SMS-коды небезопасны. Что дальше?

Д. КАЛЕМБЕРГ: «Теперь банки с минимальными затратами могут реализовать подтверждение платежных документов на мобильных устройствах квалифицированной подписью»

беседовала **Софья Мороз**

Высокая популярность мобильного банкинга способствует появлению дополнительных рисков в сфере безопасности клиентов и проводимых ими операций. Какие это риски и как можно им противодействовать, в интервью NBJ рассказал генеральный директор компании SafeTech Денис КАЛЕМБЕРГ.

NBJ: Денис, поясните, пожалуйста, о каких новых, ранее неведомых рисках идет речь?

Д. КАЛЕМБЕРГ: Риски в общем и целом остаются прежними – это возможность кражи денег со счетов клиентов. Она существовала и в Интернет-банкинге, но за счет объединения на смартфоне каналов создания и подтверждения документа эта операция для мошенников существенно упростилась.

NBJ: Сейчас много нареканий вызывает подтверждение операций с помощью SMS. С чем это связано?

Д. КАЛЕМБЕРГ: SMS-канал изначально не был предназначен для передачи конфиденциальной информации. Сообщение может быть перехвачено огромным количеством способов как в канале оператора связи, так и в самом смартфоне. И мошенники отлично научились это делать! Соответственно, отправлять таким образом коды для подтверждения платежей – не лучшая идея. Другой вопрос в том, что очень долгое время SMS были самым дешевым «транспортом» до клиента, и банки этим активно пользовались.

NBJ: Какие есть альтернативы SMS?

Д. КАЛЕМБЕРГ: Чтобы кардинально снизить риски кражи денег, необходимо соблюсти два условия:

- не передавать коды подтверждения транзакций по незащищенным каналам связи, а генерировать их на стороне клиента;
- коды подтверждения должны формироваться в привязке к реквизитам каждой транзакции: то есть если мошенники как-то перехватят пароль, то его нельзя будет использовать для подтверждения другого документа.

Это можно сделать при помощи аппаратных средств (MAC-калькуляторов), но этот вариант довольно затратный и требует сложной логистики. Второй способ – использовать программные средства подписи, которые могут быть установлены на смартфон или вообще интегрированы в приложение мобильного банкинга.

NBJ: Расскажите, пожалуйста, поподробнее о решении PayControl, которое предлагает SafeTech.

Д. КАЛЕМБЕРГ: PayControl – приложение для смартфона или планшета, которое позволяет подписывать электронные документы и аутентифицировать клиентов. Пользователь видит реквизиты операции и подтверждает их одним движением. Решение не только намного безопаснее, но и намного удобнее, чем SMS-пароли, так как не требует ожидания и ручного ввода кода подтверждения. При этом подписать транзакцию можно, даже если смартфон находится в режиме офлайн.

NBJ: Есть ли у компании планы по расширению функционала решения?

Д. КАЛЕМБЕРГ: Да. У нас выходит новая версия продукта, которая интегрирована с сервисом облачной подписи «КриптоПро DSS», разработанным нашим партнером – компанией «КриптоПро». Совместное решение позволит подтверждать платежные документы квалифицированной электронной подписью прямо на смартфоне. Решение уже передано на сертификацию в ФСБ РФ и, на наш взгляд, идеально подходит системам мобильного банкинга для юрлиц. Теперь банки с минимальными затратами могут реализовать подтверждение платежных документов на мобильных устройствах квалифицированной подписью. С появлением интегрированного комплексного решения PayControl и «КриптоПро DSS» это стало реальностью. NBJ