Вестник Евразийской науки / The Eurasian Scientific Journal https://esj.today

2025, Том 17, № s6 / 2025, Vol. 17, Iss. s6 https://esj.today/issue-s6-2025.html

URL статьи: https://esj.today/PDF/91FAVN625.pdf

5.2.4. Финансы (экономические науки)

Ссылка для цитирования этой статьи:
Тарасова, В. С. Современные механизмы защиты клиентов коммерческих банков от мошеннических действий третьих лиц российская практика и тенденции 2025 года / В. С. Тарасова // Вестник евразийской науки. — 2025. — Т. 17. — № s6. — URL: https://esj.today/PDF/91FAVN625.pdf.

For citation:
Tarasova V.S. Modern mechanisms for protecting commercial bank clients from fraudulent actions by third parties: Russian practice and trends to 2025. *The Eurasian Scientific Journal*. 2025;17(s6): 91FAVN625. Available at: https://esj.today/PDF/91FAVN625.pdf. (In Russ., abstract in Eng.).

УДК 338

Тарасова Валерия Станиславовна
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
E-mail: Tarasova.vs@list.ru
РИНЦ: https://elibrary.ru/author_profile.asp?id=1205606

Научный руководитель: **Амосова Наталия Анатольевна**
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Профессор кафедры «Банковского дела и монетарного регулирования»
Доктор экономических наук, профессор
E-mail: naamosova@fa.ru
РИНЦ: https://elibrary.ru/author_profile.asp?id=386448

Современные механизмы защиты клиентов коммерческих банков от мошеннических действий третьих лиц российская практика и тенденции 2025 года

Аннотация. Статья посвящена трансформации модели защиты клиента коммерческого банка в России в 2025 г. Показано, что после изменения правового подхода операция без добровольного согласия клиента стала пониматься шире: в нее включаются не только случаи внешнего несанкционированного доступа, но и переводы, совершенные самим клиентом под влиянием обмана или злоупотребления доверием. На этом фоне автор рассматривает, как меняются критерии оценки действий банка: значение приобретает не только проверка формального согласия, но и способность кредитной организации вовремя выявить риск, приостановить операцию, предупредить клиента и зафиксировать инцидент. В статье анализируются основные показатели ОБДС в 2024–2025 гг., их поквартальная динамика, а также различия между основными каналами хищения у физических лиц. Отдельное внимание уделяется новым мерам защиты, получившим развитие в 2025 г., включая самозапрет на получение кредита, периоды ожидания, антифрод-контроль при выдаче наличных, цифровые сервисы оперативного обращения и межведомственный обмен сведениями. Делается вывод, что российская модель стала более последовательной и многоуровневой, однако ее наиболее уязвимым звеном по-прежнему остается не стадия предотвращения, а стадия последующего имущественного возмещения. В связи с этим дальнейшее развитие правового регулирования, вероятно, будет связано с уточнением стандартов банковской осмотрительности и критериев ответственности банка при мошенничестве, основанном на социальной инженерии.

Ключевые слова: коммерческий банк; защита клиента; банковское мошенничество; ОБДС; социальная инженерия; антифрод; возмещение ущерба

Введение

Банковское мошенничество в России претерпевает качественную трансформацию, масштаб и сложность которой к 2025 году вышли за рамки привычных представлений о несанкционированном доступе к счёту. Если прежняя модель угрозы строилась преимущественно вокруг внешнего технического вторжения — кражи карты, перехвата пароля, взлома мобильного приложения, — то современная практика свидетельствует о принципиально ином характере рисков: сегодня злоумышленнику зачастую не требуется преодолевать технические барьеры, поскольку гораздо эффективнее оказывается управление действиями самого клиента посредством психологического давления, имитации доверия и создания искусственной срочности.

Актуальность исследования определяется совокупностью факторов. Российский рынок банковского мошенничества демонстрирует тревожную динамику: число зафиксированных операций без добровольного согласия клиента неуклонно растёт, средняя сумма одной операции снижается — что указывает на расширение массива относительно небольших, но многочисленных хищений. При общем объёме предотвращённых потерь, демонстрирующем рост эффективности антифрод-систем, доля фактически возвращённых клиентам средств сократилась с 9,9 до 5,9 %, обнажая принципиальную асимметрию между стадией предотвращения и стадией имущественного возмещения.

Целью настоящего исследования является анализ трансформации модели защиты клиента коммерческого банка в России в 2025 году: выявление системных изменений в правовом регулировании, оценка новых защитных механизмов, анализ поквартальной динамики операций без добровольного согласия клиента в разрезе основных каналов хищения, а также сопоставление российской практики с зарубежным опытом — прежде всего британской моделью регулирования APP-мошенничества.

1. Методы и материалы

Методологическую основу исследования образует совокупность взаимодополняющих подходов, обеспечивающих многоуровневый анализ защиты клиентов коммерческих банков от мошеннических действий.

Теоретическую базу исследования составили труды по социальной инженерии как источнику рисков в системах дистанционного банковского обслуживания, защите прав потребителей финансовых услуг, об актуальных проблемах противодействия хищениям в ДБО, защите прав потребителей в сфере платёжных услуг: Г.В. Федотовой [1], С.Н. Орлова [2], М.П. Шальнева [3], Д.С. Паниной [4], А.В. Ярашевой [5], Д.Д. Щукаревой [6], С.А. Голубцова [7], С.В. Ештокина [8], К.А. Запорожской [9], В.А. Марченко [10] и других.

Информационную базу составили: ежеквартальные и годовые обзоры Банка России по операциям без добровольного согласия клиента за 2024–2025 годы; отчёты ФинЦЕРТ о разделегировании фишинговых доменов и блокировке мошеннических номеров; официальные данные Правительства Российской Федерации о масштабах внедрения самозапрета на потребительские кредиты; аналитические материалы FCA об итогах первого года действия режима обязательного возмещения жертвам APP-мошенничества в Великобритании. Совокупность применённых методов и источников обеспечила необходимую аналитическую строгость для формулирования обоснованных выводов о состоянии и перспективах развития модели защиты клиента коммерческого банка в России.

2. Результаты и обсуждение

91FAVN625
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

В 2025 г. защита клиента коммерческого банка уже заметно отличается от той модели, которая долгое время строилась в основном вокруг охраны карты, пароля или доступа к мобильному приложению. Сейчас проблема рассматривается шире. После вступления в силу Федерального закона от 24.07.2023 № 369-ФЗ [1] в статистике Банка России операция без добровольного согласия клиента стала пониматься не только как списание при внешнем несанкционированном доступе, но и как перевод, который сам клиент совершил под влиянием обмана или злоупотребления доверием. Из-за этого меняется и сам критерий оценки действий банка. Уже недостаточно просто установить, что распоряжение формально подтверждено. Гораздо важнее становится другое: сумел ли банк вовремя заметить риск, предупредить клиента, приостановить операцию и передать нужные сведения в общую базу мошеннических реквизитов.

Такой поворот нельзя считать неожиданным. В научной литературе он, по сути, был намечен заранее. П.В. Ревенков писал о социальной инженерии как о способе управлять действиями человека без прямого технического вторжения [11]. Е.А. Русскевич показывал, что хищения в системах дистанционного банковского обслуживания нельзя объяснить только уголовно-правовыми нормами или только техническими уязвимостями, потому что здесь пересекаются сразу несколько сфер [12]. С.Л. Ларионова обращала внимание на то, что внутри кредитной организации борьба с мошенничеством не может держаться только на программных фильтрах, поскольку давление на человека для преступника часто проще и дешевле, чем атака на инфраструктуру.[2] А.Я. Курбатов, в свою очередь, отмечал раздробленность регулирования в сфере защиты потребителей финансовых услуг, когда вместо одного согласованного механизма клиент фактически сталкивается с набором не вполне синхронных норм [13]. В 2025 г. эти выводы уже не только теоретические: банковская и регуляторная практика во многом их подтвердила.

Таблица 1

Основные индикаторы ОБДС в банковской сфере России в 2024–2025 гг.

Показатель	2024 г.	2025 г.
Доля объема ОБДС в общем объеме переводов, %	0,00066	0,00071
Средняя сумма одной операции, тыс. руб.	22,9	18,6
Возвращено клиентам, % от объема ОБДС	9,9	5,9
Возвращено клиентам, млн руб.	2713,58	1731,3
Предотвращено операций, млн ед.	72,17	134,16
Предотвращенный объем, млрд руб.	13 508,04	13 895,4
Операции по картам у физических лиц, тыс. ед.	821,87	980,46
Наибольший объем хищений у физических лиц, млн руб.	ДБО/счета: 9602,57	Счета: 10 628,41

Составлено по данным Банка России[3]

Отсюда видно, что современная защита клиента в банковской сфере развивается не по одному направлению. Она складывается сразу из нескольких уровней: правового, технологического, поведенческого и межведомственного. Если хотя бы один из них работает с опозданием, общий результат заметно ухудшается. Именно поэтому высокие показатели предотвращения еще не означают столь же высокий уровень возмещения уже похищенных денег. В 2025 г. это стало особенно заметно. Банки смогли предотвратить потери на очень крупные суммы, но возврат

[1] О внесении изменений в Федеральный закон «О национальной платежной системе»: Федеральный закон от 24 июля 2023 г. № 369-ФЗ (последняя редакция). — Текст: электронный // КонсультантПлюс: справ.-правовая система. — URL: https://www.consultant.ru/document/cons_doc_LAW_452742/ (дата обращения: 20.03.2026)

[2] Ларионова, С.Л. Информационная безопасность дистанционного банковского обслуживания: учебное пособие / С.Л. Ларионова. — Москва: Прометей, 2022. — 296 с.

[3] Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций. — Текст: электронный // Банк России. — URL: https://cbr.ru/analytics/ib/operations_survey/2024/ (дата обращения: 20.03.2026).

91FAVN625
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

средств после состоявшегося списания остался слабым. В этом и состоит один из главных вопросов: способны ли существующие механизмы не только остановить хищение, но и реально компенсировать ущерб пострадавшему клиенту. Общие итоги 2024 и 2025 гг. приведены ниже (табл. 1).

Эти данные не позволяют сделать совсем простой вывод, что мошенничество либо выросло, либо сократилось как единый процесс. Картина сложнее. С одной стороны, число эпизодов увеличилось довольно сильно, а средняя сумма одной операции, наоборот, уменьшилась. Это похоже на расширение массива относительно небольших по размеру хищений. С другой стороны, доля средств, которые удалось вернуть клиентам после списания, снизилась с 9,9 до 5,9 %. Это нельзя назвать прямым доказательством того, что антифрод стал хуже. Скорее наоборот: банковская система научилась лучше отсекать массовые небольшие и средние операции еще до их завершения. Но если списание все-таки состоялось, деньги по-прежнему быстро проходят через цепочку посредников, дропов и разных счетов, и тогда вернуть их гораздо труднее. Поэтому оценивать защищенность клиента только по объему предотвращенных потерь недостаточно. Нужно смотреть сразу на три вещи: сколько операций остановлено, сколько средств потом реально возвращено и через какой канал было совершено хищение.

Если смотреть на каналы, то в 2025 г. по числу эпизодов впереди были операции с платежными картами: 980,46 тыс. у физических лиц. Но по объему ущерба первое место заняли счета и переводы через дистанционное банковское обслуживание — 10 628,41 млн руб.[4] Это важный момент. Он показывает, что представление о банковском мошенничестве как о чисто проблеме с картами уже не вполне соответствует реальности. Карта сохраняет значение как массовая точка входа, но основные денежные риски все заметнее переходят туда, где клиент сам подтверждает перевод в онлайн-банке, через СБП или под влиянием ложного звонка, вредоносной программы, поддельной ссылки или программы удаленного доступа. Банк России прямо указывал на NFC Gate, вредоносное программное обеспечение и фишинговые ссылки как на типичные инструменты 2025 г.

Эта ситуация хорошо согласуется и с позицией Е.Ж. Ганиева, который, рассматривая защиту прав потребителей в сфере платежных услуг, подчеркивал, что рост мошенничества и трудности возврата средств нельзя сводить к вопросу о формальном согласии клиента [14]. Если перевод совершен под давлением обмана, то внешнее подтверждение уже не означает, что интересы сторон действительно соблюдены. В такой ситуации у банка возникает не только обязанность выполнить распоряжение клиента, но и обязанность распознать нетипичное поведение, связаться с клиентом и корректно зафиксировать инцидент для дальнейшего спора. В 2025 г. это уже стало частью обычной банковской практики, а не только научной дискуссии.

Наибольшее значение в 2025 г. получили несколько разных механизмов. Во-первых, это двухдневная приостановка подозрительных переводов по реквизитам из базы Банка России, которая основана на поправках к Закону о национальной платежной системе.[5] Во-вторых, с 1 марта 2025 г. гражданам стал доступен самозапрет на получение потребительских кредитов и займов.[6] В-третьих, с 1 сентября 2025 г. начали действовать периоды ожидания по потребительскому кредиту: не менее 4 часов для сумм от 50 до 200 тыс. руб. и не менее 48 часов для сумм свыше

[4] Опрос о банковских операциях. — Текст: электронный // Банк России. — URL: https://www.cbr.ru/analytics/ib/operations_survey/2025/ (дата обращения: 20.03.2026)

[5] О внесении изменений в Федеральный закон «О национальной платежной системе»: Федеральный закон от 24 июля 2023 г. № 369-ФЗ (последняя редакция). — Текст: электронный // КонсультантПлюс: справ.-правовая система. — URL: https://www.consultant.ru/document/cons_doc_LAW_452742/ (дата обращения: 20.03.2026)

[6] Самозапрет на заключение договоров потребительских кредитов (займов). — Текст: электронный // Банк России. — URL: https://www.cbr.ru/ckki/self-prohibition_credit/ (дата обращения: 20.03.2026)

91FAVN625
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

200 тыс. руб.[7] Кроме того, с той же даты стала обязательной антифрод-проверка при снятии наличных через банкомат, а при наличии признаков давления со стороны мошенников банк получил возможность временно ограничивать такие операции. Еще одна мера — обязательный с 1 октября 2025 г. сервис в мобильных приложениях крупных банков для быстрого заявления об ОБДС и получения электронной справки. Наконец, большую роль играет межведомственный обмен данными через инфраструктуру ФинЦЕРТ и государственную информационную систему противодействия правонарушениям, совершаемым с применением информационно-коммуникационных технологий.

Важно, что все эти меры решают не одну и ту же задачу. Самозапрет на кредит нужен еще до возникновения обязательства и снижает риск навязанного займа. Период ожидания дает человеку время выйти из состояния давления и попытаться проверить ситуацию. Банкоматный антифрод включается уже в тот момент, когда преступник довел клиента до снятия наличных. Сервис в приложении, наоборот, особенно важен уже после списания, потому что помогает быстрее зафиксировать происшествие и собрать документы для банка и полиции. Получается, что в 2025 г. российская модель стала более последовательной: защита начала строиться до операции, во время нее и сразу после нее. По сути, это и есть главное качественное изменение.

Эффект такого подхода заметен и по масштабу охвата. По данным Правительства, к концу 2025 г. самозапрет на кредиты и займы оформили свыше 20 млн граждан.[8] Одновременно сервис «жизненная ситуация» объединил несколько мер защиты от мошенников в одном цифровом контуре. Со стороны Банка России и ФинЦЕРТ тоже видно расширение совместной работы: в информационном обмене участвует более 1 700 организаций, включая все российские банки; за 2025 г. было инициировано разделегирование 1 002 фишинговых доменов, в Генеральную прокуратуру направлены сведения о 32 566 доменах, 4 817 страницах в социальных сетях и 33 приложениях, а на блокировку передано более 69 тыс. мошеннических телефонных номеров.[9] Обычный клиент этот уровень работы может даже не замечать, но без него отдельные банковские фильтры тоже не будут достаточно эффективны.

Здесь уместно уточнить, почему кредитный блок в 2025 г. занял столь заметное место в антимошеннической политике. По оценке Банка России, около 40 % похищенных средств составляют кредитные деньги. Поэтому самозапрет и период ожидания нельзя понимать как второстепенные меры: они направлены не только на снижение долговой нагрузки, но и на пресечение типовой последовательности, при которой человека сначала убеждают оформить заем, а затем немедленно перечислить деньги на чужой счет. Банк России отдельно разъясняет, что при выдаче кредита вопреки самозапрету кредитор не вправе требовать от заемщика исполнения обязательств.[10] В документах регулятора за 2025 г. этот подход дополнен обменом сведениями между кредиторами и бюро кредитных историй в режиме, близком к реальному времени. За счет этого сокращается временной разрыв, которым ранее пользовались преступники, направляя несколько заявок почти одновременно в разные организации. В тот же пакет мер 2025 г. вошли и ограничения по каналам вывода похищенных средств: для лиц, сведения о которых находятся в базе Банка России, сумма переводов себе и другим людям не

[7] Закон о периоде «охлаждения» по кредитам для потребителей и иных мерах против мошенников опубликован. — Текст: электронный // КонсультантПлюс. — URL: https://www.consultant.ru/legalnews/27782/ (дата обращения: 20.03.2026).

[8] ОКБ: россияне в 2025 году подали 20 млн заявлений на самозапрет на кредиты. — Текст: электронный // ТАСС. — URL: https://tass.ru/ekonomika/26052111 (дата обращения: 20.03.2026).

[9] Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций. — Текст: электронный // Банк России. — URL: https://cbr.ru/analytics/ib/operations_survey/2024/ (дата обращения: 20.03.2026).

[10] Банк России ответил на вопросы по самозапрету на получение кредитов. — Текст: электронный // ГАРАНТ.РУ. — URL: https://www.garant.ru/news/1802932/ (дата обращения: 20.03.2026).

91FAVN625
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

может превышать 100 тыс. руб. в месяц, банки не должны выдавать таким клиентам новые электронные средства платежа, а внесение наличных на вновь токенизированные карты ограничено суммой 50 тыс. руб. в первые 48 часов.

Не менее важно и то, что новый цифровой канал обращения меняет саму статистическую базу наблюдения. По данным Банка России, в 2024 г. только треть пострадавших обращалась одновременно и в банк, и в полицию.[11] С 1 октября 2025 г. крупные банки обязаны принимать сообщение о мошенническом переводе через мобильное приложение и формировать электронную справку для правоохранительных органов. Уже в ноябре 2025 г. Банк России прямо связал возможный рост числа выявленных операций с тем, что пострадавшим стало легче фиксировать инцидент, прежде всего при небольших суммах ущерба. Это замечание существенно для толкования годовой динамики: рост числа ОБДС в 2025 г. отражает не только усиление преступной активности, но и уменьшение латентности. Одновременно регулятор указывает, что к середине ноября 2025 г. успешной оказывалась лишь одна из 146 попыток хищения, тогда как годом ранее на один успешный перевод приходилось только 55 неудачных попыток. Кроме того, крупнейшие банки в совокупности ежемесячно приостанавливали около 330 тыс. переводов на счета злоумышленников, сведения о которых уже содержались в базе Банка России[12]. Поэтому оценка защищенности клиента должна учитывать не только итоговый объем похищенных средств, но и изменение полноты регистрации инцидентов, а также масштаб операций, остановленных еще до списания денег со счета.

Отдельно стоит сказать об институциональной стороне вопроса. В 2025 г. защита клиента перестала быть делом только банка и клиента. Федеральный закон от 01.04.2025 № 41-ФЗ[13] о создании государственной информационной системы противодействия правонарушениям, совершаемым с применением информационно-коммуникационных технологий, закрепил движение к более тесному взаимодействию банков, операторов связи, цифровых платформ и правоохранительных органов. Это вполне логично. Если номер мошенника, реквизиты дропа, домен, канал входа и кредитная заявка находятся в разных ведомственных массивах и обмениваются слишком медленно, то преступник почти всегда будет быстрее. Но если сигнал передается синхронно, даже частичная задержка по одному элементу может сорвать весь эпизод. Поэтому значение российской практики 2025 г. связано не только с отдельными новыми нормами, но и с попыткой собрать разрозненные меры в более общий рабочий контур.

При этом среда риска в 2025 г. стала качественно сложнее. По данным Банка России, число телефонных номеров, переданных операторам связи для реагирования, оказалось ниже, чем в 2024 г.: более 69 тыс. против 171 977.[14] Само по себе это не означает ослабления телефонного мошенничества. Еще в обзоре за 2024 г. Банк России отмечал, что преступники все активнее переходят в мессенджеры, где сочетаются звонки, файлы, фальшивые документы и ссылки на поддельные ресурсы. Значит, одной блокировки номера уже недостаточно. Нужна комбинация телефонного антиспуфинга, блокировки доменов, контроля приложений и

[11] Банки проверяют все переводы на признаки мошенничества. — Текст: электронный // Банк России. — URL: https://www.cbr.ru/press/event/?id=28092 (дата обращения: 20.03.2026).

[12] Мобильные приложения крупных банков будут дополнены функционалом для пострадавших от мошенников. — Текст: электронный // Банк России. — URL: https://www.cbr.ru/press/event/?id=23465 (дата обращения: 20.03.2026).

[13] О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 1 апреля 2025 г. № 41-ФЗ (ред. от 31.07.2025). — Текст: электронный // КонсультантПлюс: справ.-правовая система. — URL: https://www.consultant.ru/document/cons_doc_LAW_502182/ (дата обращения: 20.03.2026).

[14] ЦБ выявил более 171 тыс. номеров телефонов, которые использовали мошенники. — Текст: электронный // ТАСС. — URL: https://tass.ru/ekonomika/23175765 (дата обращения: 20.03.2026).

91FAVN625
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

быстрого обмена данными о реквизитах получателей денег. Иначе говоря, количественное снижение по одному показателю здесь не отменяет общего усложнения схем.

Есть и еще одна проблема — неравномерность банковской защиты. Можно предположить, что системно значимые банки быстрее внедряют поведенческие модели, биометрию, внутренние скоринговые фильтры и удобные цифровые каналы срочного обращения. Менее крупные организации, вероятно, чаще зависят от внешних поставщиков и типовых решений. Формально требования едины, но фактический уровень защищенности клиента может различаться. В этом смысле важен тезис Л.А. Петряковой и А.Л. Репецкой из монографии 2025 г. о необходимости системы противодействия, которая учитывает конкретную криминологическую среду и региональную специфику [15]. Этот вывод вполне переносится и на банковскую сферу: одна и та же норма работает по-разному в зависимости от масштаба банка, качества данных, внутренней организации и наличия круглосуточного мониторинга.

На этом фоне особенно заметна главная асимметрия 2025 г.: российская модель пока сильнее в части пресечения, чем в части имущественного возмещения. В годовом обзоре Банка России за 2025 г. прямо сказано, что объем средств, возвращенных по основанию финансовой ответственности банка за перевод по реквизитам из базы Банка России, составил только 3,16 млн руб.[15] На фоне общего объема ОБДС это очень мало. Получается, что норма о банковской ответственности пока работает скорее как дисциплинирующий сигнал, чем как действительно массовый компенсационный механизм. Поэтому дальнейшее развитие правового регулирования, скорее всего, будет связано с более точным определением стандартов банковской осмотрительности, с фиксацией поведенческих аномалий и с оценкой поведения клиента, действовавшего под давлением обмана. Без этого превентивный блок и дальше будет развиваться быстрее, чем компенсационный. Поквартальная динамика 2025 г. приведена ниже (табл. 2).

Таблица 2

Поквартальная динамика ОБДС в 2025 г.

Показатель	I квартал 2025 г.	II квартал 2025 г.	III квартал 2025 г.
Количество ОБДС, ед.	296 591	273 089	460 130
Объем ОБДС, тыс. руб.	6 856 684,43	6 331 116,59	8 176 075,88
Возвращено клиентам, % от объема	7,6	5,2	5,1
Предотвращено операций, ед.	43 831 404	38 672 819	28 473 397
Предотвращенный объем, тыс. руб.	4 607 333 021,16	3 424 704 522,99	3 516 395 514,20

Составлено по данным Банка России[16]

По этой таблице можно заметить, как минимум, два момента. Во-первых, количество операций, которые в итоге дошли до списания, во всех кварталах намного меньше числа предотвращенных эпизодов. Это говорит о большой нагрузке на антифрод и о том, что банковские фильтры в целом работают достаточно мощно. Во-вторых, доля возврата после уже состоявшегося списания к III кварталу опустилась почти до 5 %. Следовательно, узкое место находится не только на стадии пресечения, но и позже — когда нужно быстро отследить платеж, заморозить след движения денег и решить вопрос о распределении имущественной ответственности между банком, клиентом и получателем средств.

[15] В 2025 году банки вернули 5,9 % средств, переведенных без согласия клиентов. — Текст: электронный // ТАСС. — URL: https://tass.ru/ekonomika/26443227 (дата обращения: 20.03.2026).

[16] Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. — Текст: электронный // Банк России. — URL: https://www.cbr.ru/statistics/ib/review_1q_2025/ (дата обращения: 20.03.2026).

91FAVN625
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Особенно показательным выглядит III квартал 2025 г. Количество ОБДС выросло до 460 130 эпизодов, а объем достиг 8,176 млрд руб.[17] При этом число предотвращенных операций оказалось ниже, чем в I квартале. Такое сочетание нельзя толковать прямолинейно. Скорее всего, преступная активность сильнее сместилась в массовые, быстрые и психологически подготовленные сценарии, где клиент действует сам и не всегда сразу идет в банк. То есть рост зарегистрированных ОБДС связан не только с реальным давлением со стороны преступников, но и с изменениями в регистрации и выявлении таких случаев. Этот вывод дополнительно подтверждается тем, что в 2025 г. Банк России специально отметил востребованность нового банковского сервиса для пострадавших именно у тех клиентов, которые раньше из-за небольших сумм потерь вообще не обращались ни в банк, ни в полицию.

Отдельно нужно учитывать и наличный канал обращения денег. Еще в 2024 г. Банк России отмечал, что после усиления контроля над карточными и переводными операциями преступники стали чаще убеждать людей снимать или передавать наличные. В 2025 г. этот риск получил специальный ответ: обязательную проверку операций через банкомат и возможность временного лимита при признаках давления. По словам представителей Банка России, только за первый месяц действия этой меры банки предотвратили хищения более чем на 44 млрд руб[18]. Это показывает, что новация имела не символическое, а вполне быстрое практическое значение.

Но даже здесь ситуация не совсем однозначна. Антифрод при выдаче наличных помогает защитить клиента, однако одновременно создает новую потенциальную зону конфликта между скоростью банковского обслуживания и правом банка временно вмешаться в операцию. В зарубежном регулировании похожая проблема тоже есть. При «APP fraud» подтвержденный клиентом перевод уже не рассматривается как безусловное доказательство его подлинной воли. В британском подходе это привело и к обязательному в большинстве случаев возмещению жертвам «APP fraud», и к возможности риск-ориентированной задержки платежа до 4 рабочих дней.[19] Для российской практики такой поворот очень важен. Чем больше операций совершается под воздействием социальной инженерии, тем труднее опираться на старую формулу о том, что клиент сам все подтвердил. Нужен другой критерий: имел ли банк реальную возможность вовремя увидеть манипуляцию и остановить операцию хотя бы на короткий срок. Структура основных каналов хищения в 2025 г. приведена ниже (табл. 3).

Таблица 3

Основные каналы ОБДС у физических лиц в 2025 г.

Канал	I квартал: количество, ед.	I квартал: объем, тыс. руб.	II квартал: количество, ед.	II квартал: объем, тыс. руб.	III квартал: количество, ед.	III квартал: объем, тыс. руб.
Карты	212 459	1 736 075,33	189 348	1 561 213,61	264 377	1 959 131,90
Счета и переводы в ДБО	38 272	2 903 273,23	36 868	2 224 599,81	98 209	2 704 559,76
СБП	43 349	2 008 534,55	44 610	2 192 119,80	91 881	3 087 075,22

Составлено по данным Банка России[20]

[17] Банки предотвратили хищение 3,5 трлн рублей: итоги III квартала. — Текст: электронный // Банк России. — URL: https://cbr.ru/press/event/?id=28088 (дата обращения: 20.03.2026).

[18] Зампред ЦБ Герман Зубарев раскрыл настоящий ущерб от мошенников в России. — Текст: электронный // Банк России. — URL: https://cbr.ru/press/event/?id=28288 (дата обращения: 20.03.2026).

[19] Authorised Push Payment Fraud: enabling a risk-based approach to payment processing. — Текст: электронный // Financial Conduct Authority. — URL: https://www.fca.org.uk/publication/guidance-consultation/gc24-5.pdf (дата обращения: 20.03.2026).

[20] Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств. — Текст: электронный // Банк России. — URL: https://www.cbr.ru/statistics/ib/review_1q_2025/ (дата обращения: 20.03.2026).

91FAVN625
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Из таблицы видно, что карта остается главным массовым носителем риска, но денежный центр проблемы постепенно сдвигается к переводам по счетам и через СБП. Уже в III квартале объем потерь по СБП оказался выше, чем по карточным эпизодам, и стал самым крупным среди трех основных каналов. Здесь хорошо видно важное изменение 2025 г. Мошеннику все реже нужно скрыто списывать деньги. Гораздо эффективнее заставить клиента самому перевести средства через знакомый и внешне безопасный интерфейс. Поэтому так выросла роль психологического давления, ложной срочности, поддельного статуса звонящего, а также вредоносных программ, которые помогают преступнику взять контроль над устройством.

В этом смысле российская практика движется примерно в ту же сторону, что и зарубежное регулирование. В Великобритании с 7 октября 2024 г. для Faster Payments действует обязательный в большинстве случаев порядок возмещения жертвам APP fraud, а также допускается риск-ориентированная задержка подозрительного платежа до 4 рабочих дней.[21] Российская модель этот подход пока не воспроизводит полностью, но сходство направления заметно: сначала расширяется само понятие ОБДС, затем вводятся паузы, особые признаки риска, цифровые каналы срочного обращения и более плотный обмен сведениями между участниками системы.

Зарубежный материал усиливает этот тезис, поскольку показывает, как меняется правовая оценка операций, формально подтвержденных клиентом. В британской системе после запуска обязательного возмещения по APP fraud регулятор уже в сентябре 2025 г. сообщал, что в первые три месяца действия новых правил клиентам вернули 86 % утраченных средств против 68 % годом ранее, а 84 % требований были рассмотрены в течение пяти рабочих дней. Позднее FCA в обзоре от марта 2026 г., который подвел итоги первого года действия нового порядка, указал еще более широкий показатель: 88 % средств, утраченных потребителями в пределах действия этой модели, были возвращены, а общий объем возврата составил 173 млн фунтов стерлингов.[22] На этом фоне российский показатель возврата за 2025 г., равный 5,9 % от объема ОБДС, особенно отчетливо показывает, что отечественная практика пока заметно сильнее на стадии пресечения, чем на стадии имущественного возмещения. Отсюда следует и возможное направление дальнейшего развития: спор о защите клиента все чаще будет вестись не вокруг самого факта нажатия кнопки подтверждения, а вокруг того, располагал ли банк достаточными признаками риска для временной остановки операции и последующего возврата средств.

Из этого вытекает и вероятный прогноз на ближайший период. Скорее всего, в 2026 г. число зарегистрированных ОБДС продолжит расти даже в том случае, если средняя сумма одной операции стабилизируется или немного снизится. Для такого предположения есть как минимум три причины. Во-первых, сервисы быстрого заявления в банковских приложениях выводят из латентности большое число мелких потерь, которые раньше просто не фиксировались. Во-вторых, преступная активность, видимо, и дальше будет переходить в ДБО и СБП, где переводы происходят быстрее, а формальная авторизация клиента сохраняется. В-третьих, банковская защита все больше строится на паузе и анализе поведения, а не только на проверке устройства, пароля или реквизитов. Поэтому главным показателем качества банковской защиты в ближайшее время, скорее всего, станет не просто общий объем предотвращенных потерь, а сочетание трех величин: доли остановленных переводов, доли возвращенных средств и доли ложных срабатываний антифрода.

[21] Authorised Push Payment Fraud: enabling a risk-based approach to payment processing. — Текст: электронный // Financial Conduct Authority. — URL: https://www.fca.org.uk/publication/guidance-consultation/gc24-5.pdf (дата обращения: 20.03.2026).

[22] Showing financial crime the red card. — Текст: электронный // FCA. — URL: https://www.fca.org.uk/news/speeches/showing-financial-crime-red-card (дата обращения: 20.03.2026).

91FAVN625
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Заключение

Таким образом, в 2025 г. российская практика показала не просто расширение набора антифрод-инструментов, а изменение самой конструкции защиты клиента коммерческого банка. Если раньше центральным был вопрос о несанкционированном доступе, то теперь на первый план выходит своевременное распознавание обмана, в том числе в тех случаях, когда клиент сам подтверждает перевод, снятие наличных или кредитную заявку. Российская модель уже включает важные элементы такого подхода: обновленное понятие ОБДС, самозапрет на кредит, периоды ожидания, антифрод в банкоматах, новый цифровой канал обращения и более плотный межведомственный обмен данными. Но при этом механизм возмещения пока заметно отстает от механизма предупреждения. Пока эта разница сохраняется, защита клиента будет достаточно сильной на этапе предотвращения и гораздо слабее тогда, когда хищение уже произошло.

ЛИТЕРАТУРА

1. Федотова, Г.В. Механизмы повышения информационной безопасности систем интернет-банкинга / Г.В. Федотова, А.А. Гонтарь, Е.И. Зубкова // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. — 2017. — Т. 7, № 1(22). — С. 17–28. — EDN YNVZOH.
2. Орлов, С.Н. Институциональные механизмы защиты населения от мошеннических действий в банковской сфере / С.Н. Орлов, Р.В. Реутов — DOI 10.34130/2070-4992-2023-3-3-375. // Корпоративное управление и инновационное развитие экономики Севера: Вестник Научно-исследовательского центра корпоративного права, управления и венчурного инвестирования Сыктывкарского государственного университета. — 2023. — Т. 3, № 3. — С. 375–381 — EDN KSUOHB.
3. Шальнев, М.П. Совершенствование мер по противодействию мошенничеству коммерческих банков в системе экономической безопасности государства / М.П. Шальнев, И.И. Тимонин, А.А. Тургаева // Вестник евразийской науки. — 2024. — Т. 16, № S2. — EDN NLUINP.
4. Панина, Д.С. К вопросу о безопасности банковских платежей в современной российской практике / Д.С. Панина — DOI 10.34020/1993-4386-2024-2-61-66. // Сибирская финансовая школа. — 2024. — № 2(154). — С. 61–66 — EDN ETTBBG.
5. Ярашева, А.В. Государственные меры обеспечения финансовой безопасности населения / А.В. Ярашева, С.В. Макар — DOI 10.46320/2077-7639-2025-7-140-172-179. // Дискуссия. — 2025. — № 7(140). — С. 172–179 — EDN HQVLYB.
6. Щукарева, Д.Д. Экономические интересы участников банковской сферы и особенности защиты экономических интересов банковских учреждений / Д.Д. Щукарева // Форум молодёжной науки. — 2021. — Т. 2, № 4. — С. 126–135. — EDN VFDDTN.
7. Голубцов, С.А. Современные механизмы совершения преступлений в банковской сфере, способы противодействия / С.А. Голубцов, А.С. Карпов, К.В. Карпова — DOI 10.37691/2311-5351-2021-0-1-72-82. // Вестник Московского гуманитарно-экономического института. — 2021. — № 1. — С. 72–82. — EDN LNWQGT.
8. Ештокин, С.В. Обеспечение экономической безопасности коммерческих банков с использованием архитектуры нулевого доверия (Zero Trust) / С.В. Ештокин — DOI 10.36871/ek.up.p.r.2025.06.03.011. // Экономика и управление: проблемы, решения. — 2025. — Т. 3, № 6(159). — С. 91–99 — EDN QMBVXU.

91FAVN625
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

9. Запорожская, К.А. Мероприятия по обеспечению экономической безопасности коммерческого банка / К.А. Запорожская // Научный альманах Центрального Черноземья. — 2022. — № 1-3. — С. 97–100. — EDN JTNDGH.

10. Марченко, В.А. Современные направления и механизмы обеспечения экономической безопасности банковской системы России / В.А. Марченко // Сборник научных трудов кафедры правовой культуры и защиты прав человека: сборник научных работ преподавателей, аспирантов, магистрантов и студентов / Федеральное государственное автономное образовательное учреждение высшего образования «северо-кавказский федеральный университет», юридический институт. Том ВЫПУСК 4. — Ставрополь: Общество с ограниченной ответственностью "Издательско-информационный центр "Фабула", 2020. — С. 47–50. — EDN DBJAAM.

11. Ревенков, П.В. Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания / П.В. Ревенков, А.А. Бердюгин — DOI 10.24891/ni.13.9.1747. // Национальные интересы: приоритеты и безопасность. — 2017. — Т. 13, № 9(354). — С. 1747–1760 — EDN WTCYWU.

12. Русскевич, Е.А. Актуальные проблемы противодействия хищениям в системах дистанционного банковского обслуживания / Е.А. Русскевич — DOI 10.24412/2072-4098-2022-8251-70-76. // Имущественные отношения в Российской Федерации. — 2022. — № 8(251). — С. 70–76 — EDN ASHLZG.

13. Курбатов, А.Я. Защита прав потребителей финансовых услуг: монография / А.Я. Курбатов. — Москва: Юстицинформ, 2023. — 168 с.

14. Ганиев, Е.Ж. Проблемы защиты прав потребителей в сфере платежных услуг / Е.Ж. Ганиев — DOI 10.32743/UniLaw.2024.116.6.17442. // Universum: экономика и юриспруденция. — 2024. — № 6-1(116). — С. 57–61 — EDN EFVGGO.

15. Петрякова, Л.А. Мошенничество в банковской сфере: характеристика и предупреждение / Л.А. Петрякова, А.Л. Репецкая. — Москва: Издательский дом «Юрлитинформ», 2025. — 160 с. — EDN QVVKWR.

Tarasova Valeria Stanislavovna
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: Tarasova.vs@list.ru
RSCI: https://elibrary.ru/author_profile.asp?id=1205606

Academic adviser: **Amosova Natalia Anatolyevna**
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: naamosova@fa.ru
RSCI: https://elibrary.ru/author_profile.asp?id=386448

Modern mechanisms for protecting commercial bank clients from fraudulent actions by third parties: Russian practice and trends to 2025

Abstract. This article examines the transformation of the commercial bank client protection model in Russia in 2025. It demonstrates that, following a change in the legal framework, a transaction without the client's voluntary consent has been broadened to include not only cases of external unauthorized access but also transfers made by the client themselves under the influence of fraud or abuse of trust. Against this backdrop, the author examines how the criteria for assessing a bank's actions are changing: not only is verification of formal consent becoming more important, but also the credit institution's ability to promptly identify risks, suspend transactions, warn the client, and record the incident. The article analyzes the key indicators of the OBDS in 2024–2025, their quarterly dynamics, and the differences between the main channels of theft from individuals. Special attention is given to new security measures developed in 2025, including self-prohibition on credit, waiting periods, anti-fraud controls for cash withdrawals, digital services for prompt communication, and interdepartmental information exchange. It is concluded that the Russian model has become more consistent and multi-layered, but its most vulnerable link remains not the prevention stage, but the stage of subsequent financial compensation. Therefore, further development of legal regulation will likely involve clarification of banking diligence standards and bank liability criteria for fraud based on social engineering.

Keywords: commercial bank; client protection; banking fraud; OBDS; social engineering; anti-fraud; damage compensation

91FAVN625
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com