Меркулова Серафима Сергеевна
студентка
ФГБОУ ВО «Санкт-Петербургский государственный
архитектурно-строительный университет»
г. Санкт-Петербург

ФИНАНСОВЫЕ РИСКИ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА И АНТИФРОД-АНАЛИЗ В БАНКОВСКОМ СЕКТОРЕ

Аннотация: *в статье рассматриваются финансовые риски, возникающие при дистанционном банковском обслуживании и использовании социальной инженерии. На основе актуальных данных Банка России за 2025 год анализируются масштабы операций без добровольного согласия клиентов, роль антифрод-систем, проблема дроп-счетов и особенности расследования цифровых следов. Автор приходит к выводу, что эффективная защита требует не только технической блокировки подозрительных переводов, но и объединения риск-скоринга, поведенческой аналитики, межведомственного обмена данными и финансовой грамотности клиентов.*

Ключевые слова: *финансовые риски, мошенничество, антифрод, социальная инженерия, дроп-счета, дистанционное банковское обслуживание, расследование.*

Финансовое мошенничество в цифровой среде стало одной из наиболее заметных угроз для банков, граждан и предпринимателей. Дистанционные сервисы ускорили платежи и сделали их удобными, но одновременно повысили скорость вывода похищенных средств. Поэтому анализ таких операций является важной частью дисциплины «Финансовые риски, анализ и расследование финансовых махинаций»: здесь соединяются банковский риск-менеджмент, цифровые доказательства и правовая оценка поведения участников.

Актуальность темы подтверждается статистикой Банка России. В 2025 году объем операций без добровольного согласия клиентов вырос на 6,4%, а количество таких операций – на 31,2%. Всего злоумышленники похитили 29,3 млрд

рублей, при этом банки с помощью антифрод-систем предотвратили 134,16 млн мошеннических операций на сумму 13 895,4 млрд рублей [1]. Эти данные показывают, что защита становится эффективнее, но преступники меняют тактику и чаще используют массовые схемы на небольшие суммы.

Цель данной статьи – рассмотреть финансовые риски дистанционного мошенничества, методы антифрод-анализа и особенности расследования операций, совершенных под влиянием обмана. Объектом исследования выступают операции клиентов финансовых организаций, а предметом – признаки, по которым банк, регулятор и правоохранительные органы могут выявлять и пресекать финансовые махинации.

Главной причиной потерь остается социальная инженерия. Мошенник воздействует не столько на банковскую систему, сколько на человека: представляется сотрудником банка, курьером, оператором связи или государственным сервисом, просит назвать код, установить приложение удаленного доступа, перейти по фишинговой ссылке либо перевести деньги на «безопасный счет». Для банка такая операция часто выглядит как действие самого клиента, поэтому ключевой задачей становится оценка необычности поведения, а не только проверка правильности пароля или кода подтверждения.

Финансовый риск проявляется на трех уровнях. Первый – прямой ущерб потерпевшего. Второй – расходы банка на расследование, претензионную работу, возможное возмещение и усиление защитных процедур. Третий – системный риск, связанный с падением доверия к безналичным расчетам. Если граждане считают, что цифровой платеж невозможно защитить, они чаще переходят к наличным и менее охотно используют финансовые сервисы.

В 2025 году средняя сумма одной операции без добровольного согласия клиента снизилась до 18,6 тыс. рублей против 22,9 тыс. рублей в 2024 году [1]. На мой взгляд, это не означает снижения опасности. Скорее, мошенники стали дробить хищения, чтобы отдельный перевод выглядел менее подозрительным. Для расследования это создает проблему: ущерб по одному эпизоду может казаться

небольшим, но при объединении множества эпизодов формируется крупная преступная схема.

Антифрод-анализ строится на сравнении текущей операции с обычным поведением клиента. Учитываются сумма, время, устройство, геолокация, IP-адрес, новый или старый получатель, скорость ввода данных, частота переводов и история похожих операций. Например, если клиент обычно совершает бытовые платежи в своем регионе, но ночью отправляет деньги незнакомому получателю, операция должна получить высокий риск-балл. Однако банк не может блокировать все нестандартные платежи, потому что часть из них законна. Поэтому важен баланс между безопасностью и доступностью сервиса.

Значимым инструментом является база реквизитов злоумышленников. Закон «О национальной платежной системе» предусматривает ответственность банков за ненадлежащее проведение антифрод-мероприятий при переводе по реквизитам, содержащимся в базе Банка России [2]. Кроме того, с 2023 года действует онлайн-обмен между Банком России и МВД России через ФинЦЕРТ: после обращения потерпевшего правоохранительные органы могут быстрее получать данные о мошеннической операции и ее получателе [3].

Отдельная проблема – дроп-счета. Дропом называют лицо, которое предоставляет карту или счет для приема и вывода похищенных денег. По данным Банка России, в 2025 году средний срок жизни карты дропа резко сократился: если раньше операции могли идти более месяца, то теперь они часто пресекаются в течение дня, а средняя сумма операций на одного дропа снижена с 1–3 млн рублей до 100–150 тыс. рублей [4]. Это говорит о развитии контроля, но также о переходе преступников к более дробным цепочкам.

Расследование дистанционного мошенничества отличается тем, что основные доказательства находятся в цифровой среде. Важны логи банковского приложения, детализация звонков, переписка, сведения об устройстве, адреса входа, реквизиты получателя и дальнейшая цепочка переводов. Чем быстрее потерпевший сообщает о случившемся, тем выше вероятность остановить движение денег. Поэтому специальная кнопка в мобильном приложении банка, обязательная

для крупных банков с 1 октября 2025 года, имеет практическое значение: она упрощает подачу заявления и получение электронной справки для полиции [1].

Данные МВД подтверждают масштаб проблемы. В 2025 году число киберпреступлений в России снизилось с 775 тыс. до 663 тыс., но мошенничеств было зарегистрировано около 344 тыс., а материальный ущерб составил 189,5 млрд рублей [5]. Разница между банковской статистикой и данными МВД объясняется тем, что не все случаи проходят как перевод в приложении: часть потерпевших снимает наличные, передает деньги курьерам или использует несколько каналов.

Заключение.

Дистанционное финансовое мошенничество является комплексным риском для клиента, банка и финансовой системы. Данные за 2025 год показывают, что антифрод-системы предотвращают огромный объем хищений, но число выявленных операций без согласия клиента продолжает расти. Поэтому борьба с такими махинациями должна строиться не только на расследовании, но и на раннем выявлении рискованных сценариев.

Наиболее эффективной представляется комбинация технологий и организационных мер: поведенческий анализ операций, проверка новых получателей, выявление дроп-счетов, использование базы Банка России, быстрый обмен информацией с МВД и понятные предупреждения для клиентов. Чем быстрее риск превращается в конкретное действие банка и правоохранительных органов, тем ниже ущерб от финансовых махинаций.

Список литературы

1. Усков В.В. Классические методы оценки государственного противодействия экономическим преступлениям в России / В.В. Усков, Д.Н. Полтораченко // Московский экономический журнал. – 2025. – Т. 10, №2. – С. 22–32. – DOI 10.55186/2413046X_2025_10_2_35. – EDN QATDCC.

2. Моденов А.К. Количественная оценка информационной безопасности в условиях цифровой экономики: модели и методы / А.К. Моденов, В.В. Усков // Экономика: вчера, сегодня, завтра. – 2025. – Т. 15, №8–1. – С. 318–325. – DOI 10.34670/AR.2025.22.28.033. – EDN LXKAZQ.

3. Банк России. Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций за 2025 год // Официальный сайт Банка России. – URL: https://www.cbr.ru/analytics/ib/operations_survey/2025/ (дата обращения: 03.06.2026).

4. О национальной платежной системе: Федеральный закон от 27.06.2011 №161-ФЗ: ред. от 09.04.2026 // СПС КонсультантПлюс. – URL: https://www.consultant.ru/document/cons_doc_LAW_115625/ (дата обращения: 03.06.2026).

5. Между Банком России и МВД России начнется онлайн-обмен информацией о мошеннических операциях // Официальный сайт Банка России. – URL: https://www.cbr.ru/press/event/?id=17142 (дата обращения: 03.06.2026).