Дмитрий СЛОБОДЕНЮК
коммерческий директор ARinteg

АНТИФРОД В РОССИЙСКИХ РЕАЛИЯХ

Развитие антифрод-систем в России происходило, как и во всём мире, постепенно. Основными катализаторами стали зафиксированные инциденты. Нет худа без добра. События 2011–2012 гг., когда произошла массовая серия атак на ДБО, поначалу затронувших преимущественно юридических лиц и впоследствии распространившихся на физических лиц, банковский троян «Lurk» в 2014–2015 гг. и другие вредоносные программы способствовали развитию российских антифрод-решений.

Позже подключились законодатели. В 2018 г. был принят Федеральный закон от 27.06.2018 № 167-ФЗ «О внесении изменений в отдельные законодательные акты РФ в части противодействия хищению денежных средств», касающийся представителей кредитно-финансового сектора.

На тот момент было ощущение, что для некоторых финансовых организаций потери от фрода были невелики — меньше стоимости самих антифрод-решений.

Однако, в том же 2018 году Сбербанк опубликовал статистику, согласно которой с помощью внедрённой антифрод-системы удалось сохранить более 32 млрд рублей, принадлежащих вкладчикам. В том же докладе сделан особый упор на то, что большая часть инцидентов связана с социальной инженерией и так называемыми самопереводами. 86% из всех случаев социальной инженерии составили «самопереводы» денежных средств под влиянием мошенников.

На текущий момент большое влияние на внедрение и развитие антифрода оказывает не только 167-ФЗ, а целый ряд законов, постановлений и положений ЦБ РФ, направленный на противодействие мошенничеству в банковской сфере и глобально на развитие информационной безопасности в этом секторе. Например, 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём и финансированию терроризма» не связан напрямую с кражей денег с расчётных счетов кредитных организаций, однако действия, описанные в нём, вполне можно отслеживать и пресекать с помощью автоматизированных средств — AML и антифрод-систем.

ВИДЫ АНТИФРОДОВ

Транзакционный антифрод обрабатывает те потоки данных, которые находятся внутри банковской системы, в частности, внутри ДБО. Выявляет транзакции, не соответствующие типичным действиям клиента, и анализируют платёж по «чёрным спискам». Зачастую транзакционный антифрод уже интегрирован в ДБО его разработчиком.

Другим примером транзакционного антифрода является решение компании WhyHappen — резидента Сколково. Именно это решение было успешно внедрено компанией ARinteg в АО «Морской Банк» в 2019 году.

Антифрод WhyHappen позволяет осуществлять транзакционный анализ и через систему сбора и обработки данных коррелировать те события, которые с точки зрения банковских аналитиков нелегитимны, выявлять признаки реализации как уже известных мошеннических сценариев, так и

В 2018 году Сбербанк опубликовал статистику, согласно которой с помощью внедрённой антифрод-системы удалось сохранить более 32 млрд рублей, принадлежащих вкладчикам

фиксировать аномалии в поведении клиентов или сотрудников, приостанавливать подозрительные операции и/или информировать о них.

Анализ проводится по платёжным операциям, которые генерируются клиентом в различных каналах обслуживания: интернет-банк, мобильный банк, оплата картами в магазинах и в Интернет, обслуживание в дополнительных офисах банка, операции в банкоматах и пр. И по неплатёжной активности клиента, которая фиксируется в банковских системах, например, успешные или неуспешные попытки входа в ДБО, характер перемещения пользователя по страницам личного кабинета, смена контактной информации, время и геолокация проведения операции и ещё целый ряд параметров. На базе таких параметров может формироваться «вектор», характеризующий поведение клиента, строится его типовой профиль и фиксируются отклонения (аномалии). Кросс-канальный анализ, сочетающий оценку платёжного профиля и неплатёжного поведения клиента позволяет выявлять сложные схемы мошенничества или операции клиентов с признаками сомнительности (ПОД/ФТ), используя для этого максимум информации.

Сессионный антифрод позволяет отслеживать параметры пользовательской сессии и определять мошенническую активность на банковском сервисе. Собирая обезличенные данные о пользователе, устройстве, его окружении, поведении с цифровых каналов в рамках сессии, система фрод-мониторинга на основе машинного обучения и настроенных правил формирует уникальный профиль пользователя. Данные по денежным транзакциям пользователей банка (объёмы операций, реквизиты, получатели и прочее) не собираются. В основе анализа также лежат ретроспективные данные по прошлым сессиям пользователя. Обычно в процессе внедрения сессионного антифрода рекомендуется закладывать около трёх недель на обучение системы на трафике банка для профилирования пользователей и повышения качества обнаружения. Главная задача — выявить нетипичное, аномальное поведение пользователя на протяжении сессии, основываясь на многих факторах: с какого устройства выполняется вход, как пользователь двигает мышкой или водит пальцем по экрану смартфона, GPS-координаты, используются ли средства удалённого управления, ведётся ли постороннее подключение к сессии, заражено ли устройство и многое другое. Анализируются десятки параметров. Пример сессионного антифрода — Kaspersky Fraud Prevention. В 2018 году эксперты ARinteg успешно интегрировали решение Kaspersky Fraud Prevention в одном из крупнейших российских банков.

Важно отметить, что системы сессионного фрод-мониторинга применимы не только для обнаружения мошеннической активности с пользовательскими учётными записями в интернет- и мобильном банкинге. Оценка риска заявки на выдачу кредита, выявление мошенничества на P2P и C2C-переводах, в случаях, когда пользователь даже не авторизован в системе — также востребованные сценарии в банковской сфере. И сессионный антифрод решает эти задачи. Ещё один отдельный и серьёзный вопрос, который может закрыть антифрод (не каждый!) — выявление фродовых случаев, связанных с отмыванием денежных средств через различные учётные записи с использованием разных устройств и комбинаций скомпрометированных аккаунтов юридических и физических лиц. При этом легитимный пользователь может не знать, что его учётная запись онлайн-банка была скомпрометирована и используется в преступных целях.

Комбинированный антифрод сочетает сессионный и транзакционный анализ.

КАКИЕ РИСКИ ЗАКРЫВАЮТ АНТИФРОД-СИСТЕМЫ

Любая система безопасности направлена на снижение тех или иных рисков. Банки и финансово-кредитные организации, помимо прочего, сталкиваются с двумя типами рисков: потеря денежных средств (своих или клиентов) и регуляторный риск. При этом требования регуляторов для банков зачастую строже, чем требования безопасности, т.к. штрафные санкции могут быть значительными.

Антифрод-системы позволяют реализовать как защиту от угроз информационной безопасности в банке, так и обеспечить выполнение требований регулятора, т.е. управлять регуляторным риском.

Нельзя забывать и про репутационный риск в случае инцидентов безопасности и освещения их в СМИ, социальных сетях. Негативный опыт даже одного пользователя может спровоцировать отток лояльных клиентов, уменьшение объёма новых клиентов, снижение уровня доверия к банку, повышение затрат на восстановление репутации бренда.

Банк обязан наблюдать за платёжным поведением клиента. Согласно Федеральному Закону 161-ФЗ «О национальной платёжной системе» при приёме к исполнению распоряжения клиента оператор по переводу денежных средств обязан удостовериться в праве клиента распоряжаться денежными средствами. В рамках реализуемой им системы управления рисками оператор по переводу денежных средств определяет процедуры выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, на основе анализа характера, параметров и объёма совершаемых его клиентами операций (осуществляемой клиентами деятельности).

В соответствии с Положением 382-П Банка России оператор по переводу денежных средств, банковский платёжный агент (субагент), оператор услуг платёжной инфраструктуры обязаны обеспечить выявление фальсифицированных электронных сообщений, в том числе имитацию третьими лицами действий клиентов при использовании электронных средств платежа, и осуществление операций, связанных с осуществлением переводов денежных средств, злоумышленником от имени авторизованного клиента (подмена авторизованного клиента) после выполнения процедуры авторизации.

В случаях, если нарушения организацией требований законодательства влияют на бесперебойность функционирования платёжной системы либо на услуги, оказываемые участникам платёжной системы и их клиентам, Банк России применяет одну из следующих мер принуждения:

1. направляет предписание об устранении нарушения с указанием срока для его устранения;
2. ограничивает (приостанавливает) предписанием оказание операционных услуг, в том числе при привлечении операционного центра, находящегося за пределами Российской Федерации, и (или) услуг платёжного клиринга.

Сама возможность такой санкции, как ограничение оказания операционных услуг, например, запрет на приём вкладов от физических лиц и ограничение выдачи кредитов юридическим лицам, требует от кредитной организации уделять значительное внимание вопросам, связанным с противодействием мошенничеству.

В качестве наказания ЦБ может также перевести банк на ежедневную отчётность на срок от полугода до нескольких лет.

Один раз в два года банки обязаны проходить независимый аудит инфраструктуры платёжных систем — документированную независимую экспертизу состояния защищённости платёжных систем в соответствии с требованиями Положения ЦБ от 09.06.2012 № 382-П.

Банк обязан выявлять факты отмывания денежных средств. Отмывание денег является серьёзной проблемой и влияет на национальную безопасность, так как подобная деятельность помогает финансировать организованную преступность, способствует коррупции и усиливает социальные разногласия. В таких мошеннических схемах финансовые организации становятся невольными жертвами.

В Положении Банка России 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма» перечислены факторы, влияющие на оценку риска клиента, к которым в том числе относится совпадение идентификатора устройства клиента с устройством из списка подозрительных. Финансовая организация обязана уведомлять Банк России о мошеннических аккаунтах и устройствах, задействованных в схемах по отмыванию средств.

Все указанные регуляторные риски успешно закрываются своевременным внедрением системы антифрода.

ВЫВОД

Банковское мошенничество само по себе никуда не денется. Но внедрение организациями лучших практик и систем по борьбе с фродом и соблюдение требований регулятора могут существенно повлиять на всю кредитно-финансовую экосистему. Тем более, что российские разработчики предлагают достойные и конкурентоспособные антифрод-решения.

Внедрение системы антифрода является необходимым, но недостаточным условием для эффективного противодействия мошенничеству и выполнению требований регулятора. Помимо внедрения самой системы, необходимо выстроить процессы мониторинга и реагирования, взаимодействия с клиентами и смежными подразделениями внутри банка, а также с другими кредитными организациями. Необходимо поддерживать в актуальном состоянии базу правил антифрод системы, постоянно её модернизировать с учётом текущей ситуации, опыта других банков и появления новых мошеннических схем.

* * *

Также нужно отметить, что внедрение любой кросс-канальной антифрод-системы — это ещё и довольно сложный интеграционный проект, т.к. необходимо собирать и анализировать данные из различных каналов обслуживания клиентов и банковских ИТ систем. Здесь и системы Интернет-банкинга, АБС, CRM, процессинг, шлюзы на поставщиков услуг и т.д. Поэтому такие проекты, зачастую, выполняются в партнёрстве между производителем антифрод-решений и системными интеграторами. В рамках такого партнёрства, компании могут предложить оптимальное решение и привнести опыт других заказчиков и опыт работы экспертов, экономя время, деньги и усилия для кредитной организации.