Кросс-канальная система противодействия мошенничеству: выявить сложные схемы

Аналитические решения по поиску подозрительных операций в отдельных каналах обслуживания клиентов не позволяют банкам выявить сценарии мошенничества, в которых задействовано сразу несколько, в том числе удаленных, каналов обслуживания. Комплексный характер обеспечивает аналитическая платформа, на базе которой строится кросс-канальная система противодействия мошенничеству, позволяющая не только своевременно выявлять сложные мошеннические сценарии, но и с помощью алгоритмов машинного обучения идентифицировать неизвестные ранее схемы.

Кросс-канальная система противодействия мошенничеству: выявить сложные схемы

Максим ФЕДОТОВ,
Делойт в СНГ, старший менеджер отдела форензик

Проблема выявления мошеннических операций становится для банков все более острой, особенно с развитием удаленных каналов обслуживания клиентов, а также участившимися случаями хакерских атак, в результате которых банки несут прямые убытки, репутационные потери, а также теряют доверие клиентов. С целью предотвращения мошенничества внедряются специализированные аналитические решения, ориентированные на выявление подозрительных операций в отдельных каналах обслуживания клиентов. Однако такой подход не позволяет выявить сложные сценарии мошенничества, в которых задействовано несколько каналов обслуживания, в том числе удаленных. Другой проблемой является сложность выявления мошенничества с участием персонала банка. К тому же злоумышленники постоянно изменяют применяемые ими мошеннические схемы и подходы, используют новые бреши в безопасности банковского программного обеспечения, а также прибегают к методам социального инжиниринга в отношении клиентов и сотрудников банка.

Принципы построения кросс-канальной системы

Подход к построению системы противодействия мошенничеству должен носить комплексный характер и охватывать внутренние процессы банка, построение адекватной им организационной струк-

Максим ФЕДОТОВ

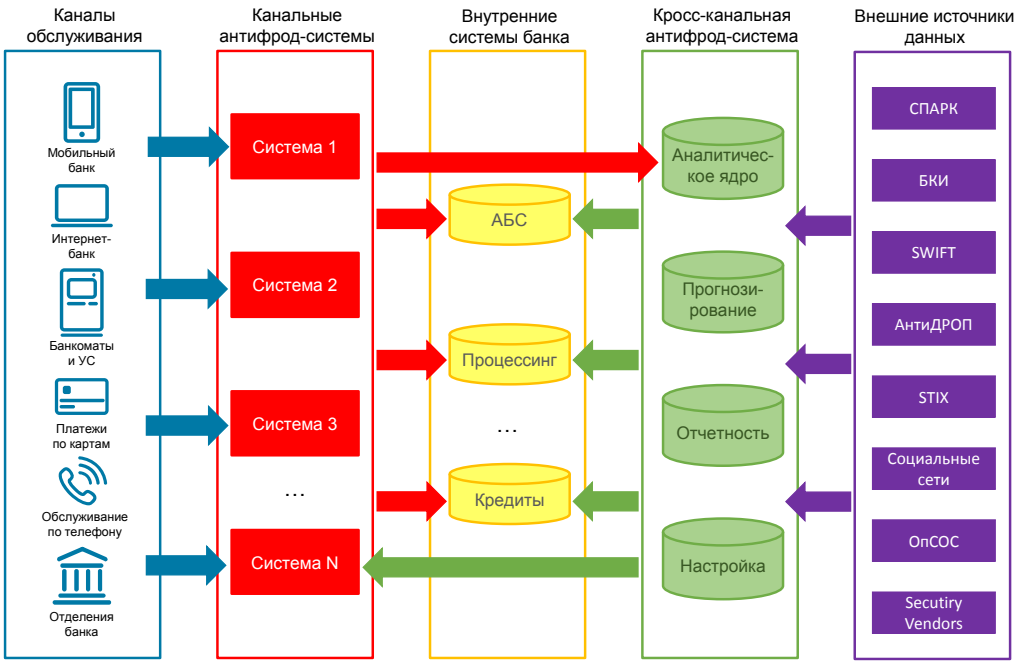
туры, а также обучение персонала в области информационной безопасности и управления рисками, использование современных технологий, построение эффективной системы управления и принятия решений по выявленным инцидентам.

Одним из ключевых элементов такой комплексной системы является аналитическая платформа[1], позволяющая обрабатывать большие массивы разнородной информации, собранной как из внутренних источников, содержащих данные о клиенте, его операциях во всех каналах обслуживания, сотрудниках банка, с которыми он взаимодействовал, так и из внешних источников данных, включая государственные реестры, системы межбанковского обмена информацией, социальные сети и др.

На базе аналитической платформы строится кросс-канальная система противодействия мошенничеству (рис. 1), позволяющая

Рисунок 1

Место кросс-канальной системы в IT-ландшафте банка



[1] Согласно исследованию Gartner в 2016 г. лидерами в области разработки аналитических платформ признаны такие гиганты, как SAS, IBM, Dell, а также более узкоспециализированные игроки KNIME и RapidMiner, предлагающие свои решения на основе свободно распространяемого кода (open-source). В исследовании упоминается и российский разработчик «Прогноз», названный нишевым игроком.

Кросс-канальная система противодействия мошенничеству: выявить сложные схемы

своевременно выявлять сложные сценарии, в которых задействовано несколько каналов обслуживания (например, мобильный и интернет-банк, банкоматы, устройства самообслуживания, покупки через интернет и различные приложения для смартфонов, а также операции, совершаемые с участием сотрудников в отделениях банка), и, кроме того, с помощью алгоритмов машинного обучения идентифицировать неизвестные ранее мошеннические схемы. Результаты анализа передаются в канальные системы фрод-мониторинга, что повышает уровень выявления мошенничества.

Ядро кросс-канальной системы строится на основе математических алгоритмов, позволяющих проводить анализ на базе статистических правил, направленных на выявление уже известных случаев мошенничества, поведенческих профилей клиентов, сотрудников банка, счетов и операций, позволяющих идентифицировать неизвестные ранее мошеннические сценарии, а также применять расширенные аналитические методы (кластерный и регрессионный анализ, метод нечеткой логики, нейронные сети, прогнозное моделирование), которые служат для выявления сложных кросс-канальных сценариев мошенничества (рис. 2).

Рисунок 2

Методы и алгоритмы интегрированной модели

Максим ФЕДОТОВ

Помимо аналитического ядра, современная кросс-канальная система противодействия мошенничеству предоставляет богатый инструментарий для проведения расследования инцидентов, включая фильтры, сквозной поиск по любым объектам и атрибутам аналитических моделей, визуальные средства анализа, позволяющие проверять гипотезы любой сложности.

Система отчетности кросс-канальной системы позволяет получить полную и объективную картину мошенничества, собрать статистику по размеру ущерба, видам мошеннических операций, каналам обслуживания клиентов, проследить динамику изменения значений индикаторов риска, а также оценивать ключевые показатели эффективности противодействия мошенничеству.

Как уже говорилось, реализация кросс-канальной аналитической системы возможна как на решениях от известных производителей, так и на свободно распространяемых платформах с открытым кодом, что позволяет существенно снизить капитальные вложения на приобретение лицензий и оплату технической поддержки от вендора.

Основные преимущества кросс-канальной аналитической системы

Внедрение кросс-канальной аналитической системы позволяет банкам снизить не только прямые потери за счет повышения качества распознавания сценариев мошенничества, но и косвенные затраты за счет сужения «серой» зоны, в которую попадают сомнительные операции, обработка которых требует значительных ресурсов, включая звонки клиентам, работу с претензиями, проведение расследования и др.

Гибкие подходы и возможность прогнозирования уровня мошенничества позволяют банкам более оперативно выводить новые продукты и услуги, оказываясь на шаг впереди конкурентов. Более того, снижение числа ложных срабатываний системы фрод-мониторинга по легитимным операциям, повышение надежности и защищенности каналов обслуживания обеспечивают более комфортное использование банковских продуктов со стороны клиентов, что способствует повышению их лояльности банку.

Внедрение кросс-канальных аналитических систем уже показало свою эффективность в крупных международных финансовых организациях. Также мы наблюдаем возрастающий интерес со стороны российских и казахстанских банков к системам противодействия мошенничеству, в том числе аналитическим решениям нового поколения, демонстрирующим свою эффективность уже на этапе пилота.