Георгий Дорофеев (НСПК): Мы развиваем собственные антифрод-сервисы

О том, почему антифрод-системам Национальной системы платежных карт (НСПК) уделяется повышенное внимание и как их развитие помогает банкам в борьбе с мошенничеством, рассказал Георгий Дорофеев, заместитель директора операционно-технологического департамента НСПК



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

— Георгий, как реагирует на изменения рынка антифрода НСПК?
— Рынок антифрода претерпел массу изменений. Это обусловлено в первую очередь ростом количества цифровых угроз, который, в свою очередь, стимулируются бурным развитием технологий. Кроме того, борьба с мошенничеством попала в фокус внимания государства, что наложило определенный отпечаток на эту сферу.

Львиную долю всех кейсов в сфере фрода составляет социальная инженерия. По нашим данным, в платежной системе «Мир» и в Системе быстрых платежей (СБП) ее доля может доходить до 90%. При этом мошенники активно адаптируются к новым технологиям.

Поэтому задача, которая стоит перед НСПК, а также перед платежным сообществом в целом, — не менее быстро, чем мошенники, адаптировать процессы и системы фрод-мониторинга к отражению текущих атак, а также предвосхищать появление новых схем. Что касается совершенствования государственного регулирования, то соответствующими органами был принят ряд законодательных инициатив. В частности, в этом году правительство одобрило создание государственной информационной системы по борьбе с мошенничеством (ГИС «Антифрод». — *Ред.*).

НСПК также не стоит на месте, мы развиваем собственные антифрод-сервисы, чтобы борьба с мошенничеством на стороне банков стала более эффективной. Речь идет о таких сервисах, как «Найди ID», который позволяет бороться с токенизированным фродом. Это и платформа для возврата похищенных денежных средств «Добрая воля», благодаря которой участники рынка могут договариваться друг с другом и осуществлять возврат похищенных денежных средств пострадавшей стороне. Кроме того, появился опциональный сервис на установку периода охлаждения при внесении наличных в приложении Mir Pay.

У НСПК есть собственная система фрод-мониторинга, которая используется для «подсвечивания» участникам платежной системы фактов потенциальной мошеннической активности. Как в платежной системе «Мир», так и в Системе быстрых платежей в режиме реального времени в рамках транзакций мы передаем банкам риск-индикаторы, в которых содержатся «подсвеченные» данные. Банки на своей стороне на основании наших риск-индикаторов и собственных риск-политик принимают решение о том, является ли данная транзакция фродом или нет.



Фото: НСПК

— В рамках своей деятельности НСПК контролирует уровень фрода в ПС «Мир» и СБП. Для этого информацию обо всех неправомерных операциях банки должны заносить в Систему информирования о мошенничестве (СиОМ) НСПК. Как и для чего проводится работа по связыванию СиОМ с иными платформами?

— НСПК не только развивает свои собственные сервисы, но и следит за уровнем мошенничества на стороне банков. Это нужно, чтобы они не превышали контрольные показатели уровня фрода. Для этого используется СиОМ, куда участники платежной системы «Мир» обязаны заносить информацию обо всех мошеннических кейсах, с которыми сталкиваются они сами и их клиенты. Кроме того, с февраля 2025 года банки обязаны использовать СиОМ при работе с СБП.

В дополнение к сказанному в СиОМ участники также могут оценивать отсутствующую информацию и причины, по которым это произошло. Это в итоге приводит к улучшению антифрод-мероприятий на их стороне.

У НСПК организован обмен данными с ФинЦЕРТ Банка России, также мы получаем большое количество запросов от правоохранительных органов, например от МВД России. Благодаря этому мы можем контролировать качество репортинга. Нам крайне важно обладать наиболее полной картиной по фроду, который на текущий момент выявлен на рынке. Это позволяет максимально эффективно развивать наши антифрод-сервисы, а также настраивать антифрод-правила в системе мониторинга. Кроме того, мы предоставляем эту информацию банкам, чтобы они также могли эффективно противодействовать мошенничеству.

— В ходе форума «Антифродум-2025» (ежегодный форум по антифроду, организованный НСПК) были названы некоторые технологии обмена конфиденциальной информацией. Каковы их преимущества?

— Для качественного выявления фрода необходимо иметь много релевантных данных, часть которых имеется у банков, а часть — у нас. Неудивительно, что вопрос безопасного обмена чувствительными данными в режиме реального времени давно стоит на повестке. Мы участвуем в некоторых пилотных проектах, о результатах которых обязательно сообщим позже. Что касается используемых в пилотных проектах технологий, то большинство из них так или иначе связаны криптопротоколами конфиденциального обмена, которые позволяют соблюсти все положения нормативных актов о защите ПДн, банковской тайны и т.д. В одной из таких технологий используются неоспоримые преимущества фильтров Блума.

— Как НСПК информирует банки о новых сервисах?

— Новые сервисы практически всегда рождаются в рамках экспертных сообществ, в ходе наших диалогов с банками и регуляторами, которые регулярно проходят на площадке НСПК. Мы находится в тесном контакте со всеми участниками рынка, в том числе через техническую документацию Поэтому полной неожиданностью появление тех или иных сервисов назвать ни в коем случае нельзя.

В прошлом году при поддержке НСПК был организован антифрод-клуб, в рамках которого мы собрали ключевых специалистов на отечественном платежном пространстве.

Совместно с ними мы расследуем новые мошеннические схемы, вырабатываем решения, обсуждаем новые стандарты, касающиеся, например, платежной системы «МИР». Какие-то нововведения в итоге выносятся в сферу регулирования, в том числе законодательного. Живой диалог экспертов можно было услышать и в рамках двух прошедших форумов «Антифродум».

— 15 февраля 2025 года подписан Федеральный закон № 9-ФЗ. Что нового он может привнести в мир антифрода?

— Это один из законов, который призван повысить эффективность борьбы с фродом. В частности, он установил обязанность банков ограничивать внесение денег на счет через банкомат с помощью вновь токенизированной карты. В законе указано, что в течение 48 часов зачислять на подобную карту можно будет только до 50 тыс. рублей. Еще до вступления в силу № 9-ФЗ НСПК запустила опциональный сервис, к которому банки могут подключиться по желанию. Он позволяет им «замораживать» платежи на токенизированные карты. То есть все операции по пополнению карт, с момента токенизации которых прошло менее двух дней, будут останавливаться. Причем это будет происходить не только с подозрительными транзакциями, а со всеми. Такой сервис позволяет банкам соблюдать требования этого закона.

— Как НСПК планирует противостоять новым угрозам, в частности NFCGate? В чем заключается этот вид мошенничества?

— НСПК постоянно находится в тесном партнерстве с банками, вендорами и другими участниками рынка, совместно вырабатывая стратегию противодействия новым мошенническим схемам, в том числе и NFCGate. Суть этой угрозы состоит в следующем: жертву убеждают поставить на свой телефон вредоносное программное обеспечение, после чего ей предлагают под воздействием социальной инженерии приложить к телефону злоумышленника свою карту. Затем данные этой карты через инфраструктуру мошенников передаются на смартфон соучастника, которой, заведомо выявив PIN-код жертвы, снимает ее денежные средства со счетов. В результате деньги пользователей утекают на счета дропов, а NFCGate стал мощным инструментом в руках киберпреступников. Для борьбы с такими видами мошенничества также важным элементом является повышение уровня финансовой грамотности населения.


Фото: НСПК

— Какие задачи по направлению борьбы с фродом вы можете доверить ИИ? Какие сферы использования ИИ вы видите?

— НСПК активно исследует и внедряет технологии ИИ. В частности, машинное обучение (ML) мы применяем в своих системах, например в сервисе принятия решений для оценки рисков аутентификаций в MirAccept. После этого мы направляем рассчитанный скоринг всем участникам платежной системы «МИР». Внедрение машинного обучения позволило существенно повысить точность этой оценки. ML также активно используется в рамках системы фрод-мониторинга, над развитием которой мы сейчас активно работаем.

И ML, и нейронные сети будут обязательно развиваться, а мы, со своей стороны, будем способствовать этому. Такое развитие необходимо в рамках борьбы с новыми мошенническими схемами, где применяется ИИ: начиная от написания скриптов для обмана жертв и заканчивая слепками голосов и дипфейками. Поэтому там, где можем, мы будем внедрять новые технологии в системах НСПК. Б.О