

Удобство и безопасность обслуживания.

Как сложить их в единый пазл?

КОНТАКТЫ
+7 495 120 9909
info@safe-tech.ru

Мобильная подпись для ДБО и 3D-Secure, банкоматы без пластика и безбумажный офис банка – как сложить в единый пазл удобство и безопасность? Дарья Верестникова, коммерческий директор компании SafeTech, резидента Кластера информационных технологий Фонда «Сколково», беседует с журналом «ПЛАС» об актуальных проблемах обслуживания клиентов в цифровых каналах, о современных технологиях мобильной электронной подписи и преимуществах ее использования, а также об инновационных решениях и сервисах, которые внедряют передовые российские банки.

ПЛАС: С какими вызовами, на ваш взгляд, сталкивается в настоящее время отечественная финансовая отрасль?

Д. Верестникова: На сегодняшний день нашими заказчиками являются свыше 70 банков, 8 из которых входят в топ-10, и все в один голос говорят, что основная проблема 2019–2020 гг. – это безопасность в цифровых каналах! Согласно информации Банка России, количество попыток банковского мошенничества растет из года в год, как в сегменте юридических, так и в сегменте физических лиц. В одном из недавних отчетов ФинЦЕРТ Банка России был отмечен рост числа попыток хищений за год на 631%, что соответствует увеличению в 7,3 раза!

Особую актуальность приобрела проблема социальной инженерии в сегменте физических лиц. По статистике ФинЦЕРТ, только в 2018 году с использованием приемов социальной инженерии со счетов физических лиц совершено более 97% хищений. Но в 2019 году картина еще более ухудшилась – злоумышленники стали активнее использовать технологии подмены реального исходящего телефонного номера на банковские номера.

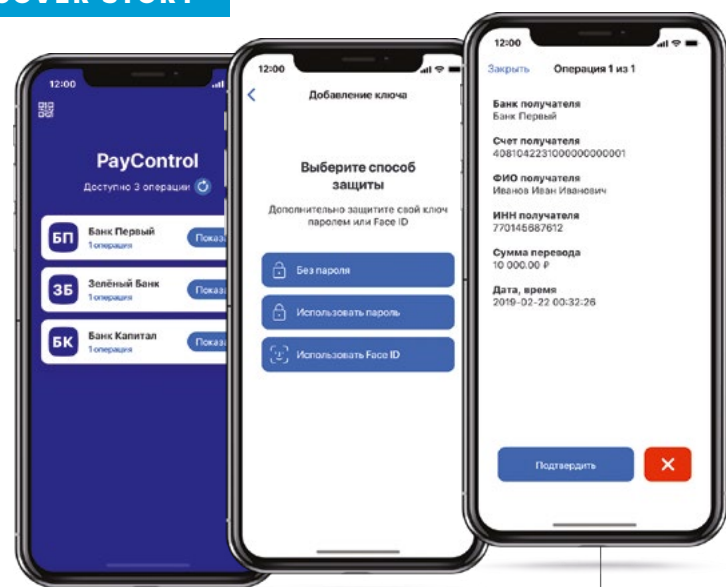
С началом «коронавирусного кризиса» ситуация усугубилась. Уже в июне заместитель председателя Совета безопасности РФ Дмитрий Медведев заявил о росте киберпреступности в условиях пандемии коронавируса – за пять месяцев 2020 года количество

киберпреступлений выросло на 85%! По информации наших коллег в российских банках, в середине года наблюдался настоящий «всплеск фрода», который потребовал беспрецедентного напряжения сил и расходования дополнительных средств.

ПЛАС: В чем, на ваш взгляд, основная причина столь масштабной активизации мошенничества?

Д. Верестникова: Чтобы ответить на этот вопрос, наверное, стоит вспомнить историю развития средств безопасности в банковском секторе и платежной индустрии. Изначально развитие дистанционных сервисов и, соответственно, средств подтверждения транзакций в ДБО юридических лиц немного опережало развитие сервисов и безопасности для частных клиентов. Помните, что когда-то доступ в банк с компьютера бухгалтера организовывался через VPN по ГОСТу, а для подписи можно было использовать только сертифицированный криптопровайдер? А как ключи электронной подписи хранились сначала на дискете или флешке, а потом и на USB-токене? Своеобразным «венцом» этого развития стало активное внедрение в ДБО антифрод-систем, а также использование устройств доверенного отображения данных – для защиты от самых «высокотехнологичных» атак на клиентов, включая «удаленное управление» и «подмену реквизитов платежа». В настоящее время активно развивающиеся технологии мобильной





При использовании PayControl клиент видит на экране своего смартфона реквизиты проводимой транзакции и подписывает ее полноценной электронной подписью

бы безопасности» банка или «представитель отдела по работе с клиентами», сообщает ему вежливым «поставленным» голосом часть информации, например, имя, фамилию и отчество, то зачастую клиент под воздействием приемов социальной инженерии поддается на обман и сам «отдает» мошенникам информацию, необходимую для проведения несанкционированных транзакций. И это мы не говорим о технической уязвимости SMS и Push, о том, что они могут быть достаточно успешно перехвачены еще до того, как клиент приступит к вводу переданных ему одноразовых паролей.

Получается, что в настоящее время SMS и Push уже неспособны защитить от наиболее распространенных атак: не только от подмены реквизитов платежа, перехвата SMS и злонамеренного ПО, но и от социальной инженерии. Да и сами сценарии использования одноразовых паролей, переданных в SMS и Push-сообщениях, уже не воспринимаются такими «удобными» – пользователи хотят подтверждать документы в цифровых каналах «в одно касание».

Исследования ряда российских экспертов¹ подтверждают, что юридически SMS можно использовать для подтверждения транзакций с очень большими оговорками, а вот Push-уведомления – и вовсе нельзя (это прямо написано в «гайдлайнах» для разработчиков мобильных платформ). Учитывая негативную судебную практику в отношении SMS, возросшую стоимость услуг операторов связи, и, самое главное, волну мошенничества с использованием методов социальной инженерии, от SMS и Push рано или поздно придется отказаться.

Весьма интересная практика сложилась в Европе. С вступлением в действие в сентябре 2019 года Второй платежной директивы Евросоюза (Revised Payment Service Directive, PSD2), финансовый сектор начал обновление решений для аутентификации и подтверждения транзакций. Так, еще в июне 2018 года Европейский платежный союз заключил, что SMS не являются подходящим методом доставки одноразовых кодов подтверждения и должны быть заменены на более безопасные методы.

Российский регулятор тоже начал работу над исправлением сложившейся ситуации с распространением SMS и Push, выпустив 17 апреля 2019 года Положение № 683-П, в котором предъявляет требования к средствам подтверждения – отныне они

подписи «превратили» в безопасные и удобные средства подписи смартфоны самих пользователей!

А что же изменилось в ДБО для физических лиц? В погоне за улучшением usability и упрощением user experience (UX), напрямую влияющих на число активных пользователей, банки зачастую предпочитали принимать риски кражи денег, чем внедрять безопасные технологии подтверждения. Так, многие сделали акцент на одноразовые пароли, передаваемые в SMS-сообщениях. Для своего времени, конечно же, это был простой и бюджетный путь, но когда цена на них выросла, то, к сожалению, банки начали передавать коды подтверждения в Push-уведомлениях. Иногда это сопровождалось даже их автоматической подстановкой или вообще пренебрежением самим процессом подтверждения транзакций.

Именно такой подход и не позволяет обеспечить ни эффективную защиту от мошенников, ни защиту позиции банка в случае судебного иска от пострадавшего или «якобы пострадавшего» пользователя. Безусловно, сейчас уже небезопасность SMS и Push всем стала очевидна, а хищения стали настолько частым явлением, что превысили все принятые банками уровни рисков, и банки наконец начали усиливать безопасность своих дистанционных каналов.

ПЛАС: Иными словами, «стандартные» средства подтверждения транзакции уже не защищают клиентов в полной мере? Считаете ли вы, что банки так или иначе будут вынуждены от них отказаться?

Д. Верестникова: Следует признать, что одним из основных «слабых звеньев» в цифровых каналах обслуживания при использовании одноразовых паролей в SMS и Push-уведомлениях является сам клиент и его неготовность в одиночку противостоять мошенникам. Когда пользователю звонит мнимый «сотрудник служ-

¹ Одним из известных исследований возможности отправки одноразовых кодов в системах мобильного и интернет-банка, а также для информирования о транзакциях в России стал анализ Центра судебных экспертиз компании RTM Group (опубликовано в открытых источниках: https://www.anti-malware.ru/analytics/Threats_Analysis/legalty-of-sending-sms-and-push-notifications-clients-banks).



Рис. 1. Структура платформы PayControl



должны обеспечивать целостность и авторство подписываемого документа. SMS и Push с трудом и большими оговорками могут выполнить данную задачу, что неизбежно приводит нас к необходимости менять средства защиты ДБО.

В настоящее время остается фундаментальная проблема – в погоне за удобством для пользователей все напрочь забыли о безопасности. Специалисты ИБ превратились во «врагов народа», которые «ходят и мешают работать». Ну что ж – теперь мы пожинаем плоды такого подхода.

ПЛАС: Какими в таком случае должны быть эти самые «более безопасные методы»?

Д. Верестникова: Ответ, с одной стороны, очень прост, с другой – весьма нетривиален в реализации. Прежде всего нужно исключить сам одноразовый код подтверждения операции, но при этом обеспечить целостность и авторство подписываемого документа. Если подтверждение транзакции или подпись электронного документа будет происходить при помощи ключа электронной подписи на смартфоне пользователя без какого бы то ни было одноразового кода или идентификатора сессии, то клиенту просто нечего будет сообщить мошенникам, к каким бы изощренным методам социальной инженерии они ни прибегали, и преступникам нечего будет перехватывать. И в настоящее время ведущие российские банки активно переходят от использования SMS и Push-уведомлений к мобильной электронной подписи.

Вообразите: полноценная мобильная электронная подпись на смартфоне пользователя, реализованная на асимметричных криптографических алгоритмах, обеспечивает контроль целостности и авторства, юридическую значимость подписанных документов и волеизъявления пользователя. Более того, она вообще избавляет от не-

обходимости высылать клиенту какую-либо информацию для подтверждения транзакций и документов. Клиент, с одной стороны, видит, что именно он подписывает, с другой – в принципе не сможет сообщить что-либо мошенникам, которым нечего и перехватывать, поскольку подпись происходит прямо в смартфоне клиента. Таким образом, человек перестает быть «слабым звеном» в цифровых каналах, и описанная проблема решается!

ПЛАС: Не могли бы вы подробно рассказать о решении для формирования мобильной электронной подписи, которое разработала компания SafeTech?

Д. Верестникова: Несколько лет назад мы представили рынку платформу PayControl для подписи «в смартфоне», призванную свести к нулю риски, возникающие при использовании SMS- и Push-уведомлений. Это решение «превращает» мобильное устройство в удобный и очень мобильный аналог привычного USB-токена, в котором формируется электронная подпись. Теперь высокий уровень безопасности операций, который раньше был доступен только в ДБО юридических лиц и только на рабочих компьютерах, стал доступен «всем и везде».

Сейчас PayControl – это полноценная платформа мобильной аутентификации и электронной подписи. При ее использовании клиенты защищены от наиболее распространенных атак: «перевыпуска» SIM-карты, фишинга, подмены документа и, самое главное в настоящее время, от рисков социальной инженерии.

Решение включает в себя несколько функциональных модулей: мобильной электронной подписи, информирования клиентов о транзакциях, разбора конфликтных ситуаций, идентификации и аутентификации клиентов, раннего выявления и предотвращения мошенничества, дополнительной биометрической аутентификации. PayControl постоянно совершенствуется, наполняясь



новыми функциональными возможностями. Объем внедрения определяется потребностями конкретного банка и его клиентов.

Эксперты в области ИБ в банках часто спрашивают нас: «На чем основывается безопасность мобильной электронной подписи в PayControl?» При использовании этого решения подпись формируется как функция от четырех аргументов: реквизиты конкретной операции, ключ подписи клиента, момент времени операции и «отпечаток» смартфона пользователя. В этот же момент проводится анализ смартфона на Root/Jailbreak и наличие подозрительных приложений, а также отправляются в систему фрод-мониторинга банка параметры рабочей сессии. Даже если пофантазировать и предположить, что злоумышленник как-то получит доступ к ключу, то он никак не сможет его использовать для другой операции, на другом устройстве, в другое время.

ПЛАС: В настоящее время на рынке идет много разговоров об обновленном протоколе 3D-Secure 2.0. Может ли PayControl использоваться для повышения безопасности онлайн-платежей?

Д. Верестникова: Использование мобильной подписи в операциях с 3D-Secure исключает необходимость

передачи клиенту SMS с кодом подтверждения. В момент оплаты клиент увидит на экране своего смартфона реквизиты проводимой транзакции и подпишет ее в мобильном приложении полноценной электронной подписью. Отличие от схемы с использованием SMS состоит только в том, что потребуются интеграция платформы PayControl с процессингом банка, в остальном все останется без изменений.

В чем преимущество использования электронной подписи в операциях с 3D-Secure для банков?

Во-первых, это повышение уровня безопасности операций: никаких возможных перехватов SMS, никаких рисков социальной инженерии – у пользователя больше не будет никаких кодов, которые можно у него выманить или незаметно похитить.

Во-вторых, это сокращение расходов банка на SMS – они просто больше не понадобятся, поскольку операции будут подписываться в мобильном приложении, в котором можно отражать и уведомления о транзакциях по карте.

В-третьих, установка приложения для подписи транзакций с 3D-Secure будет стимулировать клиентов к активному использованию мобильного банкинга. Во многих подразделениях розничного бизнеса это отдельный показатель KPI, который можно существенно увеличить, в том числе и за счет инноваций в подтверждении операции с 3D-Secure.

В-четвертых, использование приложения для мобильной электронной подписи позволит банку обогащать свою антифрод-систему и еще надежнее защитить своих клиентов во всех своих цифровых каналах.

И, наконец, в-пятых, сейчас все очень заинтересованы в адаптивной аутентификации в 3DS. Это на нашей платформе реализовано уже достаточно давно. И главное здесь, что независимо от того, как происходит аутентификация – с запросом или в автоматическом режиме, – транзакция подписывается электронной подписью, что является максимально безопасным и юридически значимым относительно всех иных реализаций.

ПЛАС: Одним из наиболее перспективных направлений развития цифровых каналов сегодня называют «бесбумажный офис банка». Как ваши технологии могут помочь в его построении?

Д. Верестникова: Действительно, большинство банков и сервисных компаний подписывают с клиентами множество бумажных документов на оказание услуг: для открытия расчетных счетов, выдачи кредитов, размещения депозитов, инвестиций и многого другого. Все это приводит к значительным затратам на печать, логистику и хранение бумажных документов, а также ограничивает взаимодействие с клиентами рамками офиса. Причем любая ошибка в распечатанных

документах, не в том месте проставленная подпись приводят к тому, что и документ становится абсолютно «невалиден»! Это большие затраты и риски для организации. Но как сократить расходы без ущерба для бизнеса и получить дополнительные преимущества?

Самым эффективным решением является согласование и подпись договоров в электронном виде. Но цифровое взаимодействие с клиентами должно быть для них не только более удобным и доступным, но и не менее безопасным и юридически значимым, чем традиционные способы. Поэтому банкам и сервисным компаниям важно предоставить клиентам возможность подтвердить свое волеизъявление на получение услуг, желательно полноценной электронной подписью, а также обеспечить контроль целостности и авторства подписываемых документов.

Совсем недавно компания SafeTech совместно со своим партнером, компанией Artsofte, представила рынку «бесбумажную» платформу, которая позволит финансовым структурам построить полноценный бесбумажный офис для взаимодействия со своими клиентами, а гражданам, индивидуальным предпринимателям, среднему и малому бизнесу – заключать друг с другом договоры в электронном виде и подписывать электронные документы.

ПЛАС: А возможно ли использование PayControl не только для цифровых каналов, но и для физической инфраструктуры обслуживания?

Д. Верестникова: Вы правы, характерной чертой современного банковского обслуживания является «омниканальность» – возможность предоставить клиентам необходимый сервис во всех доступных каналах: в офисе банка, в интернет- или мобильном банке, по телефону или в мессенджерах, в банкоматах или терминалах оплаты. При этом везде должен обеспечиваться высокий уровень безопасности, удобства работы и обеспечиваться юридическая значимость действия клиента.

Использование мобильной подписи в операциях с 3D-Secure исключает необходимость передачи клиенту SMS с кодом подтверждения

С помощью PayControl эти требования можно реализовать, например, и для банкоматов. Причем даже для тех банкоматов, которые не оснащены NFC-модулями, – нужно будет лишь обновить ПО. Все действия в банкомате, будь то перевод или снятие наличных, клиент подпишет при помощи смартфона. Банк может даже выдать клиенту виртуальную карту, с которой клиент сможет снимать денежные средства и распоряжаться ими, не имея вообще пластикового форм-фактора на руках!

ПЛАС: Несколько слов о надежности самих смартфонов с точки зрения безопасности рассматриваемых функций?

Д. Верестникова: Безусловно, поскольку в решении PayControl в качестве средства для формирования электронной подписи используется смартфон – устройство, безопасность которого зачастую вызывает у экспертов много вопросов, то этому моменту мы уделили самое пристальное внимание. Во-первых, для обеспечения безопасности ключей формирования электронной подписи использованы самые передовые криптографические технологии. Конечно же, мы исходим из аксиомы, что «абсолютной безопасности не бывает», но в настоящее время получить несанкционированный доступ к ключам подписи на мобильном устройстве в случае использования PayControl – задача очень нетривиальная, требующая больших затрат.

Во-вторых, в случае использования PayControl мобильное устройство находится под постоянным мониторингом. Решение может собирать и накапливать информацию о более чем 70 параметрах функционирования устройства и, что очень важно, выдавать интегральный показатель защищенности (так называемый скоринг устройства). Данная информация может «обогащать» банковские антифрод-системы и обеспечить адаптивную аутентификацию для различных транзакций и различного уровня скоринга устройства.

И наконец, в-третьих, компания SafeTech на постоянной основе передает актуальные версии PayControl на профессиональный аудит безопасности с применением метода «белого ящика». Безусловно, такие исследования способствуют обнаружению недостатков и развитию продукта, но за все время существования PayControl еще не было случаев обнаружения критичных уязвимостей и реализации успешных атак.

В новой версии PayControl стали доступны интерактивные уведомления для всех мобильных платформ и поддержка смарт-часов

