БАНКОВСКИЙ АНТИФРОД — ТРАНСФОРМАЦИЯ ИЛИ СМЕНА ПАРАДИГМЫ?

Сергей Афанасьев,
Исполнительный директор, Начальник управления расследования мошенничества, Банк "Ренессанс Кредит"

Банковский антифрод – молодая профессия, которой не учат в университетах. Поэтому основные инструменты мы (антифрод-специалисты) обычно берем из трех дисциплин:

- Аудит – дает нам различные инструменты ревизий, сплошных и выборочных проверок, инспектирований и т.д.;
- Криминалистика – содержит богатый инструментарий для выявления мошенничества;
- Аналитика – позволяет использовать математический аппарат для разработки антифрод-инструментов и оценки их эффективности.

За годы работы в антифроде у нас накапливается большое количество инструментов. Когда появляются новые

Рис.1. Процентная маржа снижается.

мошеннические схемы, мы разрабатываем новые инструменты, старые не выбрасываем, поэтому со временем возникает необходимость структурировать весь инструментарий, оценить его эффективность и по возможности оптимизировать. Но основная проблема сейчас не в количестве инструментов, в ближайшем будущем нас ожидают изменения другого характера.

ИГРА НА ПОНИЖЕНИЕ

Ряд грядущих изменений в банковском антифроде (да и в банковской отрасли в целом) связан с регуляторными ограничениями на полную стоимость кредита (ПСК). По данным Банка России за последние 2 года процентная маржа по кредитам и депозитам "до 1 года" снизилась с 17,3% до 14,2%, а по кредитам и депозитам "свыше 1 года" – с 9,2% до 7,8%[1]. В относительном выражении снижение составило 18% и 15% соответственно. А это значит, что при сохранении объемов кредитования, банкам приходится снижать все, что в эту маржу заложено – стоимость риска, операционные расходы и, возможно, чистую прибыль. И поскольку фрод-потери заложены в стоимость риска, то перед нами стоит задача снизить уровень мошенничества. С другой стороны, антифрод – это персонал и ИТ-системы, затраты на которые заложены в операционные расходы. И этот показатель нам тоже придется снижать. В результате отрасль оказываются в положении, когда надо повышать эффективность антифрода и при этом тратить на это меньше денег.

DARKNET — НАЙДЕТСЯ ВСЕ!

Многое о банковском мошенничестве можно узнать в Даркнете. Есть открытые и закрытые форумы на которых общаются мошенники и размещают свои заказы и предложения. На этих форумах можно найти много интересной информации, в том числе про "эффективность" банковского анифрода.

В частности можно увидеть, что банковские продукты активно продают мошенникам. Это огромный бизнес. Есть

[1] Процентная маржа - разница ставок по кредитам и депозитам. На графиках показана процентная маржа по продуктам для физических лиц.

масса объявлений где ищут дропов (наемников) для оформления дебетовых карт и последующей обналички. Также покупают и продают "оленей" (подставных лиц, обычно низкого социального статуса) под оформление кредитов.

Продаются и банковские методики. Спросом пользуются инструкции по андеррайтингу. Стоимость одной такой инструкции объемом на 100 страниц примерно 4000 рублей.

Кроме того "хантят" сотрудников банков. Ищут "своего" человека в банке для помощи в оформлении кредитов. Одно из требований к "кандидату" – позиция на уровне одобрения кредита.

Кроме того на этих форумах можно найти объявления о покупке и продажах клиентских баз данных, запросы "как обойти защиту конкретного банка", предложения "исправить" кредитную историю и многое другое.

Причем многие мошеннические схемы существуют уже много лет. И судя по количеству объявлений такие вопросы как борьба с "оленями" или "дропами" до сих пор не сняты с повестки.

БУДУЩЕЕ, КОТОРОЕ УЖЕ НАСТУПИЛО

Прошлым летом Герман Греф выступал в Калининграде перед студентами-юристами Балтийского университета. И эта цитата из его выступления разлетелась по многим новостным ресурсам:

"Назовите мне типы нейронных сетей? Не знаете двоечники! Хочу вам сказать, что это недопустимо. Вы – студенты вчерашнего дня!"

Это высказывание вызвало бурную дискуссию на тему того – нужно ли юристам знать о нейронных сетях и бросать ли свою профессию, переучиваясь на датасайнтистов? Наверно это дискуссионный вопрос, и лучше всего на него ответят сами юристы. Но на сегодняшний день можно однозначно утверждать, что антифрод-специалисты обязаны знать как устроены современные нейронные сети и как работают технологии, построенные на этих нейросетях. На это есть как минимум 7 причин.

1. Макияж от Яндекса

Практически любая современная фото-биометрическая система, представленная сегодня на рынке, работает на сверточных нейронных сетях. Принципы работы сверточных нейронных сетей достаточно простые – они выделяют контрастные участки на фотографии и в результате сравниваются только контуры на лице (без глубокой детализации).

Григорий Бакунов, директор по распространению технологий Яндекса и эксперт по нейросетевым технологиям, разработал со своими единомышленниками генетический алгоритм, который создает случайный макияж, ломающий фото-биометрические системы. Результат работы алгоритма простой – на лицо наносится несколько ярких полос и точек, которые сверточная нейронная сеть считает за контуры на лице, и в результате фото-биометрическая система не может сравнить такое лицо с базовой фотографией (считает их разными)[2]. Такой макияж позволяет, например, избежать распознавания человека городскими камерами видеонаблюдения,

[2] http://telegra.ph/Novyj-makiyazh-korolya-07-14

подключенными к биометрии. Именно поэтому Григорию пришлось "свернуть" проект, так как по его мнению, этой технологией могут воспользоваться преступники.

2. GANы против фото-биометрии

Еще один враг фото-биометрических систем – генеративно-состязательные сети (англ. Generative Adversarial Network, сокращенно GAN). GANы могут синтезировать образцы очень высокого качества за счет работы двух соревнующихся нейронных сетей – генератора, который синтезирует образцы (фотографии, видео и т.п.) и дискриминатора, который пытается отличить подделку от оригинала. И несмотря на то, что GANы были придуманы совсем недавно (в 2014 году), на этой архитектуре было разработано уже много различных приложений (например нашумевшая PRISMA, обрабатывающая фотографии в стиле известных художников).

В прошлом году на ресурсе Reddit пользователь под ником deepfakes опубликовал фейковые ролики "взрослого" содержания, в которых лица действующих героинь были заменены на лица голливудских актрис. Позже было выпущено приложение, которое позволяет создавать подобные ролики пользователям без специфических знаний технологий машинного обучения[3].

Эта разработка продемонстрировала еще одну уязвимость фото-биометрических систем – технологию Liveness detection, которая была разработана для защиты фото-биометрической системы от прохождения верификации по фотографии. Такие технологии как deepfakes позволят подставлять фотографии любого человека в онлайн видео-трансляцию и с помощью такого видео проходить фото-биометрическую верификацию и Liveness detection.

3. Face ID vs. 3D-GAN

Но под угрозой не только фото-биометрия. 3D-биометрия тоже уязвима и может быть взломана с помощью все тех же GANов.

Сразу после выхода IPhone X в СМИ появилась новость, что хакеры всего мира принялись взламывать дорогостоящую технологию Face ID, построенную на принципах 3D-биометрии. Через несколько недель после выхода этой новости исследователи из вьетнамской компании Bkav опубликовали видео, в котором продемонстрировали взлом Face ID с помощью маски, напечатанной на 3D-принтере. Как утверждали сами исследовали из Bkav, их подход не масштабируем, поскольку для создания 3D-маски необходимо затратить много усилий в части сканирования лица владельца айфона. И в их словах можно было бы не сомневаться, если бы не было GANов, а именно нейронных сетей под названием 3D-GAN, которые умеют по 2D-изображению генерировать 3D-модели объектов высокого качества[4]. И если, например, обучить такую нейронную сеть на фотографиях лиц, то можно будет создать 3D-маску любого человека, фотография которого доступна, например, в социальных сетях.

4. Голосовая биометрия и Lyrebird AI

Другой проект под названием Lyrebird позволяет генерировать речь по загруженному слепку голоса, продолжитель-

[3] https://deepfakes.cc/

[4] https://arxiv.org/pdf/1610.07584.pdf

ностью всего одну минуту[5]. Для генерации речи используют другую архитектуру порождающей нейронной сети – WaveNet, разработанной в Google DeepMind, которая на сегодняшний день является одной из лучших нейронных сетей для генерации речи.

Про Lyrebird некоторые специалисты с испугом пишут о его потенциале для преступников[6], другие утверждают, что одной минуты слепка недостаточно для генерации приличной речи. Но обе стороны сходятся во мнении, что такие технологии представляют угрозу для сервисов голосовой биометрии (даже с наличием функции Liveness detection – защита от записанного голоса).

И хотя голосовые слепки сложнее достать, чем фотографии, такие проекты будут популярны среди мошенников для взлома голосовой биометрии.

И становится очевидным, что в биометрической гонке выиграют технологии, которые используют недоступные в открытых источниках данные – такие как отпечаток пальца, рисунок вен, радужная оболочка глаза и др.

5. Мошенничество с Apple Pay

Но даже отпечатки не панацея, если использовать их не там где надо. В бесконтактной технологии оплаты покупок Apple Pay отпечаток пальца владельца айфона используется для входа в Apple-кошелек и последующей оплаты покупки. Как утверждала компания Apple, разработавшая эту технологию совместно с международными платежным и системами, такая технология более удобна для клиента и лучше защищена, чем классические ПИН-коды (нельзя подсмотреть ПИН-код во время его ввода, владельцу Apple-кошелька не надо помнить или записывать ПИН-коды всех привязанных карт и т.д.). Однако, как это обычно бывает, мошенники пришли оттуда откуда их не ждали – из социальной инженерии.

На телефон карточного клиента банка поступает звонок или смс от мошенника, который представляется сотрудником банка. У клиента спрашивают реквизиты карты и одноразовый смс-пароль, который приходит клиенту на телефон. Далее мошенник привязывает карту клиента к своему Apple-кошельку, подтверждает привязку смс-паролем и своим отпечатком пальца. После этого мошенник может оплачивать товары и услуги с карты клиента своим айфоном, используя вход в кошелек по отпечатку пальца.

Обычно, при классической социальной инженерии, мошенники выводили деньги на web-кошельки. Основной минус web-кошельков как инструмента вывода для мошенников состоит в том, что на web-кошельках выставлены лимиты на каждую операцию (на неавторизованные web-кошельки действует регуляторное ограничение – 15 000 руб.) В результате мошенникам приходилось делать несколько звонков потенциальной жертве, спрашивать несколько одноразовых смс-паролей. А с технологией Apple Pay таких неудобств не возникает.

Причем стоит отметить, что данный вид мошенничества практиковался в США еще в 2015 году, о чем писали эксперты по безопасности на зарубежных ресурсах, описывая способы защиты от

[5] https://lyrebird.ai/demo/

[6] https://thenextweb.com/insights/2018/01/22/i-trained-an-ai-to-copy-my-voice-and-scared-myself-silly/

этого мошенничества[7]. На российских интернет-ресурсах эта информация также появлялась в 2015 году[8]. В Российский банкинг этот вид мошенничества пришел в 2017 году, практически сразу после запуска Apple Pay в России. Но не смотря на обилие информации в СМИ, российские банки оказались не готовы к этому виду мошенничества и не настроили свои фрод-мониторинги вовремя. Впрочем одной из возможных причин могло стало то, что Apple не предупредили необходимые службы российских банков о данном виде мошенничества и о способах защиты от него.

6. Чат-бот «Попрошайка»

Другой классический вид социальной инженерии – это просьбы занять денег, отправленные с ворованных аккуантов в Skype или в социальных сетях.

В интервью, опубликованном на хабре в 2015 году, skype-мошенник рассказывает, как организован этот преступный бизнес. Обычно для этой работы нанимают молодых людей, дают им прочесть несколько книг по психологии. После этого их сажают в офис за компьютер, выдают ворованные аккаунты, web-кошельки, и они сидят и общаются с потенциальными жертвами, "занимая" у них деньги. Оплата примерно 40%–50% с выручки, но не более 100 000 руб. в месяц. Так организована социальная инженерия сейчас. Но в ближайшем будущем возможно все сильно поменяется. Так летом прошлого года в социальных сетях обсуждали тестирование чат-бота, который за сутки собрал с пользователей социальных сетей 15 000 долларов.

Так летом прошлого года в социальных сетях обсуждали тестирование чат-бота, который за сутки собрал с пользователей социальных сетей 15 000 долларов.

К счастью таких чат-ботов пока пишут исследователи-энтузиасты, и этим ботам пока еще далеко до профессиональных skype-мошенников. Однако такие технологии легко масштабируются, и затраты на их разработку разовые, не надо отдавать половину выручки наемникам.

7. RE:SCAM – отвлекает мошенников

Другой чат-бот, разработанный новозеландским стартапом NetSafe, общается с мошенниками, отвечая им на нигерийские письма[9]. По словам разработчиков, чат-бот

[7] https://blogs.wsj.com/digits/2015/03/03/fraud-comes-to-apple-pay/
[8] https://xakep.ru/2015/03/04/apple-pay-fraud/
[9] https://www.netsafe.org.nz/rescam/

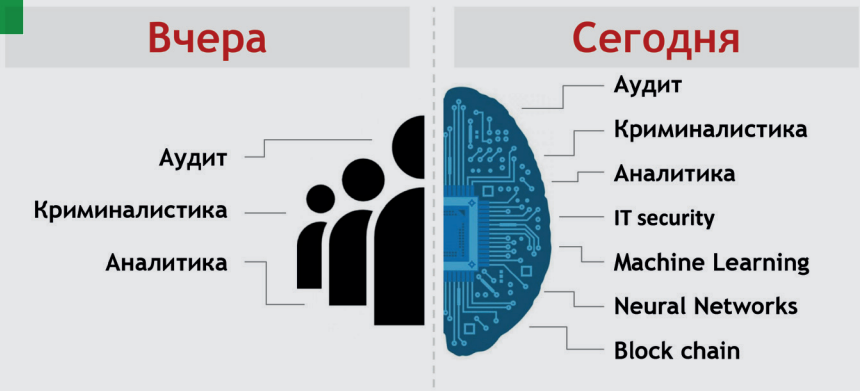

Рис. 2. Антифрод в банке.

RE:SCAM умеет распознавать тип фишинговых писем, подстраиваться под них и задавать мошенникам бесконечную серию вопросов. Чат-бот проявляет заинтересованность к собеседнику, пытается выяснить подробности, шутить и казаться «наивным». По мнению NetSafe, такое общение должно занять время мошенников и снизить их эффективность.

Григорий Бакунов из Яндекса в своем Telegram-канале пишет:

"Следующие 10 лет мы будем не только учиться создавать искусственный интеллект, но и обманывать его, делать антиобманные системы и так далее. Война предстоит не хуже, чем вирусно-антивирусная, готовьтесь."

И вполне реально, что скоро мы увидим как чат-бот "отвлекайка" общается с чат-ботом "попрошайкой", проявляет заинтересованность к "собеседнику", пытаясь шутить и казаться "наивным".

ТРАНСФОРМАЦИЯ ИЛИ СМЕНА ПАРАДИГМЫ?

Если резюмировать – каким мы видим банковский антифрод сегодня и каким он должен быть завтра, то очевидно, что аудита и криминалистики нам уже недостаточно. Нам надо снижать уровень мошенничества, бороться с новыми угрозами, не забывать о старых и при этом тратить на это меньше денег. Поэтому сегодня в антифроде нужны специалисты с новым набором знаний, которые помимо аудита и криминалистики хорошо разбираются в финансовом анализе, в кибер-безопасности, умеют моделировать, разбираются в нейронных сетях, в блокчейн-технологиях и т.д. И если отвечать на вопрос "что же это будет – трансформация или смена парадигмы?", можно ответить так: если вчера одни специалисты могли себе позволить видеть одно, а другие – другое, то сегодня нам придется научиться видеть одновременно и то и другое. tRF