К ВОПРОСУ О ФИНАНСОВОМ МОШЕННИЧЕСТВЕ В БАНКОВСКОЙ СФЕРЕ

Хильченко Лана Владимировна, студентка
Долженкова Елена Владимировна, канд. экон. наук, доц.
E-mail: lenag1981@mail.ru

НТИ (филиал) УрФУ
г. Нижний Тагил, РФ

Аннотация. Проблема неправомерных операций, совершаемых без согласия клиентов в банковской сфере, представляет серьезную угрозу для финансовой безопасности и доверия к системе банковского обслуживания. В данной статье рассматриваются типы мошеннических действий, приводящих к таким негативным последствиям, а также обсуждаются меры и технологии, которые могут быть применены Центральным Банком для предотвращения и выявления подобных случаев. Проведен подробный анализ современной Антифрод-системы, предназначенной для защиты от различных методов несанкционированного доступа к информации, показана ее практическая направленность.

Ключевые слова. Банковская система, финансовое мошенничество, фишинговые атаки, методы предотвращения мошеннических действий, машинное обучение.

Современная банковская система предполагает высокий уровень доверия со стороны клиентов к финансовым учреждениям. Однако существует ряд случаев, когда клиенты сталкиваются с ситуациями, когда операции по их счетам совершаются без их согласия или знания. Это может быть следствием действий злоумышленников, внутренних нарушений или ошибок в работе банковского персонала.

В 2021 г. (рис. 1) сумма переводов составила 3,89 трлн руб. (количество операций 0,88 млрд ед.), а в 2022 г. сумма денежных переводов увеличилась до 14,35 трлн руб. (количество операций 3,05 млрд ед.). В 2023 г. общая сумма денежных переводов составила 30,99 трлн руб. (количество операций 7,15 млрд ед.).

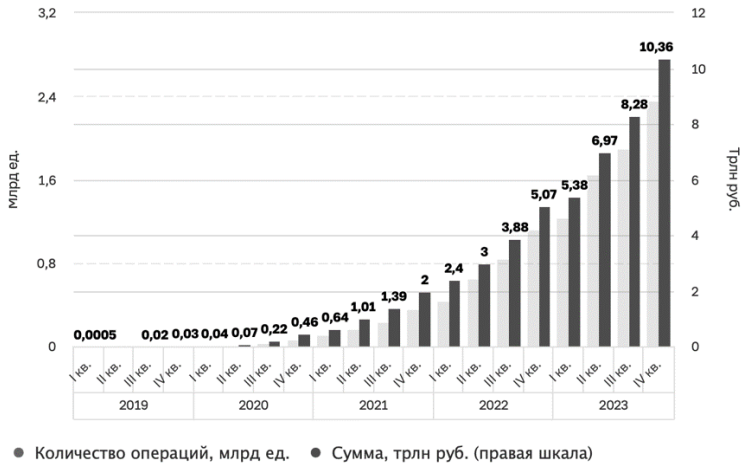

Рис. 1. Динамика безналичных переводов на территории РФ

С 2021 по 2023 г. происходит значительный рост объемов денежных переводов, однако увеличение переводов сопровождается появлением мошенников, которые крадут денежные средства без согласия клиентов. В 2021 г. объем операций без согласия клиентов составил 13 582,23 млн руб. (количество операций 1035,01 тыс. ед.), а в 2022 г. показатель увеличился до 14 165,44 млн руб. (количество операций 876,59 тыс. ед.). В 2023 г. объем операций составил 15 791,41 млн руб. (количество операций 1165,99 тыс. ед.).

В 2021 г. операции без согласия клиентов в общем объеме денежных средств составили 0,00130 %. В 2022 г. этот показатель снизился до 0,00097 %, а в 2023 г. увеличился до 0,00119 %. Следует отметить, что все рассмотренные показатели остаются ниже установленного Банком целевого показателя, который составляет 0,005 %.

Таким образом, в 2022 г. объем операций без согласия клиентов вырос на 4,29 % по сравнению с предыдущим годом в связи с активным развитием новых дистанционных платежных сервисов и увеличением объема денежных переводов с использованием электронных средств платежа. В 2023 г. этот показатель вырос на 11,48 % по сравнению с предыдущим годом. В результате принятых ЦБ мер по борьбе с мошенничеством в 2022 г. количество операций без согласия клиентов снизилось на 15,31 % по сравнению с предыдущим годом. Однако в 2023 г. произошло вновь увеличение из-за появления новых видов мошенничества, одним из которых являются фишинговые атаки.

Фишинговые атаки – это ситуации, когда злоумышленники создают поддельные веб-сайты, которые имитируют официальные сайты государственных органов, банков, популярных социальных сетей, маркетплейсов и других компаний. Целью таких атак является получение конфиденциальной информации пользователей, такой как логины, пароли, данные банковских карт, а также распространение вредоносного программного обеспечения (рис. 2, 3).

Рис. 2. Пример фишингового сайта
Источник: Фотобанк от TripTonkosti. –
URL : https://triptonkosti.ru/foto/fishingovye-shemy-eto-92-foto.html (дата обращения: 28.04.2024)

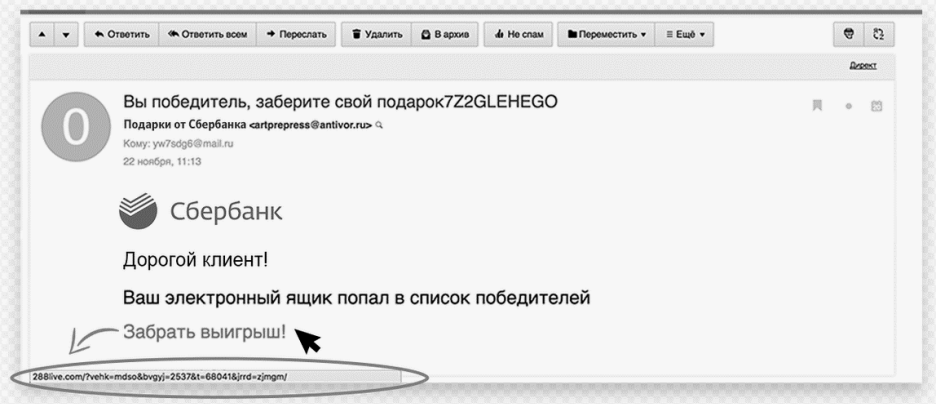

Рис. 3. Пример почтового вида фишинга
Источник: Фотобанк от TripTonkosti. –
URL : https://triptonkosti.ru/foto/fishingovye-shemy-eto-92-foto.html (дата обращения: 28.04.2024)

Рассмотрим основные методы, которые применяет ЦБ для предотвращения мошеннических действий:

– электронно-цифровая подпись с высоким уровнем обеспечения безопасности;

– применение криптографических алгоритмов для шифрования информации;

– использование средств распознавания устройств, с помощью которых клиенты осуществляют вход в личные кабинеты или пользуются системами «клиент-банк».

На современном этапе внедряются также Антифрод-системы, предназначенные для защиты от различных методов несанкционированного доступа к информационным системам. Ниже приведем их более подробную характеристику.

Первоначальная фильтрация данных в рамках алгоритма антифрода осуществляется в соответствии с определенными правилами, которые учитывают следующие параметры: количество операций за определенный период времени, сумма платежа или перевода, количество владельцев карты, установленный лимит на покупку, страна, в которой была выпущена карта, цифровой отпечаток, географическое расположение транзакции, история проведенных операций, стоп-листы и валидаторы.

Прошедшие фильтрацию транзакции получают от системы следующие метки:

– зеленая – «утверждено», фрод не обнаружен. Например, клиент регулярно оплачивает коммунальные услуги одинаковыми суммами в одно и то же время. Однако при обнаружении аномалий в поведении – скачка количества транзакций или их объема, система проведет дополнительные проверки и сменит цвет метки;

– желтая – «необходима ревизия», вероятность мошенничества повышена. Дополнительные проверки проводятся при обнаружении подозрительных ситуаций, таких как частые небольшие транзакции с одного счета на несколько других или регулярное списание средств небольшими суммами. Это может быть вызвано решением владельца магазина разделить оплату на отдельные части. И хотя нет ничего незаконного, система активизирует дополнительные проверки, такие как подтверждение личности по коду из СМС или отпечатку пальца. Иногда может потребоваться связаться с оператором для выяснения причин такого поведения.

Алгоритмы антифрода постоянно настраиваются и обновляются с использованием *Machine Learning*, который позволяет ИИ создавать поведенческие сценарии пользователей и прогнозировать их расходы на основе алгоритмов кластеризации.

Таким образом, неправомерные операции, проводимые без согласия клиентов, представляют собой серьезную угрозу в современной финансовой среде и непрерывно эволюционируют, поскольку злоумышленники постоянно разрабатывают новые методы мошенничества. Для эффективной борьбы с финансовым мошенничеством Центральному Банку необходимо постоянно обновлять и внедрять новые способы обнаружения и предотвращения незаконных операций. Это позволит снизить уровень риска для клиентов и обеспечить безопасность и надежность финансовых операций, основанных на доверии и прозрачности.