# Перед антифродом все равны

**Экономика данных создала новые возможности для бизнеса, но также открыла двери для злоумышленников. А вот они, зная о средствах защиты, вернулись к «старым добрым» схемам, но на новом техническом уровне**



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




Потерпевшая шла одна вечером с урока по рисованию, пока ее просьбами о помощи не заманили в автомобиль. Двери моментально были заблокированы, и началась психологическая обработка жертвы. Девушку заставили войти в мобильное приложение банка, что она успешно сделала, пройдя все этапы идентификации. Через пару минут ей уже был одобрен кредит наличными на 100 тыс. рублей.

Психологическая обработка пострадавшей была настолько действенной, что мошенник отпустил ее одну к банкомату в магазине, где она сняла деньги и вернулась с ними в машину, никак не привлекая к себе внимания кассиров. Далее преступник решил обобрать девушку «по полной» и попытался увеличить кредитный лимит ее карты. Но тут сработала система антифрода банка. Об этом 21 февраля 2025 года вышел сюжет в телепередаче «Человек и закон».

### О пользе «спецкнопки»

Приведенный кейс весьма показателен с точки зрения объединения преступниками как офлайн-, так и онлайн-схем принуждения жертв к практически добровольному и безропотному подчинению кукловоду. Зомбированные люди, держа в руках смартфон, боятся хоть чем-нибудь вызвать неудовольствие и агрессию мошенников.

Именно для таких случаев **Эльвира Набиуллина,** председатель Банка России, в ходе Уральского форума «Кибербезопасность в финансах 2025» в Екатеринбурге предложила внедрить «спецкнопку» в приложениях банков. Но не только для этого она может пригодиться. По словам Эльвиры Набиуллиной, «часто не хватает слаженности действий разных регуляторов с операторами связи и правоохранительными органами, что на руку мошенникам».

Речь идет не столько о том, чтобы обслуживающий банк мог предпринять в подобных случаях какие-либо меры, а о комплексном взаимодействии экстренных служб и МВД. Ведь вполне вероятны сценарии, когда требуется одновременно оказать медицинскую помощь пострадавшим, принять меры по задержанию преступников, собрать улики на месте происшествия и т.д. Да и профилактическое воздействие на криминальный мер подобной «кнопки» нельзя недооценивать.

Но почему только сейчас этот вопрос был поднят на трибуну авторитетного форума? Ответ был дан представителями федеральных силовых органов в ходе пленарной сессии: «Когда начиналась эпопея борьбы с кибермошенничеством, все заинтересованные организации, включая Банк России, чувствовали себя в полном одиночестве на этом поле боя». И только теперь многие поняли, кто их реальные союзники, а кто — мнимые. Законодатели также активизировались с принятием соответствующих законов. Мошенники, получив реальные сроки, напомнили своим «коллегам», что онлайн-мошенничество и дропперство теперь вовсе не являются безопасным видом криминального заработка.

**«Наш ответ Чемберлену»**

Это с одной стороны. А с другой: почему все же сработала система антифрода в приведенном кейсе, ведь внешне все выглядело вполне благопристойно. Эксперты объяснили: девушка на тот момент времени была безработной и не имела стабильных доходов. Банк в ответ на повторную попытку увеличить лимит по кредитной карте с учетом того, что обе они были осуществлены практически одна за другой, счел, что по совокупности факторов налицо все признаки действия по принуждению.

Трудно сказать, была ли заблокирована система ДБО или нет, ведь мошенник вполне мог найти что-то интересное для себя не только в разделе кредитных продуктов. Мог он зайти с чужого смартфона и на портал «Госуслуги», на маркетплейс и т.д. И никакая биометрическая идентификация при этом не помогла бы, поскольку это были лицо и голос хозяйки смартфона.

По большому счету, все это и стало предметом обсуждения экспертов как на самом Форуме, так и в специализированных ИБ-чатах. Например, наиболее опасно сейчас выглядит тренд использования детей в мошеннических схемах, когда они, пытаясь откупиться, например, от онлайн-буллинга, опустошают кошельки родителей. А потом в надежде на возвращение похищенных денег идут на поступки, которые «тянут» на статью УК о терроризме. Это касается и других незащищенных категорий населения, но с молодежью проблем гораздо больше, и они усугубляются их массовым увлечением соучастием в дропперстве, что добавляет им еще и статьи по отмыванию денег (AML) и мошенничеству.

Ответом государства и частного бизнеса на вал мошенничества с использованием преступностью как методов социальной инженерии, так и физического воздействия на жертву, стала консолидация всех заинтересованных сторон. Правительство страны готовит масштабные изменения в законах для борьбы с кибермошенниками. В ближайшее время комиссия по законопроектной деятельности рассмотрит пакет поправок, затрагивающий десятки нормативных актов. В частности, будет введена обязательная идентификация через ЕСИА для пользователей маркетплейсов и агрегаторов с аудиторией более 200 тыс. человек при размещении объявлений о продаже товаров и услуг. Станет нормой маркировка звонков от организаций, международных номеров и виртуальных АТС — телефон будет отображать, кто звонит: реальный сотрудник банка или мошенник.

Биометрическая идентификация устанавливается обязательной для получения выписок из бюро кредитных историй и оформления микрозаймов онлайн. А у абонентов появится поистине «революционное право» отказываться от спама — сотовые операторы должны дать возможность блокировать рекламные рассылки и нежелательные звонки. Кроме того, принято решение исключить лицензию на IP-телефонию из перечня лицензий на оказание услуг связи. Похоже, операторов наконец-то обязали реально исполнять предписанные Законом о связи нормы.

А главное: для госструктур, банков и операторов связи разработали концепцию государственной системы противодействия IT-преступлениям, предполагающей построение единой платформы, которая станет мостом для оперативного обмена информацией между ключевыми организациями. Такая координация должна, например, позволить мгновенно блокировать мошеннические транзакции и предотвращать другие киберугрозы.

**Объединяй и защищай!**

Но все-таки, о чем еще дискутируют антифрод-эксперты после всего сказанного в Екатеринбурге, на Форуме «Антифрод» в Москве и т.д.?

В чате «ИБ в финсекторе» активно комментируется пост: «Вам не приходило в голову, почему в новостях появляются сообщения, как какого-то топа развели на десятки или сотни миллионов и он свободно переводит эти деньги, а простым смертным 500 рублей блокируют?».

**Алексей Лукацкий,** ИБ-эксперт, поделится более конкретными вещами: «На хакерском форуме появилось объявление о продаже доступа к взломанному DNS-контроллеру, обслуживающему, по заверению взломщиков, 62 высоконагруженных домена с ежемесячной аудиторией более 24 млн пользователей».

Эти и множество других мнений сводятся к нескольким проблемам, которые должны решаться в ближайшем будущем.

Во-первых, закон должен стать равным для всех. Если сумели «дожать» телекомы, то пришло время и должностных лиц. Тогда, возможно, будет меньше и хакерских чатов, и утечек персональных данных. Преступность должна лишиться возможности коммуникаций.

Во-вторых, продолжится объединение баз данных различных ведомств. На примере срабатывания антифрода в рассмотренном кейсе было бы полезно всем понять: «А откуда у банка была информация о том, что девушка является безработной?». Этот тот самый случай, когда правоохранители должны знать все, что им необходимо по службе.

А главное — у людей должен появиться механизм дачи согласия на прослушивание их коммуникаций специализированными автоматическими сервисами наподобие антиспама для блокировки Deepfake. Кроме всего прочего, это даст новый импульс развитию киберкриминалистики (форензика). Б.О