DOI: 10.17117/na.2016.02.01.392

<http://ucom.ru/doc/na.2016.02.01.392.pdf>

Поступила (Received): 28.02.2016

Шумилина О.В., Езангина И.А.
Финансовая безопасность банка: риски ДБО

Shumilina O.V., Ezangina I.A.
The Bank's financial security: the risks of remote banking services

Статья посвящена проблемам обеспечения безопасности и защиты информации удаленных систем банковского обслуживания. Обозначены характерные угрозы для банковских клиентов в области дистанционного обслуживания, приведены статистические данные, характеризующие масштабы несанкционированных операций, предпринимаемые меры по минимизации рисков в данном сегменте банковской деятельности

Ключевые слова: дистанционное банковское обслуживание, ключ электронной подписи, система клиент-банк, интернет-банкинг, мобильный банкинг

Шумилина Ольга Викторовна

Студент

Волгоградский государственный технический университет

г. Волгоград, пр. Ленина, 28

Езангина Ирина Александровна

Кандидат экономических наук, доцент

Волгоградский государственный технический университет

г. Волгоград, пр. Ленина, 28

The article deals with the problems of security and data protection of remote banking systems. Marked specific threat to the bank in the field of remote customer service, the statistical data describing the scale of unauthorized transactions undertaken measures to minimize risks in this segment of the banking business

Key words: remote banking, electronic signature key client-bank system, internet banking, mobile banking

Shumilina Olga Victorovna

Student

Volgograd state technical university

Volgograd, Lenina ave., 28

Ezangina Irina Alexandrovna

Candidate of Economic Sciences, Associate Professor

Volgograd state technical university

Volgograd, Lenina ave., 28

В настоящее время дистанционное банковское обслуживание (ДБО) является неотъемлемой частью банковских услуг, объективно востребованное среди клиентов банка и получающее весомое развитие. Среди пользователей ДБО встречаются не только специалисты, способные защитить себя в информационной сфере, но и обычные люди, уделяющие недостаточно внимания компьютерной безопасности. Количество пользователей банковских услуг достигло уровня, серьезно интересующего злоумышленников, и рост популярности ДБО не замедляется – за счёт регионального развития.

О том, что проблемам обеспечения безопасности и защиты информации удаленных систем не всегда уделяется должное внимание, свидетельствует

многообразие мошеннических схем: банкоматные мошенничества, шимминг, фишинг, фарминг, атаки типа «распределенный отказ в обслуживании». Среди предпосылок развития различного рода финансового мошенничества в ДБО следует признать: количественный рост пользователей услуг; расширение качества и количества предоставляемых услуг; использование мобильных платформ при всем их разнообразии для работы с ДБО; недостаточная на сегодняшний день защита всего спектра устройств и платформ [2, с. 946].

В качестве базовой проблемы ДБО отмечаем сложность регулирования растущего количества пользователей. Действия, предпринимаемые клиентом для обеспечения достаточного уровня безопасности при совершении платежей с использованием дистанционных систем, банк только может зарегистрировать в соответствующем договоре. Заставить соблюдать клиента нужные требования банк не имеет возможности. В этой связи подчеркиваем необходимость поиска механизмов воздействия на каждого отдельного пользователя дистанционных услуг, их соответствующего обучения, а также привлечения внимания к уже имеющимся фактам мошенничества.

Основными угрозами для ДБО являются перехват ключей электронной подписи, кража регистрационных данных клиента (логин, пароль), одноразовых паролей и кодов авторизации. Несмотря на бесчисленное множество предупреждений на сайтах банков, в договорах, а также в СМИ, некоторые клиенты недостаточно понимают опасность и пути кражи денежных средств. Пользователи уделяют слишком мало внимания собственной безопасности в Интернете. Традиционными методами взлома систем ДБО выступают:

1. Кража закрытых ключей электронной подписи из оперативной памяти. Применяется в случае использования клиентом средства защищенного хранения ключей электронной подписи, которое позволяет извлекать их из закрытой области памяти устройства.

2. Кража ключей электронных подписей с незащищенных носителей. Наиболее простой вид атаки, которая реализуется на клиентах систем ДБО, которые хранят ключи электронной подписи на флешках, на жестком диске.

3. Подмена документа при передаче его на подпись в смарт-карту. Один из сложных и опасных видов атак. Пользователь на экране монитора видит одну информацию, а в смарт-карту на подпись отправляется другая. Также могут быть подменены данные о выполненных транзакциях, об остатке средств.

4. Несанкционированный доступ к криптографическим возможностям смарт-карты. Реализуется с помощью удаленного управления компьютером пользователя или с использованием удаленного подключения к USB-порту.

Также серьезное влияние на обеспечение безопасности ДБО систем оказывает уровень квалификации персонала и бюджет информационной безопасности. Недостаточный уровень квалификации ведет к такой проблеме как установленный по умолчанию на сетевом оборудовании пароль, единый пароль на разных ресурсах.

Согласно статистике Банка России в 2014 году было совершено более 300 тысяч несанкционированных операций на общую сумму более 3,5 млрд. рублей.

За 2014 год в Банк России было сообщено 4,89 тыс. случаев попыток осуществления несанкционированных операций посредством систем ДБО на общую сумму 1,64 млрд. рублей. Из них 825 операций на сумму около 900 млн. рублей были остановлены в полном объеме. Более 80% от количества всех операций с использованием систем ДБО связаны со списанием денежных средств со счетов физических лиц. Вместе с тем, при меньшем количестве несанкционированных операций, направленных на списание денежных средств со счетов клиентов – юридических лиц, на такие операции приходится больший объем денежных средств (73% объема операций).

Наибольшее число несанкционированных операций с использованием платежных карт осуществляется посредством сети Интернет и с помощью мобильной связи – на них приходится 65,8% всех операций. С начала 2014 года количество незаконных операций, совершенных посредством банкоматов и платежных терминалов, снизилось на 40,4% [4, с. 57].

Для снижения рисков и повышения безопасности, связанных с дистанционным обслуживанием, банки предпринимают организационные и технические меры. К организационным мерам относится предупреждение пользователей о возможных атаках, наложение ограничений на объемы операций, проведение соответствующего инструктажа клиентов. С точки зрения технических мер для защиты доступа клиентов к своим реквизитам предлагается использование электронных ключей и паролей. Эти меры направлены на обеспечение доказательств подлинности клиента при доступе к информационным ресурсам банка и обеспечение защиты информации пользователей.

Кроме того, 10 марта 2015 года вступило в силу Указание Банка России № 3361-У о необходимости кредитным организациям организовать регистрацию всех устройств, которые используют их клиенты для входа в приложения интернет-банкинга и мобильный банк [1]. Провести операции с незарегистрированных телефонов, компьютеров и планшетов будет невозможно. Кроме того, банки обязаны блокировать рассылку служебных SMS-сообщений (одноразовые пароли и т.п.) при смене клиентом номера или SIM-карты.

Среди новых решений в области безопасности электронных финансовых услуг отмечается также преимущества внедрения автоматизированной системы голосового подтверждения подозрительных платежей FraudInform. Последний реализует обратную связь с клиентом банка, с аккаунта которого был создан подозрительный платеж, обнаруженный антифрод-системой. Голосовое общение системы антифрода с клиентом включает подтверждение личности абонента и проверку реквизитов созданного платежа. Функции синтеза и распознавания речи позволяют организовать процесс подтверждения мошеннических платежей полностью в автоматическом режиме [3, с.856].

Таким образом, факторами, оптимизирующими риск мошенничества, выступают: надежность и защищенность программного обеспечения ДБО; механизм хранения и смены электронных ключей для доступа в ДБО и логина/пароля пользователя; уровень защищенности персонального компьютера, с которого осуществляются банковские операции; организационные процедуры проведения банковских операций через систему ДБО в организации.

Список используемых источников:

1. Указание Банка России от 14.08.2014 N 3361-У «О внесении изменений в Положение Банка России от 9 июня 2012 года N 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».
2. Езангина И.А. Научно-технический стратегический альянс: воплощение реализации принципа «открытых инноваций» // *Фундаментальные исследования*. 2013. №6-4. С. 945-948.
3. Езангина И.А., Шахбазян Е.М. Микрофинансовые организации в России: опыт прошлого, настоящее, будущие перспективы // *Экономика и предпринимательство*. 2015. № 4-1 (57-1). С. 854-859.
4. Езангина И.А., Шумилина О.В. PFM-система управления личными финансами клиента банка: будущее в России // *Современные тенденции развития науки и технологий*. 2015. № 8-7. С. 56-59.

© 2016, Шумилина О.В., Езангина И.А.
 Финансовая безопасность банка: риски ДБО

© 2016, Shumilina O.V., Ezangina I.A.
 The Bank's financial security: the risks of remote banking services