Мобильная связь и безопасность ДБО

Мобильные средства связи (телефоны, смартфоны, планшеты...) уже давно и прочно вошли в нашу жизнь, став одним из необходимых «помощников» современного горожанина. Банки также оценили удобства, предоставляемые наличием у клиента постоянно действующего персонального средства связи. Начав с sms-рассылок и звонков с маркетинговыми предложениями или напоминаниями о необходимости сделать платеж по кредиту, сегодня большинство банков используют sms-пароли в качестве средства аутентификации клиента и авторизации платежей в системах интернет-банкинга, а некоторые развернули на платформах смартфонов полноценные банковские приложения, позволяющие клиенту управлять средствами на своих счетах, делать переводы и платежи. Да и сами мобильные операторы постоянно расширяют спектр «околобанковских услуг», превращая текущий счет абонента в аналог банковского счета.

Так мобильный телефон, вместе с sim-картой, оформленной на имя клиента банка, превратились из современного средства доступа к услугам связи в средство доступа к управлению банковским счетом. Насколько безопасна такая конвергенция? Можно ли дополнительно защитить средства на банковском счете клиента при компрометации телефона или sim-карты? Какие административные меры необходимо применить для упорядочения обращения sim-карт? Ситуацию комментируют наши эксперты.

- Сегодня банки используют мобильные устройства клиентов в качестве одного из факторов (а иногда – и единственного фактора) аутентификации и авторизации операций при работе клиента в системе ДБО (и физлиц, и юрлиц). Насколько допустимо такое использование средств связи, изначально не предназначенных для хранения и передачи конфиденциальной информации? Что делать банку, который по правилам международных платежных систем должен использовать для авторизации интернет-платежей по выпущенным картам технологию 3DSecure, надежность которой существенно зависит от конфиденциальности sms-сообщений?

Алексей Бабенко: Использование мобильного устройства для аутентификации пользователей – вынужденная необходимость. Несомненно, более надежным способом является использование, например, отдельного устройства, предназначенного для аутентификации. Но готовы ли клиенты идти на дополнительные траты? В большинстве своем, к сожалению, нет. В этом случае в некотором роде «арбитрами» выступают сами банки – например, ограничивая суммы операций, которые можно проводить, используя менее надежные методы подтверждения. Многие банки для аутентификации и подтверждения операций юридических лиц позволяют использовать только физический токен, имеющий более высокую степень защищенности.

Еще одним примером, когда из-за сложности реализации для массового клиента технология не продолжает развиваться, является протокол Secure Electronic Transaction (SET). SET являлся надежным механизмом обеспечения безопасности, но именно сложность реализации заставила платежные системы выработать новый, менее надежный протокол - 3D-Secure.

3D-Secure обеспечивает независимую аутентификацию предъявителя карточных данных со стороны эмитента. Аутентификация проводится не по данным, содержащимся на карте, а по альтернативным каналам: смс-сообщениям, одноразовым паролям, данным криптокалькулятора. Наиболее популярный способ подтверждения – смс сообщения, конфиденциальность которых сомнительна. Однако учитывая, что информация в sms является вторым фактором при аутентификации, использование данной процедуры имеет смысл и безусловно повышает безопасность.

Павел Есаков: Действительно, если окинуть беглым взглядом имеющиеся в банках решения по аутентификации клиентов и транзакций, то наиболее частым механизмом, используемым для этой цели, является одноразовый пароль по sms (sms-OTP). Для розничных клиентов это может быть единственным средством аутентификации, в корпоративных решениях это, как правило, дополнительная мера защиты. Подтверждение операций по банковским картам в электронной коммерции тоже чаще всего реализуется с помощью одноразового пароля, отправляемого клиенту банком на его мобильный телефон. Очевидно, что столь широкое применение sms-OTP делает компрометацию данного метода аутентификации весьма насущным желанием для мошенников. Нашим банкам, похоже, невдомек, что они работают на грани фола: sms-OTP на сегодня очень часто является практически единственным механизмом

Текст:
Андрей Новиков

подтверждения операций, и в случае его компрометации, банку придется либо смириться с потерями, либо прекратить обслуживание клиентов в системах ДБО. Резервного механизма у банков, как правило, нет. Однако существует масса других механизмов аутентификации, которые могут обеспечить существенно более высокий уровень защищенности, чем механизм sms-OTP. По видимому, в соревновании «удобство пользователя» или «безопасность операций» сегодня верх одерживает удобство.

Николай Носов: Технология 3D-Secure – большой шаг в обеспечении безопасных платежей физических лиц, значительно усложнивший жизнь злоумышленникам. Вспомните ситуацию трехлетней давности, когда пользователь проводил оплату, используя только пароль в свою систему интернет-банкинга (как правило, очень простой) или просто указывая на сайте номер своей пластиковой карты и CVV2 / CVC2 код. Все было намного хуже, и для хищения денег было достаточно переписать данные или просто сфотографировать вашу пластиковую карту, например, когда вы ее отдавали официанту для того, чтобы расплатиться в ресторане. Тем не менее, число реальных хищений у нас в стране по статистике было не так уж велико.

Двухфакторная идентификация с использованием мобильного устройства клиента – простой, удобный и дешевый для клиента способ повышения безопасности, и от него не надо отказываться. Другое дело, что клиент должен понимать, что 3D-Secure не дает абсолютной защиты. И подходить к вопросу безопасности комплексно:

- Своевременно обновлять ОС, антивирусы на своих компьютерах и смартфонах,
- следить за «странностями» в поведении мобильного устройства,
- не переходить по ссылкам, приходящим из недостоверных источников, в том числе на известные сайты,
- своевременно уведомлять кредитную организацию о смене номера телефона мобильной связи, который клиент предоставил кредитной организации для получения услуги «мобильный банкинг», в том числе, на который происходит информирование об операциях по счету клиента,
- не скачивать на устройство мобильной связи приложения из непроверенных источников,
- не передавать устройство мобильной связи и платежную карту для использования третьим лицам, никому не сообщать ПИН-код платежной карты, код CVC, пароли от «Клиент-банка»,
- минимизировать риски, имея как минимум две платежных карты – одну для зарплаты, другую для текущих расчетов.




Павел Есаков, заместитель директора по продажам в финансовом секторе, компания CompuTel • **Алексей Бабенко,** ведущий менеджер по развитию бизнеса, компания «Информзащита». • **Николай Беляков,** начальник Службы информационной безопасности банка «Кредит-Москва» (ПАО) • **Николай Носов,** к.т.н., член АРСИБ (Ассоциации руководителей служб информационной безопасности)

Вопрос информационной безопасности – вопрос оценки рисков и стоимости работ по их снижению. Юридические лица, как правило, используют в ДБО более сложные способы защиты, например, ключи на токенах. Но и «цена вопроса» у них совсем другая.

Николай Беляков: На мой взгляд, вопрос не совсем точно сформулирован. Если вести речь о мобильных устройствах, как о традиционных сотовых телефонах, то их использование в качестве средства авторизации финансовой транзакции подразумевает только лишь то, что сотовый телефон – это независимый, дополнительный канал доставки сведений, достаточных для подтверждения транзакции. Защищённость канала, в данном случае, не так важна, важна его независимость и изолированность от устройства, на котором проводится сама транзакция. Тоже самое относится и к технологиям авторизации интернет-платежей, например, 3D-Secure. Эти технологии также подразумевают использование sms в качестве дополнительного канала подтверждения платежа. Клиент должен получить цифровой код, который сам по себе не несёт никакой конфиденциальной информации, и ввести в форму подтверждения платежа.

Однако мобильный телефон в традиционном виде сейчас встречается крайне редко, большинство людей использует смартфоны. И речь уже не может идти в плоскости «допустимо/недопустимо». Особенно, если мы говорим о

клиентах – физических лицах. Тут важную роль играют такие факторы, как стоимость ДБО и, что крайне важно, удобство пользования сервисом. Сервис, которым неудобно пользоваться, не будет востребован. Современные мобильные устройства – это не просто телефон, а, фактически, компьютер с достаточно большими возможностями. Это делает их привлекательными и удобными для авторизации и проведения финансовых транзакций. Уже сейчас наметилась тенденция к снижению количества финансовых транзакций, совершаемых физическими лицами с использованием персонального компьютера. Подавляющее большинство инцидентов в ДБО, связанных с мобильными устройствами – это результат осознанных, либо не осознанных действий самих пользователей. Заражённые смартфоны используются, например, и для рассылки sms-спама, что так же приводит к финансовым потерям владельца смартфона. Тем не менее, ни у кого не возникает мысли, что смартфоны не пригодны для передачи sms, т.к. они разработаны для звонков. Авторизация финансовых транзакций – это ещё одно функциональное применение для смартфона.

Решать же эту проблему необходимо в двух направлениях: ведя просветительскую работу, повышая уровень осведомлённости пользователей, и развивая технологическое сотрудничество между разработчиками систем ДБО и разработчиками анти-фрод систем. К сожалению, на практике наблюдается нежелание крупных разработчиков ДБО идти на активное технологическое сотрудничество с разработчиками анти-фрод систем. Они пытаются «изобрести свой велосипед», а в результате страдает конечный пользователь. Надеюсь, это изменится в скором времени.

- Недавно произошло несколько случаев, связанных с получением злоумышленниками несанкционированного доступа к sms-сообщениям, направляемым банковским клиентам (как с помощью внедрения «троянов» в смартфон, так и с помощью «перевыпуска» sim-карты клиента у сотового оператора). Означает ли это, что мошенники уже компрометировали этот канал доставки информации, и банкам пора перестать относиться 4.к «мобильникам» клиентов как к защищенным устройствам? Или, по крайней мере, предлагать клиентам средства, повышающие защищенность этого канала связи (если «да», то какие средства)?

Павел Есаков: Собственно, методы взлома системы sms-OTP уже неоднократно были реализованы на практике: начиная с вульгарного получения новой sim- карты у оператора связи по поддельным документам и заканчивая использованием специализированных мобильных троянов, похищающих sms с мобильного телефона клиента и отправляющего одноразовый пароль мошеннику. Заметим, что имеется и еще не использованная (на сегодняшний день) мошенниками возможность взлома sms-шлюзов операторов связи. И если с заменой sim-карт банки научились бороться, то все остальные возможности для компрометации этого метода аутентификации живут и существуют. Создается впечатление, что наши банки не подозревают о наличии каких-либо более надежных методов для подтверждения операций, которые, несомненно, имеются на рынке. Достаточно просто перечислить возможные средства аутентификации:

- Токены с PIN клавиатурой на основе симметричных криптоалгоритмов.
- Кардридеры (автономные и подключаемые) стандарта EMV CAP (получившие в России красивое, но, по сути, неправильное название «криптокалькуляторы»).
- Мобильные телефоны с Secure Element (элемент безопасности) – их не более 18% от общего числа мобильных телефонов, и доступ к функциональности этих элементов не всегда предоставляется изготовителем телефона.

На кардридеры следует обратить особое внимание – с июня 2015 года все банки обязаны осуществлять эмиссию платежных карт с чипом, а именно эти карты и являются необходимым компонентом технологии EMV CAP. К сожалению, в России весьма небольшое число банков, которые используют эту технологию: НОМОС банк (ныне Банк «Открытие»), Московский Индустриальный Банк, Россельхозбанк, ВТБ24, Возрождение, Банк Санкт-Петербург. И общее число используемых устройств не превышает 100 000. Хищения при использовании данного метода аутентификации никогда не регистрировались.

Николай Беляков: Думаю, что данные моменты не могут говорить о компрометации канала в целом. При выстраивании системы безопасности платежей, необходимо изначально относиться к мобильному устройству клиента, как к недоверенному, ведь ни сотовый оператор, ни банк, ни прочие организации не могут контролировать,

что с ним происходит, и что с ним делает его владелец.

Для того чтобы вредоносное ПО получило доступ к sms, пользователь сам должен совершить определённые действия. Главная проблема в том, что многие люди нажимают на кнопки в телефоне, совершенно не думая, они устанавливают программное обеспечение из недоверенных источников, предоставляют программному обеспечению полномочия, даже не прочитав, какие. В случае же с получением полномочий root в Android либо jailbreak в iOS речь идёт об осмысленном и целенаправленном снижении уровня безопасности устройства. Именно это приводит к компрометации конкретного устройства и к инциденту.

Случаи с «перевыпуском» SIM-карт – это внутреннее мошенничество со стороны отдельных работников сотового оператора. С тем же успехом можно говорить, что отдельные случаи внутреннего мошенничества в банках – это компрометация банковской системы.

Против подобных моментов бессильна любая система безопасности, которая не превращает работу с системой в пытку. Так что речи о компрометации канала, как такового, идти не может.

Как со всем этим бороться? Против ошибок и необдуманных действий пользователей – только повышение осведомлённости. Желательно, чтобы это была государственная программа, а не попытки банков обучить клиентов (последнее малоэффективно). Вплоть до внесения в школьную программу, в рамках предмета по информационным технологиям, обязательного раздела по информационной безопасности. Если родители ребёнка с детства не научат мыть руки, он и не будет этого делать во взрослой жизни. То же самое относится и к вопросам информационной безопасности. В одиночку банки тут, по факту, бессильны. Со случаями же внутреннего мошенничества должны бороться, и борются сами сотовые операторы. Самое большое, что тут может быть предпринято – усиление ответственности сотовых операторов перед надзорными органами. Простая экономика: если ответственность компании перед клиентом и государством не значительная, то никто и не будет тратить средства на выстраивание более тщательного внутреннего контроля.

Алексей Бабенко: Мобильные устройства никогда не считались доверенными средствами с точки зрения ИБ. Здесь важно понимать, что, доверяя какую-то часть сервиса третьей, независящей от вас стороне, необходимо оценивать риски. И речь не только о конфиденциальности передаваемых

Глеб Альтер, ведущий менеджер по развитию бизнеса компании «Информзащита»:

Противодействие мошенничеству, основанному на нелегальной замене sim-кары пользователя ДБО - это вопрос обоюдной и равной ответственности сторон, как телеком-операторов, так и банков. Операторы должны нести ответственность в ситуации, когда по вине нелегитимной передачи sim-карт мошенникам произошел претензионный случай. Так и банк, в случае использования sms как канала для подтверждения операций, должен перед каждой транзакцией проверять, была заменена sim-карта или нет.

Конечно, Закон №115-ФЗ должен распространяться и на операторов связи, так как лицевые счета операторов связи по своей функциональности сейчас ни чем не уступают счетам кредитных организаций. Это задача Росфинмониторинга. ЦБ со своей стороны может рекомендовать использовать системы анти-фрод или anti-money laundering (AML).

данных или аутентификации сторон. Если вход в ДБО связан с вводом информации из sms, нужно быть готовым к тому, что клиент не сможет использовать сервис банка из-за отказа сервиса рассылки sms-сообщений.

Николай Носов: Действительно, специалисты по ИБ никогда не относились к «мобильникам» клиентов как к защищенным устройствам, понимая существующие риски. Но это не значит, что их нельзя использовать. А средства, повышающие защищенность этого канала связи, - «токенизация» и биометрические технологии. Но здесь все опять упирается в экономику. Пойдут ли на дополнительные траты клиенты?

- Возможно ли предусмотреть меры, обязывающие клиента банка использовать дополнительные средства защиты информации (выносные средства шифрования, токены и т.д.) при использовании мобильного устройства для получения доступа к управлению своим банковским счетом? Возможно ли в современных условиях хотя бы переложить на клиента банка убытки от незаконного доступа к счету со стороны злоумышленников при отказе от использования дополнительных средств защиты информации – не «по договору», а в реальных условиях?

Алексей Бабенко: Данные меры будут работать только при общем регулировании и являются в какой-то мере навязанной услугой. Есть, на мой взгляд, более прогрессивный, риск-ориентированный подход: чем менее надежное средство аутентификации используется, тем более ограниченный функционал получает клиент. Если же вернуться к «навязыванию» сервисов безопасности, то логичными выглядят сервисы, не создающие для клиента дополнительных неудобств. Например, установка встроенного в мобильное приложение антивируса, контроль безопасности окружения ДБО, интеллектуальные системы антифрода.

Николай Беляков: Здесь работают два фактора. Первый – неудобный сервис не будет востребован, а «заставлять» клиентов носить с собой дополнительное устройство - это неудобство. С физическими лицами такой вариант работать не будет. С юридическими лицами проще, т.к. в договоре дистанционного банковского обслуживания обговорить такие моменты, в определённых границах, возможно. Второй фактор – в некоторой степени, излишняя защищённость физических лиц от последствий действий мошенников с электронными средствами платежей, принадлежащими клиенту-физическому лицу. Фактически, статья 9 закона 161-ФЗ «О Национальной платёжной системе» закрепила презумпцию вины банка перед клиентом – физическим лицом. Это даёт дополнительный повод клиентам безответственно относиться к собственным деньгам, хранящимся на кредитных картах, лицевых счетах у сотовых операторов, электронных кошельках и т.п. По моему мнению, должна быть законодательно закреплённая обоюдная ответственность клиента и поставщика финансовых услуг.

Николай Носов: В современных условиях – маловероятно. Общая тенденция обратная: убытки пытаются переложить на банк. Другое дело, что у банков, как правило, хорошая юридическая служба и так просто деньги они не отдают.

Павел Есаков: Надо сказать, что даже регулятор обратил внимание на рост мошенничества в каналах ДБО банков (20-30% в год), что опережает прирост количества пользователей систем ДБО. Банк России планирует потребовать в обязатель-

ном порядке наличия механизма подтверждения онлайн-операций в системах ДБО путем внесения изменений в документ ЦБ 382-П. Правда, если посмотреть список предлагаемых средств, то можно понять, что некоторые из них либо уже скомпрометированы (как sms), либо не могут обеспечить высокий уровень защиты: скретч-карты, получение одноразовых кодов в банке. Правда, среди предлагаемых средств упоминаются и криптокалькуляторы, которые в состоянии практически полностью исключить мошеннические операции. Несомненно, банки могут и должны использовать простой и доступный механизм для повышения безопасности транзакций и сохранения удобства использования каналами ДБО. Для этого банк должен выстроить систему лимитов: часть транзакций может подтверждаться и с помощью sms (например, при переводе небольших сумм в пользу стандартных поставщиков услуг, налоговых платежей), а при проведении операций на большие суммы, особенно в пользу ранее неизвестных контрагентов, требовать других, более надежных механизмов подтверждения.

- Не секрет, что лицевые счета у операторов мобильной связи, привязанные к sim-картам, часто используются в различных мошеннических схемах для вывода украденных денежных средств. Сделать это злоумышленникам нетрудно, ведь каждый может легко купить десяток активных sim-карт без предъявления каких-либо документов. Таким образом, «подпольный» оборот sim-карт часто становится той самой легализацией (отмыванием) денежных средств, которая должна подпадать под регулирование известного Закона №115-ФЗ «О противодействии легализации...» и подзаконных актов. Не пора ли навести порядок с выпуском и перевыпуском sim-карт абонентов, в том числе, путем распространения норм Закона №115-ФЗ на взаимоотношения операторов связи и абонентов? Возможно ли это, на ваш взгляд? Не пора ли банкирам требовать вмешательства в ситуацию уполномоченных регуляторов (ЦБ, Росфинмониторинг)?

Николай Носов: Считаю это возможным и разумным. Сотовые операторы сейчас активно пытаются выйти на традиционный банковский рынок переводов и платежей. Вот пусть и играют с банками на нем по одинаковым правилам. В противном случае они получают на этом рынке серьезное конкурентное преимущество.

KPI менеджеров сотовых операторов зависит от числа реализованных sim-карт, и никак не зависит от «качества» клиентов. Отсюда и покупка карт без предъявления документов, и даже получение дубликатов sim -карт других людей. Яркий пример – недавний скандал с кражами sim-карт Билайн.

Если же регуляторы начнут серьезно наказывать за такие проступки операторов связи, то и они изменят свои требования к менеджерам. Например, будут лишать премии в случае выдачи sim-карты без проверки документов, подтверждающих личность покупателя.

Павел Есаков: Да, такая проблема есть. Но метод решения представляется в корне неправильный. Следует взглянуть на юридическую сторону вопроса. Оператор связи - это не кредитное учреждение, это не банк! Нормы Закона №115-ФЗ не применимы к операторам связи. А вот использование абонентских счетов, как платежных, уподобление их банковским счетам - такую практику следует пресечь! Вот вопрос к регуляторам (ЦБ, Росфинмониторинг). И конечно, не следует банковским учреждениям создавать и поддерживать эту порочную практику.

Кстати, если взглянуть на юридическую сторону использования sms как средства подтверждения платежа, то сразу становятся видны коренные недостатки данного метода: у оператора связи есть (скромные) обязательства по отношению к клиенту, но нет никаких обязательств по отношению к банку. Нужно понимать, если sms используется как средство подтверждения платежа, делается это исключительно на страх и риск клиента. Более того, Закон о связи, например, в явном виде исключает участие банка, то есть постороннего <во взаимоотношениях оператора связи и абонента – ред.>, в случае расследования инцидента с мошенничеством.

Николай Беляков: Это достаточно сложный юридический вопрос, и решать его должны юристы. На мой взгляд, существующего законодательства достаточно, чтобы навести порядок. Например, sim-карты не должны выдаваться без предъявления документов, удостоверяющих личность. То, что это не так, - это уже вопрос качества внутреннего контроля внутри самих сотовых операторов и качества работы надзорных органов, которые обязаны контролировать соблюдение норм законодательства операторами связи.