

В ответе за тех, кого обслужили

Оборотная сторона цифровизации финансовых организаций — неуклонный рост попыток покушения мошенников на хранимые в банках денежные средства граждан. Благодаря новым требованиям ЦБ к антифрод-процедурам, вступившим в силу летом 2024 года, в противодействии мошенничеству наблюдается положительная динамика

Текст
АЛЕКСАНДРА КРЫЛОВА,
ОБОЗРЕВАТЕЛЬ «Б.О»

О динамике и дополнительных мерах регулятора

По данным Банка России, в 2024 году антифрод-системы кредитных организаций отразили 72,17 млн попыток злоумышленников похитить деньги клиентов. В 2023-м отраженных попыток было почти вдвое меньше — 34,77 млн. Также в 2024 году банки смогли спасти более чем в два раза больше средств клиентов. Если в 2023 году этот объем составлял 5,8 трлн рублей, то в 2024-м — уже 13,5 трлн.

В первом квартале 2025 года количество случаев покушения мошенников на средства, которые граждане держат в банках, выросло, достигнув почти половины всех попыток хищений в 2024 году — 43,8 млн, их общая сумма составила 4,6 трлн рублей. Вместе с тем, по данным, которые по запросу «Б.О» привел **Павел Коваленко**, директор центра противодействия мошенничеству компании «Информзащита», при этом фактические потери клиентов за этот период составили 6,9 млрд рублей. Это вдвое больше пресеченных случаев и примерно на треть меньше ущерба, зафиксированного годом ранее, заметил эксперт.

Положительная динамика подтверждает эффективность последовательных шагов Банка России, в частности ввода с 25 июля 2024 года дополнительных мер по защите от переводов мошенникам. Это и распространение понятия антифрода на операции, совершенные с согласия клиента, полученного в результате его обмана или злоупотребления доверием, и введение трех новых признаков подозрительных переводов. К ним относятся переводы на счета, по которым антифрод-системы банков фиксировали мошеннические операции; информация об уголовном деле, возбужденном в отношении получателя средств, а также данные от сторонних организаций, свидетельствующие о мошеннической операции.

Другими дополнительными мерами ЦБ являются описание алгоритма действий оператора при выявлении подозрительных переводов, а также возложение ответственности на оператора за игно-



рирование данных из антифрод-базы ЦБ РФ и блокировка подозрительных банковских карт и иных электронных средств платежа.

Антифрод-процедуры и антифрод-системы

Введение регулятором дополнительных мер по защите от переводов мошенником совпало с пиком роста попыток хищений средств со счетов граждан. Так, по словам **Александра Петровского**, заместителя начальника управления информационной безопасности ББР Банка, летом и осенью прошлого года его кредитная организация столкнулась с беспрецедентным ростом активности мошенников и массовыми случаями мошенничества в отношении клиентов. Для выхода из этой ситуации банку пришлось оперативно принять меры и усиливать системы защиты. Благодаря этому к первому кварталу 2025 года удалось добиться снижения уровня мошенничества в 3-4 раза по сравнению с пиковыми значениями предыдущего периода.

Системы защиты, или антифрод-системы, внедрены и развиваются в банках на протяжении как минимум шести лет. С осени 2019 года регулятор начал штрафовать кредитные организации за отсутствие у них программных средств распознавания мошеннических операций. Такие системы автоматизируют процессы мониторинга транзакций, обнаружения нетипичных для клиента операций, принятия решений и реагирования.

«Антифрод-системы анализируют поведение клиентов, суммы платежей и их привычки, обучаясь на реальных кейсах. Это позволяет эффективно выявлять подозрительные операции, включая дроперство. Обучение систем происходит на основе реальных данных, что повышает их точность», — рассказал **Михаил Петров**, начальник управления по контролю за внедрением и технологическим развитием РосДорБанка.

Поскольку процедуры противодействия мошенничеству неодинаковы в разных банках, системы, которые используются для их автоматизации, тоже различаются. Общее у них то, что процессы мониторинга и обнаружения подозрительных транзакций идут непрерывно в режиме, максимально приближенном к реальному времени. «Современные антифрод-системы предотвращают до 90% попыток мошенничества за счет автоматического скоринга каждого платежа (<50 мс) и поведенческой биометрии, остальные случаи обрабатываются операторами и информационными кампаниями», — пояснил **Павел Коваленко**, директор центра противодействия мошенничеству компании «Информзащита».

Вместе с тем даже самая быстрая и умная антифрод-система, позволяющая в режи-

ме реального времени анализировать транзакции, выявлять и блокировать подозрительные операции, обеспечивает только половину успеха в борьбе с операциями, совершенными без согласия клиентов банков, считает **Александр Петровский**. Вторая половина, по его мнению, зависит от бдительности, осведомленности самих клиентов и соблюдения ими базовых правил цифровой гигиены и безопасности. «Борьба с мошенничеством — это всегда партнерство между банком и клиентом», — заключил **Александр Петровский**.

Не вдаваясь в детали

Раскрывать подробности о действующих в банках антифрод-процедурах и автоматизированных системах, их поддерживающих, руководители служб ИБ кредитных организаций не хотят, опасаясь, что эта информация может стать достоянием злоумышленников. Завесу секретности немного приподнял представитель системного интегратора ИБ. «Чаще всего банки используют российские платформы, дополняя их собственными правилами, — констатировал **Павел Коваленко**. — Типовой уровень обнаружения держится на высоком уровне — 95–97% при ложных срабатываниях около 0,2%; пользователи также отмечают круглосуточную поддержку и SLA 24/7».

То, что в крупных банках такие процедуры хорошо работают, отмечала в своем выступлении на Уральском форуме и глава ЦБ РФ **Эльвира Набиуллина** в феврале 2025 года.

Вызовы

И от крупных банков, и от средних, и уж тем более от небольших кредитных организаций объявленные регулятором дополнительные меры по противодействию мошенничеству требуют расширения функционала антифрод-систем. Так, уже 1 сентября 2025 года в мобильных приложениях банков должна появиться специализированная «красная кнопка», нажав на которую клиент может подать заявление и в режиме онлайн, без визита в отделение банка получить справку для обращения в полицию. К этой же дате кредитным организациям предстоит автоматизировать процессы, обеспечивающие реализацию «периода охлаждения» до 48 часов для сомнительных переводов и кредитов от 50 тыс. рублей. Помимо этого банковские системы защиты должны непрерывно проводить автоматическую сверку с реестром ФИИ-ЦЕРТА (Центра взаимодействия и реагирования департамента информационной безопасности Банка России).

Как отметил **Павел Коваленко**, ключевые трудностями, с которыми уже столкнулись кредитные организации, старающиеся выполнить требования регулятора, это сжатые сроки, выдерживание ответа ≤60 мс при росте трафика и использование функции «красная кнопка» с устаревшими АБС и колл-центрами.

Схожую точку зрения высказал и **Александр Петровский**. По его словам, основным и наиболее значимым вызовом при внедрении новых функций и доработке антифрод-системы стала необходимость интеграции новых, современных решений и алгоритмов в существующую, исторически сложившуюся ИТ-инфраструктуру банка. Такая работа требует тщательного анализа, адаптации новых компонентов, обеспечения их совместимости со старыми системами, что может быть трудоемко и занимать значительное время.

Баланс безопасности и комфорта для клиентов

Хотя регулятор видит своей задачей защиту накоплений граждан в банках от покушений злоумышленников, такие меры защиты, как «период охлаждения» до 48 часов или блокировка платежных

карт, оказавшихся в антифрод-базе ЦБ, создают определенные неудобства для тех, кого они должны защищать. И банкам, которые дорожат лояльностью клиентов, очень важно найти баланс между защищенностью и удобством использования. Особенно он важен для не очень крупных кредитных организаций, для которых удержание клиентов — заметная статья расходов.

«В условиях, когда требования к проверкам значительно выросли, поддерживать этот баланс стало сложнее», — констатировал Александр Петровский. По его словам, увеличение количества и глубины проверок, которые необходимы для соответствия регуляторике и эффективной защиты средств клиентов, может влиять на скорость и простоту проведения некоторых операций. «Но мы работаем над тем, чтобы минимизировать неудобства», — заявил эксперт.

Больше всего жалоб поступает от клиентов, которым нужно было провести крупный платеж. Что касается не очень объемных платежей, то, как заверил Павел Коваленко, большинство клиентов, проводя их, не чувствует ограничений. «Девять из десяти платежей до 15 тыс. рублей проходят без дополнительного подтверждения, а среднее “трение” для пользователя выросло лишь на 0,1–0,2 с, что незаметно глазу», — заметил он.

Вектор развития антифрод-систем

«К сожалению, абсолютно совершенной защиты на сегодняшний день не существует, и именно это мотивирует банковский сектор и финтех развивать эффективные инструменты для борьбы с мошенничеством», — дополнила ответ Павла Коваленко **Евгения Боднар**, руководитель отдела сопровождения клиентов по кредитам и долгам компании «Финансово-правовой Альянс».

А это значит, что наступает пора подключать к борьбе с мошенничеством искусственный интеллект. Глубокая интеграция ИИ для анализа данных в реальном времени позволит автоматизировать обработку платежей и прогнозировать новые схемы мошенничества, адаптируясь к меняющимся тактикам злоумышленников, отметил Михаил Петров. При этом он не исключает из процесса борьбы с мошенничеством людей. По его словам, необходимо делать акцент на обучении моделей на расширенных наборах данных, включая паттерны поведения клиентов, геопозицию, устройства и историю операций. «В сложных случаях, таких как попытки обхода антифрод-защиты через альтернативные каналы или сомнения в легитимности операции, решение передается экспертам для прямой коммуникации с клиентом. Такой гибридный подход обеспечивает баланс между скоростью автоматизированных систем и точностью ручной верификации, минимизируя ложные срабатывания и повышая уровень защиты», — заключил Михаил Петров.

В условиях, когда разработка новых сценариев обмана держателей средств в банках поставлена злоумышленниками «на поток», от систем противодействия мошенническим операциям требуются гибкость и адаптивность. Антифрод-системы кредитных организаций должны находиться в полной готовности к появлению любых, даже самых неожиданных, схем обмана вкладчиков. **Б.О**

СОЦИАЛЬНАЯ РЕКЛАМА

Вы можете помочь детям победить болезнь, просто отправив СМС на короткий номер

6162

СМС пожертвования на лечение детей с онкологическими и гематологическими заболеваниями (от 10 до 15 000 рублей).
Услуга бесплатная и доступна абонентам МТС, Мегафон, Билайн и ТЕЛЕ2.

Подари Жизнь

любая сумма может спасти ЖИЗНЬ

www.podari-zhizn.ru