

Международный научно-исследовательский журнал

«Прогрессивная экономика»

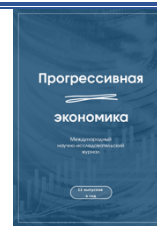
№ 10 / 2026 https://progressive-economy.ru/vypusk_1/czifrovoe-moshennichestvo-kak-ugroza-ekonomicheskoy-bezopasnosti-rossii-problema-izmereniya-ushherba-i-ocenka-effektivnosti-mer-protivodejstviya/

Научная статья / Original article

Шифр научной специальности ВАК: 5.2.3

УДК 338.24:004.738.5

DOI: 10.54861/27131211_2026_10_497



ЦИФРОВОЕ МОШЕННИЧЕСТВО КАК УГРОЗА ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ: ПРОБЛЕМА ИЗМЕРЕНИЯ УЩЕРБА И ОЦЕНКА ЭФФЕКТИВНОСТИ МЕР ПРОТИВОДЕЙСТВИЯ

Меньшов В.Н., МИРЭА – Российский технологический университет, вице-президент ООО «Промсельхозбанк», г. Москва, Россия

119454, Москва, пр-т Вернадского, д. 78

ORCID: <https://orcid.org/0009-0003-5609-7710>

e-mail: menshov@mirea.ru

Аннотация. Цифровизация экономики сопровождается ростом дистанционного мошенничества, которое становится фактором экономической безопасности, однако его масштаб оценивается ведомствами по несопоставимым методикам. Целью статьи является оценка ущерба от цифрового мошенничества в России в 2024–2025 гг. с учетом межведомственных расхождений и обоснование направлений совершенствования мониторинга экономической безопасности. Гипотеза исследования состоит в том, что платежная статистика систематически занижает масштаб угрозы, а потери смещаются в каналы, не охватываемые банковским контролем. Научная новизна заключается в разработке трехконтурной модели измерения ущерба (платежный, уголовно-правовой и совокупный экономический контуры) и системы коэффициентов предотвращения, возмещения и статистического покрытия. Методы исследования: сравнительный и структурный анализ, расчет относительных показателей, триангуляция данных Банка России, МВД России, Генеральной прокуратуры, Росстата, НИУ ВШЭ и ПАО Сбербанк, сопоставление с данными Великобритании и США. Получены следующие результаты: оценки ущерба за 2025 г. различаются почти на порядок – от 29,3 до 275–295 млрд руб. (0,014–0,14% ВВП); платежная статистика отражает около 10% совокупных потерь; при предотвращении банками около 99,8% попыток хищений по объему пострадавшим возмещается лишь 5,9% похищенного. Гипотеза подтверждена: снижение показателей платежного контура сопровождается миграцией хищений в каналы, не охватываемые платежной статистикой. Практическая значимость состоит в возможности использования предложенных индикаторов органами власти и Банком России при мониторинге экономической безопасности. Перспективы исследования связаны с оценкой косвенных потерь, расходов на защиту и угроз, связанных с применением технологий искусственного интеллекта.



Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.

Ключевые слова: экономическая безопасность, цифровая экономика, кибермошенничество, антифрод, латентный ущерб, дропперство, ГИС «Антифрод».

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Для цитирования: Меньшов В.Н. Цифровое мошенничество как угроза экономической безопасности России: проблема измерения ущерба и оценка эффективности мер противодействия // Прогрессивная экономика. 2026. № 10. С. 497–514. https://doi.org/10.54861/27131211_2026_10_497.

Статья поступила в редакцию: 17.09.2026 г. Одобрена после рецензирования: 21.10.2026 г. Принята к публикации: 26.10.2026 г.

DIGITAL FRAUD AS A THREAT TO RUSSIA'S ECONOMIC SECURITY: THE PROBLEM OF MEASURING LOSSES AND ASSESSING THE EFFECTIVENESS OF COUNTERMEASURES

*Menshov V.N., MIREA – Russian Technological University, Moscow, Russia;
Vice President, Industrial Agricultural Bank Limited
119454, Moscow, Vernadsky Ave., 78
ORCID: <https://orcid.org/0009-0003-5609-7710>
e-mail: menshov@mirea.ru*

Abstract. The digitalization of the economy is accompanied by the growth of remote fraud, which is becoming an economic security factor, while its scale is assessed by agencies using incomparable methods. The purpose of the article is to estimate losses from digital fraud in Russia in 2024–2025, taking into account interagency discrepancies, and to substantiate ways to improve economic security monitoring. The hypothesis is that payment statistics systematically underestimate the threat, and losses shift to channels not covered by bank control. The scientific novelty lies in a three-contour loss measurement model (payment, criminal-law and aggregate economic contours) and a system of prevention, reimbursement and statistical coverage ratios. Methods: comparative and structural analysis, relative indicators, triangulation of data from the Bank of Russia, the Ministry of Internal Affairs, the Prosecutor General's Office, Rosstat, HSE University and Sberbank, comparison with UK and US data. Results: estimates of losses for 2025 differ by almost an order of magnitude, from RUB 29.3 billion to RUB 275–295 billion (0.014–0.14% of GDP); payment statistics reflect about 10% of aggregate losses; banks prevent about 99.8% of attempted thefts by volume, but only 5.9% of stolen funds are reimbursed. The practical significance lies in the possibility of using the proposed indicators by public authorities and the Bank of Russia for economic security monitoring. Research prospects include assessing indirect losses, protection costs and threats related to artificial intelligence.

Keywords: economic security, digital economy, cyber fraud, anti-fraud, latent losses, money mules, Antifraud state information system.



JEL classification: K42, G21, O33, H56.

Conflict of interest. The author declares that there is no conflict of interest.

For citation: Menshov V.N. (2026). Tsifrovoe moshennichestvo kak ugroza ekonomicheskoi bezopasnosti Rossii: problema izmereniya ushcherba i otsenka effektivnosti mer protivodeistviya [Digital fraud as a threat to Russia's economic security: the problem of measuring losses and assessing the effectiveness of countermeasures]. *Progressivnaya ekonomika* [Progressive Economy], 10, 497–514. https://doi.org/10.54861/27131211_2026_10_497. (In Russ., abstract in Eng.)

The article was submitted to the editorial office: 17/09/2026. Approved after review: 21/10/2026. Accepted for publication: 26/10/2026.

Введение

Цифровая трансформация стала одним из ключевых источников экономического роста России. По оценке ИСИЭЗ НИУ ВШЭ, валовые внутренние затраты на развитие цифровой экономики в 2024 г. достигли 6,7 трлн руб. (+22% к 2023 г. в текущих ценах), а их отношение к ВВП выросло с 3,1 до 3,3% [1]; по предварительным данным за 2025 г., затраты составили около 7,1 трлн руб. при замедлении прироста до 6,5% [2]. Вместе с тем расширение безналичных расчетов, дистанционного банковского обслуживания, маркетплейсов и мессенджеров формирует новую поверхность атаки для преступной деятельности. По данным Генеральной прокуратуры, преступления, совершаемые с использованием информационно-телекоммуникационных технологий (ИТТ), составляют около 38% в общей структуре преступности [3], а основная их часть приходится на дистанционные хищения. Данные статистики позволяют рассматривать цифровое мошенничество как угрозу экономической безопасности в смысле Стратегии экономической безопасности Российской Федерации, определяющей ее как состояние защищенности национальной экономики от внешних и внутренних угроз [4].

Ключевая проблема состоит в том, что ущерб от цифрового мошенничества измеряется разными институтами по разным правилам: Банк России учитывает безналичные операции без добровольного согласия клиентов, МВД России – ущерб по зарегистрированным преступлениям, а участники рынка оценивают и латентные потери. В перечне из 40 показателей состояния экономической безопасности эта угроза отражена лишь косвенно – через общий «уровень преступности в сфере экономики» [4].

Таким образом, целью статьи является оценка масштаба и динамики ущерба от цифрового мошенничества в России в 2024–2025 гг. с учетом межведомственных расхождений и обоснование направлений совершенствования мониторинга и мер противодействия в системе обеспечения экономической безопасности. Задачи исследования:



систематизировать подходы к оценке потерь от киберпреступности; сопоставить официальные и отраслевые оценки ущерба; оценить результативность институциональных мер; сравнить российскую ситуацию с данными Великобритании и США; сформулировать предложения по развитию системы индикаторов.

Обзор литературы

В исследованиях экономической безопасности в условиях цифровизации сложились три направления. Первое связано с осмыслением цифровых угроз в общей системе экономической безопасности. Г.Н. Мустафина классифицирует угрозы процессу цифровизации предприятий на внешние и внутренние, относя к внешним недостаточную цифровую грамотность населения и несовершенство механизмов защиты данных [5]. Л.А. Бурдина обосновывает, что информационная компонента экономической безопасности выходит на первый план по сравнению с материальной [6], а О.Б. Скрипник относит кибербезопасность к ключевым цифровым рискам, поскольку цифровизация увеличивает число объектов атак [7]. А.К. Мухамадиярова и соавторы, сопоставляя выгоды и затраты цифровизации, приходят к выводу о стратегическом характере сопутствующих рисков [8]. Эти работы корректно фиксируют значимость угрозы, но носят преимущественно классификационный характер и не предлагают количественных индикаторов, пригодных для мониторинга.

Второе направление посвящено угрозам финансовому сектору. Г.В. Семеко показала, что в 2019 г. объем хищений с использованием электронных средств платежа превысил 6,4 млрд руб., а банки возместили клиентам около 15% похищенного [9]. Н.В. Щербакова связала опережающую цифровизацию банковского сектора с ростом числа несанкционированных операций по картам с 260,9 тыс. в 2015 г. до 416,9 тыс. в 2018 г. [10]. П.В. Ревенков, К.Р. Ошманкевич и А.А. Бердюгин детально описали фишинговые схемы и обосновали задачи регулирования, акцентируя внимание на киберграмотности населения [11]. П.С. Насонова рассматривает информационную безопасность как условие финансовой безопасности в экономике данных и указывает, что доля расходов на нее в ИТ-бюджетах российских финансовых компаний (5%) ниже мирового уровня (8–10%) [12]. С.Л. Ларионова предложила оценивать эффективность противодействия мошенничеству в кредитной организации системой коэффициентов по числу и обороту выявленных и приостановленных операций [13], а Д.А. Степаненко рассматривает антифрод как криминалистическое средство предупреждения преступлений [14]. Вместе с тем эти работы анализируют уровень отдельного банка и не оценивают, какая доля совокупных потерь граждан попадает в поле зрения банковских систем.

Третье направление связано с инфраструктурой мошенничества и уголовно-правовыми мерами. С.Л. Кисленко и А.Д. Фокин рассматривают

мошенничество с использованием ИТТ как угрозу национальной безопасности и оценивают хищения в 2024 г. в 250–300 млрд руб. [15]. А.Н. Калужный приводит рост числа зарегистрированных преступлений по ст. 187 УК РФ с 366 в 2021 г. до 2096 в 2024 г. и указывает на противоречивость судебной практики [16]. А.В. Богданов, И.Н. Волосевич и Е.Н. Хазов оценивают численность дропов в России в 0,5–2 млн человек [17], а Ю.И. Антонов и А.Д. Костиков показывают, что новые ч. 3–6 ст. 187 УК РФ не охватывают токенизированные карты и средства платежа иностранных банков [18]. Наиболее близка к теме настоящего исследования работа А.Н. Литвиненко и Л.А. Гузиковой, указывающих на несогласованность понятий и статистики, различие темпов прироста похищенных средств по разным источникам и необходимость оценивать меры противодействия с экономических позиций [19]. Однако авторы ограничиваются констатацией расхождений, не предлагая способа их согласования.

В зарубежной литературе Р. Андерсон и соавторы разработали рамку измерения стоимости киберпреступности, разделяющую прямые и косвенные потери и расходы на защиту, и показали, что последние могут многократно превышать прямой ущерб [20]. Модель Л. Гордона и М. Лоэба обосновывает зависимость оптимальных инвестиций в информационную безопасность от величины ожидаемых потерь [21], что делает точность оценки ущерба условием рационального распределения ресурсов.

Анализ научных источников показал, что проблема межведомственных расхождений в оценке ущерба от цифрового мошенничества и ее последствия для мониторинга экономической безопасности систематически не исследованы. Восполнению этого пробела посвящена настоящая статья.

Материалы и методы

Методологическую основу исследования составляют положения теории экономической безопасности и подход к измерению стоимости киберпреступности [20]. Информационную базу составили обзор операций без добровольного согласия клиентов и итоги работы Банка России за 2025 г. [22; 23], данные МВД России и Генеральной прокуратуры [3; 24; 25], данные Росстата о ВВП [26], материалы НИУ ВШЭ [1], оценка ПАО Сбербанк [27], отчеты FBI и UK Finance [28; 29], нормативные правовые акты [4; 30; 31]. Период анализа – 2024–2025 гг.: с 25 июля 2024 г. в число операций без согласия включены переводы, совершенные клиентом вследствие обмана или злоупотребления доверием [32], поэтому более ранние ряды несопоставимы.

Использованы методы сравнительного и структурного анализа, расчет относительных показателей и триангуляция источников. Для упорядочения оценок предложена трехконтурная модель измерения ущерба:

– контур 1 (платежный) – безналичные операции без добровольного согласия клиента, фиксируемые операторами по переводу денежных средств и Банком России;



– контур 2 (уголовно-правовой) – материальный ущерб по зарегистрированным преступлениям с использованием ИТТ, включая случаи передачи наличных;

– контур 3 (совокупный экономический) – общие потери граждан, включая латентные случаи, не ставшие предметом заявлений в банк или полицию.

Для оценки результативности мер рассчитаны коэффициент предотвращения по объему:

$$K_{\Pi} = \frac{V_{\text{пред}}}{V_{\text{пред}} + V_{\text{хищ}}}$$

где $V_{\text{пред}}$ – объем предотвращенных операций, $V_{\text{хищ}}$ – объем хищений; аналогичный коэффициент по количеству операций;

Коэффициент возмещения:

$$K_{\text{В}} = V_{\text{возвр}}/V_{\text{хищ}}$$

где $V_{\text{возвр}}$ – объем возвращенных средств;

Коэффициент статистического покрытия:

$$K_{\text{с}} = \frac{V_i}{V_{\text{сов}}}$$

где V_i – оценка i -го контура, $V_{\text{сов}}$ – середина интервала совокупной оценки (285 млрд руб.). Относительный масштаб ущерба рассчитан к номинальному ВВП 2025 г. (213,5 трлн руб. [26]) и к затратам на цифровую экономику (7,1 трлн руб. [2]). Расчетные показатели выполнены автором.

Результаты и обсуждение

Данные за 2024–2025 гг. демонстрируют разнонаправленную динамику (табл. 1). В платежном контуре объем операций без согласия клиентов вырос на 6,4% – до 29,3 млрд руб., а их количество – на 31,2%, до 1,6 млн [22; 23]. В уголовно-правовом контуре число зарегистрированных киберпреступлений снизилось примерно на 12%, а материальный ущерб – с 205 до 189,5 млрд руб. [24].

Таблица 1

Ключевые показатели цифрового мошенничества в России в 2024–2025 гг.

Table 1

Key indicators of digital fraud in Russia in 2024–2025

Показатель	2024 г.	2025 г.	Изменение
Платежный контур (Банк России)			
Объем операций без согласия клиентов, млрд руб.	27,5	29,3	+6,4%
Количество операций без согласия, млн	1,2	1,6	+31,2%
Средняя сумма операции (физлица), тыс. руб.	22,9	18,6	–18,8%*
Доля возвращенных средств, %	9,9	5,9	–4,0 п.п.
Объем предотвращенных операций, трлн руб.	13,5	13,9	+2,9%*
Количество предотвращенных операций, млн	72,2	134,2	+85,9%*
Доля в общем объеме переводов, %	0,00066	0,00071	+0,00005 п.п.
Уголовно-правовой контур (МВД России)			
Зарегистрировано киберпреступлений, тыс.	775	663	–12%
в т.ч. мошенничеств, тыс.	378	344	–9%
в т.ч. краж, тыс.	105	80	–23,8%
Материальный ущерб, млрд руб.	205	189,5	–7,6%*
Число потерпевших, тыс. чел.	565,6*	534,5	–5,5%

* По более поздним данным МВД и Генеральной прокуратуры за 2025 г. – 675,4 тыс. преступлений и 195 млрд руб. ущерба [3; 25].

Источник: расчеты автора по данным [22; 23; 24]

Source: the author's calculations based on the data [22; 23; 24]

Разнонаправленность не означает ослабления угрозы. Рост количества операций в платежном контуре частично объясняется институциональными изменениями: с октября 2025 г. крупные банки обязаны предоставлять клиентам функцию оперативного сообщения о мошеннической операции, что повысило выявляемость инцидентов [22]. Снижение средней суммы операции с 22,9 до 18,6 тыс. руб. указывает на дробление хищений – адаптацию злоумышленников к лимитам и антифрод-правилам. Средний ущерб на одного потерпевшего в уголовно-правовом контуре (189,5 млрд руб. / 534,5 тыс. чел. $\approx$ 355 тыс. руб.) примерно в 19 раз превышает среднюю сумму операции в платежном контуре, что свидетельствует о концентрации крупных потерь в схемах социальной инженерии, где жертва многократно переводит средства или передает наличные. Сопоставление трех оценок за 2025 г. представлено в табл. 2 и на рис. 1.

Таблица 2

**Оценки ущерба от цифрового мошенничества в России за 2025 г. в
трехконтурной модели**

Table 2

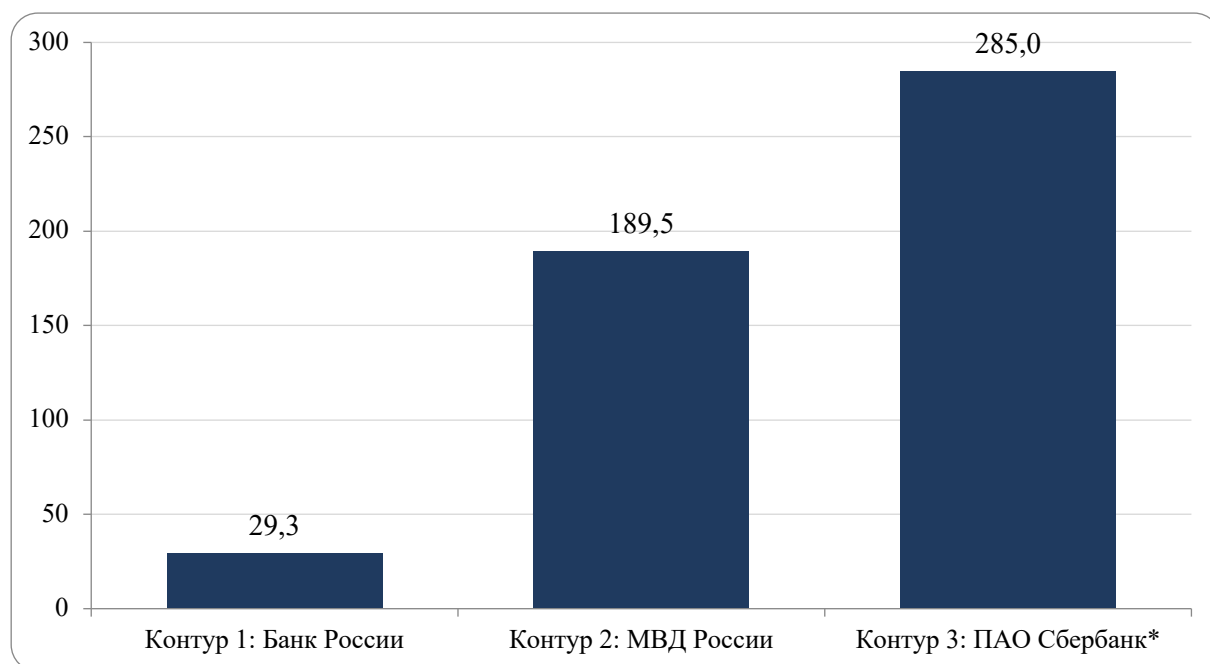
**Estimates of losses from digital fraud in Russia in 2025 in the three-contour
model**

Контур (источник)	Ущерб, млрд руб.	% ВВП*	% затрат на цифровую экономику*	Кратность к контуру 1*	Кс*, %
1. Платежный (Банк России)	29,3	0,014	0,41	1,0	10,3
2. Уголовно-правовой (МВД России)	189,5	0,089	2,67	6,5	66,5
3. Совокупный (ПАО Сбербанк)	275–295	0,13– 0,14	3,9–4,2	9,4–10,1	100

* для Кс использована середина интервала контура 3 (285 млрд руб.)

Источник: составлено автором по данным [2; 22; 24; 26; 27]

Source: compiled by the author based on [2; 22; 24; 26; 27]



* середина интервала 275–295 млрд руб.

**Рис. 1. Оценки ущерба от цифрового мошенничества в России в 2025 г.
по контурам измерения, млрд руб.**

Источник: составлено автором по данным [22; 24; 27]

**Fig. 1. Estimates of losses from digital fraud in Russia in 2025 by
measurement contour, RUB billion**

Source: compiled by the author based on [22; 24; 27]



Расхождение между контурами достигает порядка величины: платежная статистика охватывает лишь около 10% совокупных потерь. При этом оценки внутренне согласованы. По данным ПАО Сбербанк, 30–40% потерь не попадает ни в какую официальную статистику [27]; расчетное покрытие уголовно-правового контура составляет 64–69% от интервала 275–295 млрд руб., т.е. латентная часть оценивается в 31–36%, что соответствует заявленному интервалу. Разница между контурами 1 и 2 объясняется тем, что Банк России учитывает только безналичные переводы, тогда как в правоохранительную статистику попадают передача наличных, перевод кредитных средств и средств от продажи имущества [27]. Следовательно, сокращение показателей платежного контура может сопровождаться не уменьшением потерь, а их миграцией в каналы, не охватываемые платежной статистикой, и использование только данных Банка России систематически занижает масштаб угрозы. Тем самым гипотеза исследования подтверждается.

Расчеты коэффициентов результативности мер, развивающих подход С.Л. Ларионовой [13] на уровне всей платежной системы, приведены в табл. 3.

Таблица 3

**Показатели результативности мер противодействия цифровому
мошенничеству**

Table 3

Indicators of the effectiveness of digital fraud countermeasures

Показатель	2024 г.	2025 г.
Коэффициент предотвращения по объему Кп, %	99,80	99,79
Коэффициент предотвращения по количеству операций, %	98,37	98,82
Коэффициент возмещения банками Кв, %	9,9	5,9
Возмещено по линии правоохранительных органов, млрд руб.	8	13
Похищенные кредитные средства у клиентов крупных банков, млрд руб.	12,8*	7,8

Источник: составлено автором по данным [22; 23; 25]

Source: compiled by the author based on [22; 23; 25]

Банки предотвратили 134,2 млн мошеннических операций на 13,9 трлн руб. [23], однако коэффициент предотвращения по объему остается на плато около 99,8%: по оценке регулятора, злоумышленникам в среднем достается 7 копеек из каждых 10 тыс. руб. переводов [23]. Дальнейшее наращивание защиты исключительно на стороне банков дает убывающую предельную отдачу, что согласуется с логикой модели Гордона – Лоэба [21]. Адресные меры оказались результативнее: объем похищенных кредитных средств у



клиентов крупных банков сократился на 39,2%, до 7,8 млрд руб., а их доля в мошеннических операциях – с 37 до 18% [23]; применение ст. 115.2 УПК РФ о приостановлении операций позволило увеличить возмещение ущерба по линии правоохранительных органов с 8 до 13 млрд руб. [25]. Вместе с тем коэффициент возмещения банками снизился с 9,9 до 5,9% (в 2019 г., по данным Г.В. Семяко, он составлял около 15% [9]), т.е. основное бремя потерь несут домохозяйства.

Расширен нормативный контур. Федеральный закон от 24.06.2025 № 176-ФЗ дополнил ст. 187 УК РФ ч. 3–6, установив самостоятельную ответственность за дропперство [31], однако, как показывают Ю.И. Антонов и А.Д. Костиков, новая норма содержит пробелы [18]. Федеральный закон от 01.04.2025 № 41-ФЗ предусмотрел создание государственной информационной системы противодействия правонарушениям с использованием ИКТ (ГИС «Антифрод»), участниками которой являются органы власти, Банк России, кредитные организации и операторы связи [30]. Тем самым осуществляется переход от банкоцентричной модели защиты к межотраслевой, затрагивающей звенья, где начинается большинство схем социальной инженерии. Прямое международное сопоставление абсолютных величин затруднено различиями в методологии учета, поэтому сравнение проводится по структуре и динамике (табл. 4).

Таблица 4

Сравнительная характеристика потерь от мошенничества в России, Великобритании и США за 2025 г.

Table 4

Comparative characteristics of fraud losses in Russia, the UK and the USA in 2025

Параметр	Россия	Великобритания	США
Источник и охват	Банк России: операции без согласия клиентов	UK Finance: платежное мошенничество	FBI IC3: заявления о киберпреступлениях
Объем потерь	29,3 млрд руб.	1,28 млрд ф. ст.	20,9 млрд долл.
Динамика к 2024 г.	+6,4%	+4%	+26%
Структурный сдвиг	Рост социальной инженерии, смещение в наличные	Несанкционированное –5%, APP +19%	85% потерь – мошенничество с использованием киберсредств
Возмещение пострадавшим	5,9%	61% по APP-мошенничеству	Нет единого механизма

Источник: составлено автором по данным [22; 28; 29]

Source: compiled by the author based on [22; 28; 29]



Общей тенденцией является переход от несанкционированных хищений к переводам, совершаемым самой жертвой под влиянием обмана: в Великобритании убытки от несанкционированного мошенничества снизились на 5%, а от АРР-мошенничества (authorised push payment) выросли на 19% [29]. Принципиальное различие – модель распределения потерь: британский режим обязательного возмещения обеспечил возврат 61% потерь от АРР-мошенничества [29], тогда как в России коэффициент возмещения составляет 5,9%. В США отмечен рост мошенничества с использованием криптовалют (11,4 млрд долл.) и технологий искусственного интеллекта (около 0,9 млрд долл.) [28], что задает ориентиры для прогнозирования угроз в российских условиях.

С позиций рамки Р. Андерсона и соавторов [20] прямые потери являются лишь частью стоимости киберпреступности: к ним следует добавить расходы на защиту и косвенные потери – снижение доверия к дистанционным каналам и ошибочные блокировки добросовестных клиентов. На противоречие между безопасностью и удобством пользователей указывают и А.Н. Литвиненко и Л.А. Гузикова [19]. Поэтому объем «предотвращенных» операций, включающий повторные попытки и ложные срабатывания, некорректно интерпретировать как сбереженную стоимость. Соотношение совокупных потерь с затратами на цифровую экономику (около 4%) показывает, что ущерб уже сопоставим со значимой долей инвестиций в цифровизацию. Ограничения исследования связаны с коротким сопоставимым периодом и непубличностью методики оценки ПАО Сбербанк.

На основе полученных результатов предлагаются следующие меры:

- дополнить мониторинг экономической безопасности частными индикаторами «совокупные потери от цифрового мошенничества, % ВВП», «коэффициент возмещения» и «коэффициент статистического покрытия»; в качестве ориентира порогового значения совокупных потерь можно рассматривать 0,1% ВВП;

- сформировать единую межведомственную методику учета ущерба на базе ГИС «Антифрод» со сверкой данных Банка России, МВД России и операторов связи и выборочными обследованиями населения для оценки латентной части;

- ввести долевую ответственность банка отправителя, банка получателя, оператора связи и цифровой платформы по аналогии с британским режимом возмещения;

- обеспечить раскрытие доли ложных срабатываний антифрод-систем для оценки баланса между защитой и доступностью финансовых услуг.

Заключение

В процессе исследования автором было выявлено, что масштаб угрозы цифрового мошенничества для экономической безопасности России существенно зависит от контура измерения. Предложенная трехконтурная модель позволила упорядочить оценки за 2025 г.: 29,3 млрд руб. в платежном контуре, 189,5 млрд руб. в уголовно-правовом и 275–295 млрд руб. в совокупном экономическом, т.е. от 0,014 до 0,14% ВВП. Платежная статистика отражает около 10% совокупных потерь, латентная часть составляет 31–40%.

Банковские антифрод-системы достигли высокой результативности, однако их предельная отдача снижается, а потери смещаются в наличный и небанковские каналы. Адресные меры дают измеримый эффект, но коэффициент возмещения пострадавшим остается низким. Научная новизна работы заключается в разработке трехконтурной модели измерения ущерба и системы коэффициентов предотвращения, возмещения и статистического покрытия. Практическая значимость состоит в возможности использования предложенных индикаторов органами власти, Банком России и кредитными организациями. Перспективы дальнейших исследований связаны с оценкой косвенных потерь и расходов на защиту, а также угроз, связанных с технологиями искусственного интеллекта и цифровыми активами.

Литература

1. Динамика затрат на развитие цифровой экономики // ИСИЭЗ НИУ ВШЭ. URL: <https://issek.hse.ru/mirror/pubs/share/1132489160.pdf>.
2. Рост цифровых инвестиций в России замедляется // Кабельщик. URL: <https://www.cableman.ru/content/rost-tsifrovyykh-investitsii-v-rossii-zamedlyaetsya>.
3. Число IT-преступлений в России в 2025 году сократилось до 675 тыс. // ТАСС. URL: <https://tass.ru/obschestvo/26385451>.
4. Указ Президента РФ от 13.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // ГАРАНТ.РУ. URL: <https://www.garant.ru/products/ipo/prime/doc/71572608/>.
5. Мустафина Г.Н. Актуальные угрозы экономической безопасности процесса цифровизации предприятий и механизмы их нейтрализации // Вестник экономики, права и социологии. 2025. № 3. С. 85–89.
6. Бурдина Л.А. К вопросу об экономической безопасности предприятия: ключевые риски и угрозы в современном мире // Современная конкуренция. 2025. Т. 19. № 5. С. 90–107.
7. Скрипник О.Б. Управление цифровыми рисками в современной экономике // Вестник евразийской науки. 2024. Т. 16. № 1.



8. Мухамадиярова А.К., Абрамова С.Р., Редников Д.В. Влияние цифровизации на экономическую безопасность государства через оценку выгод и затрат // Дискуссия. 2025. № 7 (140). С. 140–145.
9. Семеко Г.В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. 2020. № 1. С. 77–96.
10. Щербакова Н.В. Цифровые технологии в банковском секторе РФ: особенности и сопутствующие угрозы // Вестник Кемеровского государственного университета. Серия: Политические, социологические и экономические науки. 2021. Т. 6. № 1. С. 136–146.
11. Ревенков П.В., Ошманкевич К.Р., Бердюгин А.А. Фишинговые схемы в банковской сфере: рекомендации пользователям интернета по защите и разработка задач регулирования // Финансы: теория и практика. 2021. Т. 25. № 6. С. 212–226.
12. Насонова П.С. Правовое обеспечение информационной безопасности в финансовой сфере // Уральский журнал правовых исследований. 2024. № 3. С. 38–48.
13. Ларионова С.Л. Организация работы по борьбе с мошенничеством в кредитной организации // Вопросы безопасности. 2022. № 4. С. 15–26.
14. Степаненко Д.А. Антифрод как криминалистическое средство предупреждения преступлений в банковской сфере // Дискуссия. 2024. Вып. 122. С. 128–138.
15. Кисленко С.Л., Фокин А.Д. Мошенничество с использованием информационно-телекоммуникационных технологий как угроза национальной безопасности Российской Федерации // European and Asian Law Review. 2025. Т. 8. № 1. С. 41–54.
16. Калюжный А.Н. Способы преступной деятельности дропперов: криминалистический и уголовно-правовой подходы // Вестник Санкт-Петербургского университета. Право. 2026. Т. 17. № 1. С. 156–173.
17. Богданов А.В., Волосевич И.Н., Хазов Е.Н. «Дропперство» как один из способов легализации денежных средств и имущества, приобретенного преступным путем // Судебная экспертиза и исследования. 2026. № 2. С. 14–21.
18. Антонов Ю.И., Костиков А.Д. Об уголовной ответственности за дропперство (чч. 3–6 ст. 187 УК РФ) // Образование и право. 2026. № 1. С. 760–766.
19. Литвиненко А.Н., Гузикова Л.А. Проблемы и противоречия системы противодействия кибермошенничеству в условиях цифровизации экономики // Экономическое возрождение России. 2026. № 1. С. 153–175.
20. Anderson R., Barton C., Böhme R., Clayton R., van Eeten M., Levi M., Moore T., Savage S. Measuring the Cost of Cybercrime // The Economics of Information Security and Privacy. Berlin; Heidelberg: Springer, 2013. P. 265–300.



21. Gordon L.A., Loeb M.P. The Economics of Information Security Investment // ACM Transactions on Information and System Security. 2002. Vol. 5. No. 4. P. 438–457.
22. Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций, за 2025 год // Банк России. URL: https://www.cbr.ru/analytics/ib/operations_survey/2025/.
23. Коротко о главном: итоги 2025 года // Банк России. URL: https://www.cbr.ru/StaticHtml/File/187433/kg0_2025.pdf.
24. МВД сообщило о снижении числа киберпреступлений в РФ в 2025 году // Интерфакс. URL: <https://www.interfax.ru/digital/1073418>.
25. Контрмеры приносят результат // МВД Медиа. URL: <https://mvdmedia.ru/publications/police-of-russia/pravovye-konsultatsii/kontrmery-prinosyat-rezultat/>.
26. Росстат представляет первую оценку ВВП за 2025 год // Росстат. URL: <https://rosstat.gov.ru/folder/313/document/277380>.
27. «Сбер» раскрыл, сколько средств мошенники похитили у россиян за _____ год // _____ РБК. URL: <https://www.rbc.ru/finances/29/01/2026/697b2a379a7947671694187e>.
28. Internet Crime Report 2025 // Federal Bureau of Investigation. URL: https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.
29. Annual Fraud Report 2026 // UK Finance. URL: <https://www.ukfinance.org.uk/policy-and-guidance/reports/annual-fraud-report-2026>.
30. Федеральный закон от 01.04.2025 № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации» // Официальный интернет-портал правовой информации. URL: <http://publication.pravo.gov.ru/document/0001202504010010>.
31. Федеральный закон от 24.06.2025 № 176-ФЗ «О внесении изменений в статью 187 Уголовного кодекса Российской Федерации» // КонсультантПлюс. URL: <https://www.consultant.ru/law/hotdocs/89782.html>.
32. Банковские мошенники в I квартале похитили у россиян 6,9 млрд рублей // Интерфакс. URL: <https://www.interfax.ru/business/1026035>.

References

1. Dinamika zatrat na razvitie tsifrovoi ekonomiki [Dynamics of expenditures on the development of the digital economy]. ISIEZ NIU VShE [Institute for Statistical Studies and Economics of Knowledge, HSE University]. Retrieved from: <https://issek.hse.ru/mirror/pubs/share/1132489160.pdf>. (In Russ.)
2. Rost tsifrovyykh investitsii v Rossii zamedlyaetsya [Growth of digital investment in Russia is slowing]. Kabel'shchik [Cableman]. Retrieved from: <https://www.cableman.ru/content/rost-tsifrovyykh-investitsii-v-rossii-zamedlyaetsya>. (In Russ.)
3. Chislo IT-prestuplenii v Rossii v 2025 godu sokratilos' do 675 tys. [The number of IT crimes in Russia decreased to 675 thousand in 2025]. TASS. Retrieved from: <https://tass.ru/obschestvo/26385451>. (In Russ.)
4. Ukaz Prezidenta RF ot 13.05.2017 № 208 «O Strategii ekonomicheskoi bezopasnosti Rossiiskoi Federatsii na period do 2030 goda» [Decree of the President of the Russian Federation dated May 13, 2017 No. 208 “On the Economic Security Strategy of the Russian Federation for the period up to 2030”]. GARANT.RU. Retrieved from: <https://www.garant.ru/products/ipo/prime/doc/71572608/>. (In Russ.)
5. Mustafina G.N. (2025). Aktual'nye ugrozy ekonomicheskoi bezopasnosti protsessa tsifrovizatsii predpriyatii i mekhanizmy ikh neitralizatsii [Current threats to the economic security of enterprise digitalization and mechanisms for their neutralization]. Vestnik ekonomiki, prava i sotsiologii [Bulletin of Economics, Law and Sociology], 3, 85–89. (In Russ., abstract in Eng.)
6. Burdina L.A. (2025). K voprosu ob ekonomicheskoi bezopasnosti predpriyatiya: klyuchevye riski i ugrozy v sovremennom mire [On the economic security of an enterprise: key risks and threats in the modern world]. Sovremennaya konkurentsia [Journal of Modern Competition], 19(5), 90–107. (In Russ., abstract in Eng.)
7. Skripnik O.B. (2024). Upravlenie tsifrovymi riskami v sovremennoi ekonomike [Digital risk management in the modern economy]. Vestnik Evraziiskoi nauki [The Eurasian Scientific Journal], 16(1). (In Russ., abstract in Eng.)
8. Mukhamadiyarova A.K., Abramova S.R., Rednikov D.V. (2025). Vliyanie tsifrovizatsii na ekonomicheskuyu bezopasnost' gosudarstva cherez otsenku vygod i zatrat [The impact of digitalization on the economic security of the state through the assessment of benefits and costs]. Diskussiia [Discussion], 7(140), 140–145. (In Russ., abstract in Eng.)
9. Semeko G.V. (2020). Informatsionnaya bezopasnost' v finansovom sektore: kiberprestupnost' i strategiya protivodeistviya [Information security in the financial sector: cybercrime and counteraction strategy]. Sotsial'nye novatsii i sotsial'nye nauki [Social Innovations and Social Sciences], 1, 77–96. (In Russ., abstract in Eng.)



10. Shcherbakova N.V. (2021). Tsifrovye tekhnologii v bankovskom sektore RF: osobennosti i soputstvuyushchie ugrozy [Digital technologies in the Russian banking sector: specific features and associated threats]. Vestnik Kemerovskogo gosudarstvennogo universiteta. Seriya: Politicheskie, sotsiologicheskie i ekonomicheskie nauki [Bulletin of Kemerovo State University. Series: Political, Sociological and Economic Sciences], 6(1), 136–146. (In Russ., abstract in Eng.)

11. Revenkov P.V., Oshmankevich K.R., Berdyugin A.A. (2021). Fishingovye skhemy v bankovskoi sfere: rekomendatsii pol'zovatelyam interneta po zashchite i razrabotka zadach regulirovaniya [Phishing schemes in the banking sector: recommendations for Internet users on protection and development of regulatory tasks]. Finansy: teoriya i praktika [Finance: Theory and Practice], 25(6), 212–226. (In Russ., abstract in Eng.)

12. Nasonova P.S. (2024). Pravovoe obespechenie informatsionnoi bezopasnosti v finansovoi sfere [Legal support for information security in the financial sector]. Ural'skii zhurnal pravovykh issledovaniy [Ural Journal of Legal Studies], 3, 38–48. (In Russ., abstract in Eng.)

13. Larionova S.L. (2022). Organizatsiya raboty po bor'be s moshennichestvom v kreditnoi organizatsii [Organization of anti-fraud activities in a credit institution]. Voprosy bezopasnosti [Security Issues], 4, 15–26. (In Russ., abstract in Eng.)

14. Stepanenko D.A. (2024). Antifrod kak kriminalisticheskoe sredstvo preduprezhdeniya prestupleniy v bankovskoi sfere [Anti-fraud as a forensic tool for preventing crimes in the banking sector]. Diskussiya [Discussion], 122, 128–138. (In Russ., abstract in Eng.)

15. Kislenko S.L., Fokin A.D. (2025). Moshennichestvo s ispol'zovaniem informatsionno-telekommunikatsionnykh tekhnologii kak ugroza natsional'noi bezopasnosti Rossiiskoi Federatsii [Fraud using information and telecommunication technologies as a threat to the national security of the Russian Federation]. European and Asian Law Review, 8(1), 41–54. (In Russ., abstract in Eng.)

16. Kalyuzhnyi A.N. (2026). Sposoby prestupnoi deyatelnosti dropperov: kriminalisticheskii i ugovovno-pravovoi podkhody [Methods of criminal activity of droppers: forensic and criminal law approaches]. Vestnik Sankt-Peterburgskogo universiteta. Pravo [Vestnik of Saint Petersburg University. Law], 17(1), 156–173. (In Russ., abstract in Eng.)

17. Bogdanov A.V., Volosevich I.N., Khazov E.N. (2026). «Dropperstvo» kak odin iz sposobov legalizatsii denezhnykh sredstv i imushchestva, priobretennogo prestupnym putem [“Dropperism” as one of the methods of laundering money and property acquired by criminal means]. Sudebnaya ekspertiza i issledovaniya [Forensic Examination and Research], 2, 14–21. (In Russ., abstract in Eng.)

18. Antonov Yu.I., Kostikov A.D. (2026). Ob ugolovnoi otvetstvennosti za dropperstvo (chch. 3–6 st. 187 UK RF) [On criminal liability for dropper activities (Parts 3–6 of Article 187 of the Criminal Code of the Russian Federation)]. *Obrazovanie i pravo* [Education and Law], 1, 760–766. (In Russ., abstract in Eng.)
19. Litvinenko A.N., Guzikova L.A. (2026). Problemy i protivorechiya sistemy protivodeistviya kibermoshennichestvu v usloviyakh tsifrovizatsii ekonomiki [Problems and contradictions of the cyber fraud counteraction system in the context of economic digitalization]. *Ekonomicheskoe vozrozhdenie Rossii* [Economic Revival of Russia], 1, 153–175. (In Russ., abstract in Eng.)
20. Anderson R., Barton C., Böhme R., Clayton R., van Eeten M., Levi M., Moore T., Savage S. (2013). Measuring the Cost of Cybercrime. In: *The Economics of Information Security and Privacy*. Berlin; Heidelberg: Springer, 265–300. (In Eng.)
21. Gordon L.A., Loeb M.P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 5(4), 438–457. (In Eng.)
22. Obzor operatsii, sovershennykh bez dobrovol'nogo soglasiya klientov finansovykh organizatsii, za 2025 god [Review of transactions carried out without the voluntary consent of financial institution clients in 2025]. Bank Rossii [Bank of Russia]. Retrieved from: https://www.cbr.ru/analytics/ib/operations_survey/2025/. (In Russ.)
23. Korotko o glavnom: itogi 2025 goda [In brief: results of 2025]. Bank Rossii [Bank of Russia]. Retrieved from: https://www.cbr.ru/StaticHtml/File/187433/kg0_2025.pdf. (In Russ.)
24. MVD soobshchilo o snizhenii chisla kiberprestuplenii v RF v 2025 godu [The Ministry of Internal Affairs reported a decline in the number of cybercrimes in Russia in 2025]. Interfax. Retrieved from: <https://www.interfax.ru/digital/1073418>. (In Russ.)
25. Kontrmery prinosyat rezul'tat [Countermeasures are producing results]. MVD Media. Retrieved from: <https://mvdmedia.ru/publications/police-of-russia/pravovye-konsultatsii/kontrmery-prinosyat-rezultat/>. (In Russ.)
26. Rosstat predstavlyaet pervuyu otsenku VVP za 2025 god [Rosstat presents the first GDP estimate for 2025]. Rosstat. Retrieved from: <https://rosstat.gov.ru/folder/313/document/277380>. (In Russ.)
27. «Sber» raskryl, skol'ko sredstv moshenniki pokhitali u rossiyan za god [Sber revealed how much money fraudsters stole from Russians over the year]. RBC. Retrieved from: <https://www.rbc.ru/finances/29/01/2026/697b2a379a7947671694187e>. (In Russ.)
28. Federal Bureau of Investigation. (2025). Internet Crime Report 2025. Retrieved from: https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf. (In Eng.)

29. UK Finance. (2026). Annual Fraud Report 2026. Retrieved from: <https://www.ukfinance.org.uk/policy-and-guidance/reports/annual-fraud-report-2026>. (In Eng.)

30. Federal'nyi zakon ot 01.04.2025 № 41-FZ «O sozdanii gosudarstvennoi informatsionnoi sistemy protivodeistviya pravonarusheniyam, sovershaemym s ispol'zovaniem informatsionnykh i kommunikatsionnykh tekhnologii, i o vnesenii izmenenii v otдел'nye zakonodatel'nye akty Rossiiskoi Federatsii» [Federal Law No. 41-FZ of April 1, 2025 “On the creation of a state information system for countering offenses committed using information and communication technologies and on amendments to certain legislative acts of the Russian Federation”]. Ofitsial'nyi internet-portal pravovoi informatsii [Official Internet Portal of Legal Information]. Retrieved from: <http://publication.pravo.gov.ru/document/0001202504010010>. (In Russ.)

31. Federal'nyi zakon ot 24.06.2025 № 176-FZ «O vnesenii izmenenii v stat'yu 187 Ugolovnogo kodeksa Rossiiskoi Federatsii» [Federal Law No. 176-FZ of June 24, 2025 “On amendments to Article 187 of the Criminal Code of the Russian Federation”]. Konsul'tantPlyus [ConsultantPlus]. Retrieved from: <https://www.consultant.ru/law/hotdocs/89782.html>. (In Russ.)

32. Bankovskie moshenniki v I kvartale pokhitali u rossiyan 6,9 mlrd rublei [Bank fraudsters stole 6.9 billion rubles from Russians in the first quarter]. Interfax. Retrieved from: <https://www.interfax.ru/business/1026035>. (In Russ.)

© Меньшов В.Н., 2026

