amendments to the Federal Law «On the National Payment System» dated 24.07.2023 N 369-FL. Available from: <https://www.consultant.ru/>
3. Overview of transactions conducted without the voluntary consent of financial institution customers. Available from: [https://cbr.ru/analytics/ib/operations\\_survey/2023/](https://cbr.ru/analytics/ib/operations_survey/2023/) (accessed on 08.07.2025). (In Russ.).
4. Kuts DA, Bragina GN. Financial Security as a Form of Economic Security / D. A. Kuts, // Science through the Prism of Time. 2023;4(73):28-31. Available from: [https://elibrary.ru/download/elibrary\\_50735018\\_37332284.pdf](https://elibrary.ru/download/elibrary_50735018_37332284.pdf) (In Russ.).
5. Simonova VV. Security of the payment and monetary and credit systems as part of the financial security of the state. Research of the development of ecosystems in the digital economy : collection of scientific articles, Kursk, March 27, 2024. Kursk: ZAO Universitetskaya Kniga; 2024. P. 336-344. <http://doi.org/10.47581/2024.FK-04.Simonova-01>. Available from: [https://elibrary.ru/download/elibrary\\_65594572\\_5428/](https://elibrary.ru/download/elibrary_65594572_5428/) (In Russ.).
6. Roberts MV. Improving Financial Literacy in the Fight Against Financial Fraud. Financial Education: The 14th All-Russian Scientific and Practical Online Conference on Financial Education in Russia. Collection of Materials, Moscow, September 24-26, 2024. Moscow: Financial Literacy Development Association; 2024. P. 179-187. Available from: [https://elibrary.ru/download/elibrary\\_80491666\\_68139321.pdf](https://elibrary.ru/download/elibrary_80491666_68139321.pdf) (In Russ.).
7. Uryadova OA. Financial Fraud as a Result of the Digitalization of the Financial Products and Services Market. Smart Technologies in the Modern World : Proceedings of the 6th All-Russian Scientific and Practical Conference, South Ural State University (National Research University), February 28-29, 2024. Chelyabinsk: South Ural State University (Na-



- tional Research University); 2024. P. 79-85. Available from: [https://elibrary.ru/download/elibrary\\_66998976\\_88713967.pdf/](https://elibrary.ru/download/elibrary_66998976_88713967.pdf/) (In Russ.).
8. Balabanov AI. Forms of Financial Fraud that Affect the Financial Well-Being of Citizens. Architecture of Finance: Transformation in the Context of a New Multipolarity: Collection of Materials from the XIII International Scientific and Practical Conference, St. Petersburg, April 10-13, 2024. Saint Petersburg: St. Petersburg State University of Economics; 2024. P. 189-194. Available from: [https://elibrary.ru/download/elibrary\\_80647157\\_21473519.pdf/](https://elibrary.ru/download/elibrary_80647157_21473519.pdf/) (In Russ.).
  9. Zelenov MV. Features of the Financial Security of the Population of the Russian Federation. Modern Problems of Economics and Management and Their Solutions: Collection of Materials from the XII (69) Annual Scientific and Practical Conference of Teachers, Students, and Young Scientists of the North-Caucasus Federal University, Stavropol, April 14-27, 2025. Stavropol: North-Caucasus Federal University; 2025. P. 292-294. Available from: <https://www.elibrary.ru/item.asp?id=82645174/> (In Russ.).
  10. Aseev OV, Sayymova MD, Bogdanova EA. Application of blockchain technology for managing information security risks in the electronic banking system. Newsletter of North-Caucasus Federal University. 2023;4(97):39-47. <http://doi.org/10.37493/2307-907X.2023.4.4>. Available from: <https://www.elibrary.ru/item.asp?id=54523100/> (In Russ.).

### ИНФОРМАЦИЯ ОБ АВТОРАХ

**Эльвира Анцассовна Русецкая** – доктор экономических наук, профессор, Северо-Кавказский федеральный университет, Scopus ID: 57000386000; Researcher ID: Y-5511-2018

**Максим Владимирович Зеленев** – студент 4-го курса, направления подготовки 38.03.01 Экономика, направленность (профиль) «Финансы», Северо-Кавказский федеральный университет, Researcher ID: NTQ-2807-2025

**Эллина Владимировна Ключкова** – студент 2-го курса, направления подготовки 38.04.08 Финансы и кредит, направленность (профиль) «Финансы устойчивого развития», Северо-Кавказский федеральный университет, Researcher ID: JXX-4186-2024

**Елена Александровна Нейман** – студент 4-го курса, направления подготовки 38.03.01 Экономика, направленность (профиль) «Финансы», Северо-Кавказский федеральный университет, Researcher ID: NTQ-2825-2025

### ВКЛАД АВТОРОВ

**Эльвира Анцассовна Русецкая**

Подготовка и редактирование текста – формирование его окончательного варианта. Утверждение окончательного варианта – принятие ответственности за все аспекты работы, целостность всех частей статьи и ее окончательный вариант.

**Максим Владимирович Зеленев**

Проведение исследования – сбор, интерпретация и анализ полученных данных.

**Эллина Владимировна Ключкова**

Подготовка и редактирование текста, составление черновика рукописи, участие в научном дизайне.

**Елена Александровна Нейман**

Разработка рекомендательных мер и анализ последствий.

### INFORMATION ABOUT THE AUTHORS

**Elvira A. Rusetskaya** – Dr. Sci. (Econ.), Professor, North-Caucasus Federal University, Scopus ID: 57000386000; Researcher ID: Y-5511-2018.

**Maxim V. Zelenov** – 4th year Student of the Direction of Preparation 38.03.01 Economics Orientation (profile) «Finance», North-Caucasus Federal University, Researcher ID: NTQ-2807-2025.

**Ellina V. Klochkova** – 2th year Student of the Direction of Preparation 38.04.08 Finance and credit Orientation (profile) «Sustainable development finance», North-Caucasus Federal University, Researcher ID: JXX-4186-2024.

**Elena A. Neiman** – 4th year Student of the Direction of Preparation 38.03.01 Economics Orientation (profile) «Finance», North-Caucasus Federal University, Researcher ID: Researcher ID: NTQ-2825-2025.

### CONTRIBUTION OF THE AUTHORS

**Elvira A. Rusetskaya**

Preparation and editing of the text – formation of its final version. Approval of the final version – acceptance of responsibility for all aspects of the work, the integrity of all parts of the article, and its final version.

**Maxim V. Zelenov**

Conducting research – collecting, interpreting, and analyzing the obtained data.

**Ellina V. Klochkova**

Preparation and editing of the text, drafting of the manuscript, and participation in scientific design.

**Elena A. Neiman**

Preparation and editing of the text, drafting of the manuscript, and participation in scientific design.