Доброва В.А.

Студентка предметно-цикловой комиссии банковского и страхового дела,

Колледж Среднерусского института управления – филиал РАНХиГС,

Г. Орёл, Россия,

Кузнецов М.Р.

Студент предметно-цикловой комиссии банковского и страхового дела,

Колледж Среднерусского института управления – филиал РАНХиГС,

Г. Орёл, Россия,

ДЕЯТЕЛЬНОСТЬ БАНКОВ ПО ЗАЩИТЕ КЛИЕНТОВ ПРИ ОСУЩЕСТВЛЕНИИ РАСЧЕТОВ

Аннотация*: Проблема защиты клиентов банков от мошенничества приобретает особую значимость в условиях развития цифровых технологий и увеличения объема безналичных расчетов. В настоящее время финансовая система постоянно сталкивается с угрозами мошенничества, особенно это касается сферу электронных платежей. Банки играют ключевую роль в обеспечении безопасности расчетных операций, защищая права и законные интересы своих клиентов. В данной статье мы рассмотрим правовые механизмы защиты клиентов банками при проведении операций с финансами.*

Ключевые слова: *защита клиентов, экономика, банки, электронные платежи, подозрительные операции.*

BANKS' ACTIVITIES TO PROTECT CLIENTS DURING TRANSACTIONS

Annotation: *The issue of protecting bank customers from fraud has become particularly important in the context of the development of digital technologies and the*

increasing volume of cashless payments. Currently, the financial system is constantly facing threats of fraud, especially in the field of electronic payments. Banks play a crucial role in ensuring the security of payment transactions and protecting the rights and legitimate interests of their customers. In this article, we will explore the legal mechanisms that banks use to protect their customers when conducting financial transactions.

***Key words**: customer protection, economics, banks, electronic payments, and suspicious transactions.*

Регулирование вопросов по защите клиентов банков от мошенничества осуществляется с помощью ряда федеральных законов и нормативных актов, наиболее распространенные из которых мы и рассмотрим [1]:

1. Гражданский кодекс Российской федерации. С начала 2026 года в России действуют обновленные критерии о блокировке карт и счетов при переводах, признанные обеспечить более надежную защиту клиентов от мошеннических действий.

2. Федеральный закон №161-ФЗ «О национальной платежной системе» в 2026 году рассматривает более расширенный список признаков подозрительных переводов, например:

- Наличие вредоносного ПО на устройстве клиента;
- Использование нетипичных параметров сессии ДБО;
- Совпадение данных получателя с информацией в государственной системе противодействия киберпреступлениям;
- Информация о риске компрометации данных электронного средства платежа;
- Особое внимание переводам через СБП между счетами клиента на сумму свыше 200 тыс. рублей, если они являются частью подозрительной цепочки операций.

Если операция проходит хотя бы по одному из признаков, то банк может ее приостановить для последующей проверки.

3. Федеральный закон №115-ФЗ «О противодействии легализации доходов, полученных преступным путем, и финансированию терроризма». Изменения включают в себя: автоматизация контроля – контроль за операциями стал преимущественно автоматизированным; контроль за операциями, осуществленными под влиянием мошенников – банки получили новые основания для блокировки, если операция проводится под влиянием мошенника (ч. 3.1 ст. 8); распространение правил блокировки на операции с цифровыми рублями.

4. Приказ Банка России №ОД-2506. Документ устанавливает обязательные для всех кредитных организаций признаки перевода денежных средств без добровольного согласия клиента. С марта 2026 года эти критерии распространяются на операции с цифровым рублем.

Эти законы устанавливают обязанности банков по обеспечению безопасности транзакций и выявлению подозрительных операций.

Согласно данным Центрального Банка Российской Федерации с 1 января 2026 года к признакам подозрительности переводов относятся [2]:

- Превышение времени обмена данными при бесконтактной операции;
- Смена номера телефона менее чем за 48 часов до перевода;
- Перевод незнакомому лицу после крупного перевода самому себе;
- Использование нетипичного провайдера или ПО;
- Нетипичная операция для клиента (необычная сумма, время или периодичность перевода);
- Перевод на реквизиты, находящиеся в базе данных Банка России о мошеннических операциях;
- Большое количество переводов от разных лиц;
- Снятие крупных сумм сразу после получения кредита или завершения вклада и т.д.

Рассмотрим этапы контроля банками подозрительных операций в 2026 году. Банковский контроль подозрительных операций осуществляется в

соответствии с Федеральным законом №115-ФЗ и разработанными на его основе правилами внутреннего контроля. Ключевыми этапами на данный момент являются:

1) Создание системы внутреннего контроля. Каждый банк создает и внедряет в работу собственную систему внутреннего контроля, основанную на Положении Банка России №242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах» [3]:

- Назначение уполномоченного должностного лица, ответственного за мониторинг соблюдения законодательных норм;
- Утверждение развернутых правил внутреннего контроля в кредитных организациях, которые регламентируют процедуры идентификации клиентов, порядок и хранение документации и организации обучения работников;
- Организация регулярного ознакомления сотрудников с новыми мошенническими схемами.

2) Идентификация клиента. Перед началом обслуживания в банке каждый клиент проходит обязательную идентификацию, которая включает в себя:

- Сбор персональных данных о физическом или юридическом лице;
- Проверка клиента по всевозможным государственным реестрам (террористы, дроперы и т.д.) с использованием личных документов на сайтах Росфинмониторинга и Банка России;
- Оценка уровня риска клиента на основе собранной информации.

Гистограмма 1 – Доля способов идентификации клиентов в банке в 2023-2025 годах (%) [4].

3) Мониторинг и выявление подозрительных операций. Автоматизированный мониторинг всех совершаемых операций позволяет оперативно выявлять нестандартные или высокорисковые транзакции. Наиболее распространенными критериями являются [4]:

- Частота операций. Более 10 контрагентов в день, более 30 зачислений/списаний в день;
- Суммы. Переводы свыше 100 тыс. руб. в день или 1 млн. руб. в месяц;
- Нетипичные схемы расчетов. Расходы организаций на личные нужды сотрудников;
- Операции, характерные для мошеннических схем, например, взлом, подмена реквизитов и другие.

4) Ограничительные меры. При выявлении подозрительных операций банк немедленно вводит соответствующие ограничения [6]:

- Временная приостановка операции. Банк уведомляет об этом через СМС или телефонный звонок службы безопасности;
- Временное ограничение использование карты (конкретного типа транзакций). Например, онлайн-банкинга, но при этом входящие переводы поступают;

- Предложение подтвердить перевод. В этом случае он сразу отправится получателю, но клиент берет всю ответственность по этому решению на себя;
- Отказ в проведении операции. Банк присылает клиенту отдельное сообщение, уведомляя об отказе;
- Прекращение обслуживания клиента. Это крайняя мера, которую банк использует только в случае, если нельзя убедиться в законности операций пот счету.

После обнаружения подозрительной операции банк проводит внутреннее расследование, запрашивая документацию, подтверждающую происхождение средств, а также анализируется финансовая история клиента.

5) Уведомление государственных органов. Все случаи подозрительных операций фиксируются и передаются в уполномоченные государственные структуры (Росфинмониторинг, Банк России).

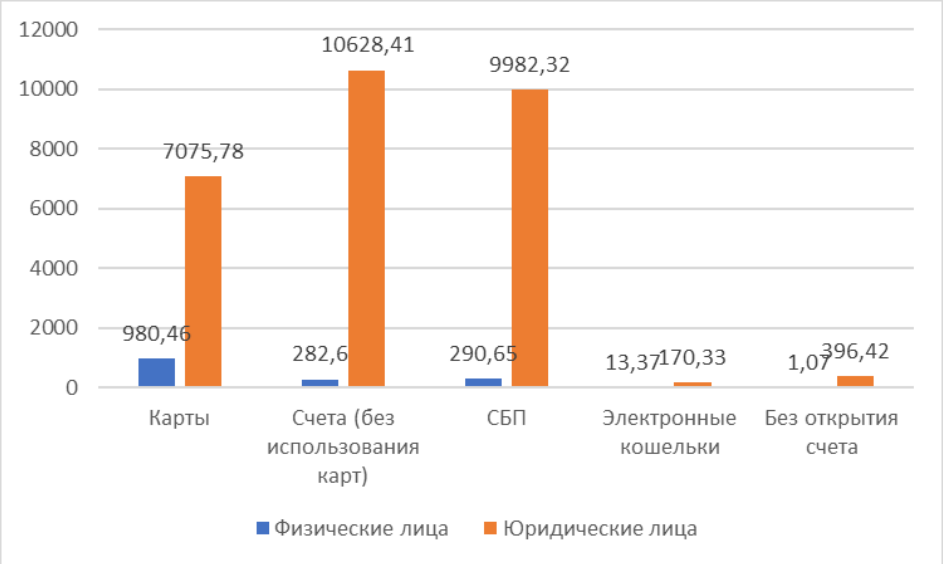
6) Реабилитационные процедуры. В случае ошибочно признанных подозрительными операций, клиенты проходят реабилитационную процедуру:

- Получение от банка письменных объяснений о причинах наложения ограничений на конкретную операцию;
- Направление в банк комплекта подтверждающих документов и официального заявления о пересмотре решения;
- Рассмотрение банком поступившего обращения в срок, не превышающий 15 рабочих дней.

Как происходит проверка подозрительных операций? Первичный анализ операции производит ИИ – компьютерные программы автоматически анализируют все операции по установленным критериям. Если операция кажется подозрительной, то она приостанавливается и передается на рассмотрение сотруднику банка. Далее расследование проводит сотрудник банка – запрашивает у клиента документы, подтверждающие законность перевода денежных средств. Затем банк выносит окончательное решение – при

предоставлении достоверных доказательств легальности операции – проводит ее. В противном случае доступ к счету может быть ограничен.

Далее мы рассмотрим причины и количество совершенных киберпреступлений в 2023-2025 годах. За период с 2023 по 2025 год произошел значительный рост числа киберпреступлений, направленных против банковских клиентов. Согласно данным Центрального Банка Российской Федерации, количество попыток хищения средств с банковских карт увеличилось на 38% в 2023 году и еще на 22% в 2024 году. Не смотря на такие негативные показатели за предыдущие годы в 2025 году доля успешных атак снизилась на 15% в связи с внедрением новых технологий и активному усилению контроля за операциями. Согласно данным Центрального Банка Российской Федерации, связанные с мошенническими операциями за 2025 год, совершенные без добровольного согласия клиентов, совершались с юридическими и физическими лицами по следующим типам:



Гистограмма 2 – типы мошеннических операций с физическими и юридическими лицами за 2025 год (тыс. рублей) [7].

Мошенники чаще всего убеждали граждан не только самостоятельно произвести операцию, но и перейти по фишинговой ссылке или скачать вредоносное ПО на свое устройство. Объем предотвращенных хищений в 2025 году составил 13 895,4 млрд рублей (больше на 386,36 млн рублей, чем в 2024 году).

Атаки с использованием фишинговых сайтов. В 2025 году Банк России направил информацию о 1002 сайтах с целью их последующего делегирования. Среднее время делегирования доменов сайтов (.ru; .рф; .su) составило от 3 часов до нескольких дней. Наибольший объем хищений был обусловлен применением мошеннических схем, комбинирующих методы социальной инженерии с использованием фишинговых веб-сайтов, имитирующих официальные интернет-ресурсы.

Банк России продолжает активно работать над ограничением на территории Российской Федерации доступа к ресурсам, с помощью которых распространяется информация о возможности получения финансовых услуг без наличия лицензии Банка России. В 2025 году количество ресурсов, к которым был ограничен доступ составило 37 416 единиц, что на 16,3% меньше аналогичного показателя в 2024 году.

Гистограмма 3 – мошеннические интернет-ресурсы, направленные регистраторам доменных имен (единиц) [7].

Проблема защиты клиентов от мошенничества при совершении операций продолжает оставаться одной из приоритетных задач государства и Банка России. Современная динамика роста демонстрирует рост числа правонарушений в данной области в связи с быстро развивающимся технологическим уровнем оснащенности мошенников. Банки активно внедряют

различные системы защиты и информируют клиентов о технике безопасности для минимизации и предотвращения данных случаев в практике. Обеспечение эффективной защиты клиентов банков остается важной задачей для поддержания общественного доверия к банковской системе и экономики нашей страны.

Список литературы:

1. Мошенничество с банковскими картами \ 2026 год \ Акты, образцы, формы, договоры \ КонсультантПлюс. URL: https://www.consultant.ru/law/podborki/moshennichestvo_s_bankovskimi_kartami/?ysclid=mlo7o7es4h147279524 (дата обращения 28.03.2026)
2. Какие признаки мошеннических переводов применяются с 1 января 2026 года? | Банк России. URL: https://cbr.ru/Reception/TopicalMessage/Page/11403 (дата обращение 28.03.2026)
3. Положение ЦБ РФ от 16.12.2003 N 242-П — Редакция от 15.11.2023 — Контур. Норматив. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=466231&ysclid=mmjp3dm4qa672682418 (дата обращения 29.03.2026)
4. Биометрия в банках: что это, зачем и к чему приведет | РБК Тренды. URL: https://trends.rbc.ru/trends/industry/5fd3ac6a9a79475333bfcb4f?ysclid=mlgv1nm4et832723760 (дата обращения 29.03.2026)
5. Как банк контролирует операции по банковской карте | Банки.ру. URL: https://www.banki.ru/news/columnists/?id=10967494&ysclid=mmjpfohcuw726542480 (дата обращения 29.03.2026)
6. Что может сделать банк, если посчитает операцию подозрительной Методические рекомендации. Что нужно знать предпринимателю об ограничениях операций по счету (Федеральный закон N 115-ФЗ и не только) (подготовлены Банком России, Росфинмониторингом, ФТС России, НСФР). URL: https://sudact.ru/law/metodicheskie-rekomendatsii-dlia-predprinimatelia-30-

chto-delat/metodicheskie-rekomendatsii/chto-mozhet-sdelat-bank-esli/?ysclid=mmjpilog51225465054 (дата обращения 01.04.2026)

7. Обзор операций, совершенных без добровольного согласия клиентов финансовых организаций | Банк России. URL: https://cbr.ru/analytics/ib/operations_survey/2025/ (дата обращения 01.04.2026)