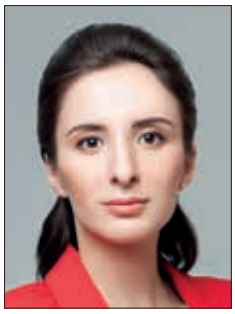

Дарья ВЕРЕСТНИКОВА
коммерческий директор
компании SafeTech

ПОДПИСЬ В СМАРТФОНЕ — ДЛЯ БЕЗОПАСНОСТИ И ДЛЯ БИЗНЕСА

КАК ЦИФРОВЫЕ КАНАЛЫ МОГУТ БЫТЬ БЕЗОПАСНЫМИ, УДОБНЫМИ И ДОСТУПНЫМИ

В последние годы экспертное сообщество непрерывно говорит о бурном развитии цифровых каналов банковского обслуживания, а также о связанных с ними проблемах: увеличением активности мошенников, использующих социальную инженерию, уязвимости кодов подтверждения операций, передаваемых в SMS и PUSH, непреодолимых ограничениях на реализацию сервисов для мобильных пользователей. О том, как решить актуальные проблемы безопасности Интернет- и мобильного банкинга, а также создать необходимые условия для самых инновационных и востребованных сервисов мы побеседовали с Дарьей Верестниковой, коммерческим директором компании SafeTech.

— Дарья, расскажите, пожалуйста, какие вопросы, связанные с информационной безопасностью, являются сейчас наиболее актуальными в области цифровых каналов обслуживания?

— На наш взгляд, самым актуальным вопросом на сегодняшний день является проблема социальной инженерии. В частности, по информации ФинЦЕРТ Банка России, в 2018 году с использованием приёмов социальной инженерии было совершено более 97% хищений со счетов физических лиц. А в прошедшем 2019 году ситуация усугубилась ещё больше — мошенники стали активно использовать возможность подмены исходящего телефонного номера на «реальные» номера колл-центров банков. Вы же помните, как прошедшей осенью новостные ленты пестрили сообщениями об успешных попытках злоумышленников получить данные пользователей, представившись «сотрудниками банков»? Мы в компании SafeTech уверены, эта проблема останется актуальной и в наступившем году.

Вторым важным вопросом и направлением активной деятельности экспертного сообщества в финансовых институтах является обеспечение соответствия требованиям Положения Банка России № 683-П от 17.04.2019 г. Очевидно, что в условиях увеличения числа преступлений в финансовой сфере регулятор продолжает задавать основные направления борьбы с ними. По информации МВД России в течение девяти месяцев 2019 года был зафиксирован 70%-ый рост количества преступлений в сфере IT, в том числе с использованием банковских карт и мобильных устройств. И выполнение требований Банка России, какими бы сложными в реализации они ни казались, является в полном смысле слова, велением времени.

Третьим актуальным вопросом, связанным с информационной безопасностью, является уязвимость распространённых, но уже устаревших методов аутентификации пользователей ДБО и подтверждения проводимых ими операций по одноразовому SMS-коду. Показательным является международный опыт: за последние 6 месяцев 2019 года 6 крупнейших банков Германии посчитали такой способ подтверждения платежей небезопасным и приняли решение отказаться от него. Аналогичные сообщения поступали из ряда других стран Евросоюза и из Турции. Как известно, проблема заключается в недостатках протокола ОКС-7 (SS7). Уязвимости в этом протоколе позво-

ляют злоумышленникам «незаметно похитить» номер телефона пользователя, даже без ведома Оператора связи, а также «отслеживать» все коммуникации его владельца, и в конечном счёте — похитить денежные средства у ничего не подозревающего легального клиента банка.

— Дарья, давайте обсудим эти вопросы подробнее. Расскажите подробнее о проблеме социальной инженерии, и как с ними бороться?

— Это очень серьёзная проблема, которая настигла, прежде всего, простых граждан. Конечно же, банки активно предупреждают пользователей об опасности, но истории про то, как мошенник «выудил» у клиента код подтверждения и похитил деньги мы слышим всё чаще и чаще.

Существует несколько наиболее массовых сценариев хищений, в которых клиента просят сообщить присланный код подтверждения. Самым распространённым в 2019 году способом стал звонок «представителя службы безопасности банка» с просьбой для отмены «свершающейся прямо сейчас попытки мошенничества» срочно сообщить код из SMS или PUSH. Второй популярный способ — звонок из «кредитного отдела банка» для погашения задолженности. В условиях стрессовой ситуации продиктовать мошеннику код может даже очень осторожный клиент.

«Технологическая» сторона проблемы социальной инженерии заключается в том, что в одном SMS или Push-сообщении невозможно представить все реквизиты платежа, чтобы человек сам видел, какая операция совершается в действительности. Если же дать клиенту возможность подтверждать своё волеизъявление только после просмотра реальных реквизитов и вообще без необходимости вводить какой бы то ни было код, это кратно сократит число успешных для мошенников попыток кражи! В частности, одно из возможных решений проблемы — мобильная аутентификация и подпись в смартфоне — реализовано таким образом, что никаких кодов подтверждения нет, но есть полное отображение реквизитов операции и гарантия того, что на конкретном телефоне клиента будет исполнена именно эта операция.

— Некоторые эксперты говорят, что помимо проблемы социальной инженерии коды в SMS или Push-сообщениях обладают и собственными недостатками, прежде всего, в отношении выполнения требований Положения Банка России № 683-П от 17.04.2019 г. Вы согласны?

— Мы считаем, что сама концепция передачи уже известного банку кода на смартфон клиента через недоверенные каналы связи является порочной и не должна использоваться для подтверждения финансово значимых операций. Кроме того, такие коды только «на бумаге» можно привязать к выполнению требований 683-П о гарантии целостности и авторства подписываемого документа. И именно поэтому судебная практика в России всё чаще сводится к признанию SMS «неперсонифицированным» средством подтверждения и, как результат, банки вынуждены возвращать клиентам похищенные средства.

Но есть ещё и экономический аспект данного вопроса. Несколько лет назад удорожание SMS привело к тому, что банки начали использовать PUSH-коды. На первый взгляд, это казалось оптимальным, и многие перешли на эту технологию. Но эксперты в области безопасности справедливо называют такой вариант «профанацией электронной подписи». Судите сами: на сервере прикладной системы «сгенерировался» какой-то одноразовый пароль (OTP), он как-то был передан клиенту на смартфон, иногда даже сам за клиента «подставился» в интерфейс и сам «подписал» транзакцию. Это же страшный сон любого специалиста ИБ!

— Итак, для решения перечисленных проблем Вы предлагаете подпись в смартфоне. Чем она отличается от обычной, и в чём преимущество её использования для клиентов?

— Несколько лет назад мы представили рынку решение PayControl для подписи в смартфоне, призванное кардинально улучшить ситуацию с безопасностью цифровых каналов по отношению к классическим SMS- и PUSH-кодам, и позволяющее «превратить» мобильное устройство в аналог USB-токена с таким же высоким уровнем безопасности и очень простым пользовательским сценарием. Сейчас PayControl — это полноценная платформа мобильной аутентификации и электронной подписи. При её использовании обеспечивается эффективное противостояние наиболее распространённым атакам на клиентов («перевыпуск» SIM-карты, фишинг, подмена документа, социальная инженерия и т.д.). Главный принцип — клиент видит реквизиты платежа на своём смартфоне и подтверждает их одним нажатием кнопки.

Стоит отметить, что в основе PayControl лежит асимметричная криптография, а это значит, что банк не может от имени клиента подписывать какие-либо операции. Закрытый ключ «рождается», «живёт» и «умирает» в конкретном смартфоне — попытки его воспроизведения на другом устройстве ни к чему не приведут. Подпись формируется как функция от 4-х аргументов: реквизиты конкретной операции, закрытый ключ клиента, момент времени и «отпечаток» смартфона пользователя. С точки зрения удобства использования очень важно, что SDK PayControl может быть полностью встроено в мобильное приложение банка.

— А как быть с классическими пользователями Интернет-банка?

— Конечно, концепция Mobile First — это тренд, но мы никогда не забываем о других каналах. Для PayControl абсо-

«Технологическая» сторона проблемы социальной инженерии заключается в том, что в одном SMS или Push-сообщении невозможно представить все реквизиты платежа, чтобы человек сам видел, какая операция совершается в действительности

лютно не имеет значения, в каком канале был создан документ, который пользователь подпишет в своём смартфоне. Это может быть не только мобильный банк, но и Интернет-банк, рабочее место операциониста и даже банкомат. Важно то, что информация о совершенной операции приходит прямо в смартфон клиента, где он проверяет детали операции и подписывает её электронной подписью.

Более того, мобильная подпись для пользователей Интернет-банка предоставляет ещё и весьма интересные дополнительные возможности. К примеру — вход без логина и пароля, при помощи смартфона в личный кабинет. Совсем недавно с одним из банков из «топ 5» мы запустили самый масштабный проект для физических лиц, где реализовали не только подпись операций, но и такой вход в Интернет-банк. Работает это так: на экране компьютера вместо окна с логином и паролем отображается QR-код. Вы открываете мобильное приложение банка, считываете QR-код, и автоматически «проваливаетесь» в личный кабинет! Важно отметить, что в этом сценарии исключается перехват логина и пароля клиента, даже если он работает в недоверенной сети.

Аналогично клиент сможет работать при помощи своего телефона и с банкоматами. И для этого не требуется внедрять NFC-модули — нужно лишь обновить ПО. На экране, по аналогии с Интернет-банком, появится QR-код, который клиент сканирует своим смартфоном и получает доступ к своему карточному счёту. Все действия в банкомате, будь то перевод или снятие наличных, клиент подтвердит при помощи смартфона. Банк может даже выдать клиенту виртуальную карту, с которой клиент сможет снимать денежные средства и распоряжаться ими, не имея вообще пластикового аналога на руках. И всё это благодаря полноценной электронной подписи, которая формируется в мобильном устройстве клиента и может однозначно указать на конкретного пользователя и совершённое им действие и подписать любой тип волеизъявления.

— Можно ли с помощью мобильной подписи решить ещё и проблему организации безбумажного офиса и подписи договоров клиентами без бумаг?

— Конечно! Клиенты прямо со своего смартфона смогут подписывать любые договоры, которые раньше приходилось подписывать в офисе банка: от открытия новых счетов и карт, до оформления депозитов и кредитов. Сейчас банки тратят огромные средства на печать, подписание, хранение и логистику документов. А безбумажный документооборот, помимо того, что упрощает действия пользователя, ещё и значительно сокращает затраты Банка на коммуникации с клиентами.

— Говоря о подписи договора, мы вплотную подошли к вопросу о формировании на мобильном устройстве квалифицированной электронной подписи. Это возможно?

— Нам удалось предложить рынку два решения для формирования «мобильной» подписи: «облегчённую» версию, которая идеально подходит для обслуживания физических и юридических лиц, а также «полновесное» решение, востребованное в тех областях, где необходима квалифицированная электронная подпись (КЭП). Решение для формирования КЭП при помощи смартфона называется myDSS и представляет собой совместную разработку компаний «КриптоПро» и SafeTech на базе программно-аппаратного комплекса облачной электронной подписи «КриптоПро DSS» и платформы PayControl. В 2018 году на это решение был получен сертификат ФСБ России.

Выбирая из двух решений, очень важно понимать, что различным сегментам клиентов и наборам сервисов необходим разный уровень безопасности и юридической значимости. Например, при дистанционном обслуживании физлиц или небольшого бизнеса простой или усиленной неквалифицированной подписи может быть вполне достаточно, но для предприятий с государственным участием или тех, кто взаимодействует с госструктурами (сдача налоговой отчётности, регистрация юридических лиц и прочее), необходимо использовать сертифицированные средства электронной подписи и усиленную квалифицированную электронную подпись.

— Какие услуги банков уже были реализованы с использованием квалифицированной электронной подписи со смартфона?

— На рынке уже представлены такие сервисы: удалённая регистрация бизнеса из интерфейса банка, сдача налоговой отчётности, дистанционный банкинг, торги и Госзакупки прямо с мобильного устройства. Таких проектов с каждым днём появляется всё больше и больше. Если у нас совместно с регулятором отрасли, совместно с удостоверяющими центрами, с ведущими производителями криптографических решений в России получится предоставить банкам технологии, которые помогут жителям страны экономить время, деньги, силы, то таких проектов станет ещё больше, и мы сможем «оКЭПить» каждого жителя страны, чтобы он стал полноценным участником безопасного электронного взаимодействия.

— В каком направлении происходит дальнейшее развитие ваших технологий мобильной аутентификации и электронной подписи?

Мы активно развиваем решение, проводим интеграцию с различными системами обеспечения безопасности, в частности, с биометрическими системами аутентификации и антифрод-системами. Это необходимо, например, для предоставления банкам возможности «адаптивной аутентификации», а также возможности ещё большего повышения уровня безопасности и удобства клиентов. Интеграция с биометрическими системами позволит добавить дополнительные факторы аутентификации при совершении так называемых «высокорисковых» операций, а использование передовых антифрод-систем позволит «на лету», в момент совершения операции, оценивать риск её подписи и работы пользователя на конкретном мобильном устройстве.

Таким образом, PayControl — это действительно полноценная платформа мобильной электронной подписи и аутентификации, которая позволит банкам, как кубики, собирать те функциональные возможности, которые им необходимо получить. Это позволяет нам говорить о новом классе систем обеспечения безопасности транзакций, которые мы сейчас выводим на рынок, и которые будут «взрывать» его в ближайшие несколько лет.