ТЕХНИЧЕСКИЕ НАУКИ

Фирсова Анна Михайловна
студентка
Абдулаева Зада Лахилавна
канд. экон. наук, доцент, заведующая кафедрой

филиал ФГБОУ ВО «Санкт-Петербургский государственный
экономический университет» в г. Кизляре
г. Кизляр, Республика Дагестан

ПРИНЦИПЫ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

Аннотация: *в данной статье рассматриваются основные методы взлома систем дистанционного банковского обслуживания, а также принципы защиты от атак мошенников.*

Ключевые слова: *интернет-банкинг, банковские карты, электронная подпись.*

Дистанционное банковское обслуживание (ДБО) предоставляет возможность получения банковских услуг удаленно, при помощи компьютерных либо телефонных сетей [3]. Система интернет-банкинга стала неотъемлемой частью услуг, предоставляемых сегодняшними банковскими системами [1]. Доля операций, совершаемых по электронным каналам связи, постоянно растет, и вместе с этим растет роль систем ДБО. Вместе с этим растут и угрозы потери финансов в результате действий мошенников. Число преступлений в области ДБО за период 2013–2014 год увеличилось в 4 раза.

Рассмотрим методы взлома систем дистанционного банковского обслуживания:

1. Кража ключей электронной подписи. Эта технология является наиболее распространенной. Она подразумевает кражу электронной подписи с незащищенных носителей – флеш-карт, дисков либо папок на жестком диске.

2. Кража закрытых ключей электронной подписи из оперативной памяти. Если клиент пользуется средствами защищенного хранения электронной подписи, то мошенники используют вирусы, которые позволяют извлекать электронную подпись из оперативной памяти компьютера.

3. Несанкционированный доступ к криптографическим возможностям смарт-карты. Одна из наиболее опасных и перспективных атак. Реализуется либо при помощи средств удаленного управления компьютером клиента (класса TeamViewer), либо с использованием удаленного подключения к USB-порту (технология USB-over-IP). Ограничением для данной атаки является обязательное подключение смарт-карты (токена) в момент ее проведения.

Подмена документа при передаче его на подпись в смарт-карту. Наиболее сложный и опасный на сегодняшний день вид атак. В данном случае пользователь видит на экране монитора одну информацию, а в смарт-карту на подпись отправляется другая. Параллельно могут быть подменены данные об остатках на счете, выполненных транзакциях [4].

Рассмотрим, как можно защититься от атак мошенников. Почти все российские банки перешли на технологию двухфакторной аутентификации. В этом случае вся ключевая информация хранится в смарт-карте и её нельзя извлечь. Смарт-карта предоставляет множество возможностей. Она одновременно может являться и банковской картой, и картой доступа к другим сервисам, к примеру, порталу государственных услуг. Если банку не безразличны риски, которые возникают при внедрении технологии дистанционного банковского обслуживания, то он должен предлагать клиенту смарт-карту. Смарт-карта не может обеспечить полной защиты. Аутентификацию можно дополнить введением одноразовых паролей. Эта система может быть реализована по-разному, в виде OTP-токенов или приложений, функционирующих на мобильном телефоне, с использованием SMS-канала, специальных SIM-карт или защищенных SD-карт, установленных в мобильное устройство. Хорошим вариантом дополнительного фактора аутентификации является биометрия. Она может использоваться как средство доступа к

токену, если считыватель смарт-карты оснащен еще и биометрическим датчиком. Применение биометрии делает перехват пароля к USB-ключу гораздо более проблематичным [5].

Не следует забывать и о среде, в которой исполняются банковские приложения. Программное обеспечение банковских приложений зачастую имеет уязвимости. Защита должна быть построена на высоком уровне. На рынке уже появились средства, предоставляющие доверенную среду для проведения операций электронной подписи. Среди них – компьютеры, в которых средства доверенной загрузки реализованы в BIOS (например, фирмы Kraftway). Это позволяет исключить воздействие вирусов, загружаемых до запуска системы, и вирусов, модифицирующих сам BIOS. Появились на рынке и считыватели смарт-карт с визуализацией значимых полей подписываемого документа. Платежный документ после формирования передается по USB в считыватель и на его экран выводятся значимые поля документа. Наложение подписи инициируется нажатием кнопки на устройстве и происходит в его изолированной среде, а уже подписанный документ передается обратно в компьютер. Таким образом, исключается возможность атак с подменой документа и с захватом управления компьютером.

Серьезное влияние на безопасность ДБО оказывает уровень квалификации персонала, его достаточность и мотивация, а также бюджет информационной безопасности. Недостаточная квалификация и мотивация ведут к таким, казалось бы, уже давно надоевшим, но все еще актуальным проблемам, как установленный пароль по умолчанию на сетевом оборудовании, единый пароль на разных ресурсах, удаленный доступ в обход общих правил и политик. Поголовная виртуализация и стремление «в облака» также не уменьшают количество проблем [2].

Пользователю ДБО следует быть внимательным, так как чаще всего причиной мошеннического доступа к счету пользователя Интернет-банкинга является неосторожность самого пользователя. А потому, чтобы избежать возможных проблем, владельцу учетной записи следует беречь данные доступа к ней. Во-

первых, эксперты советуют периодически изменять пароли для доступа в систему, желательно делать это раз в месяц и не использовать интернет-банкинг на непроверенных компьютерах (например, в интернет-кафе). Помимо этого, следует соблюдать осторожность при работе в Интернете. Мошенники широко используют приемы «социальной инженерии» для того, чтобы выманить аутентификационные данные (логин, пароль и т. д.) клиентов. Наиболее старый метод – «фишинговые» письма электронной почты, которые провоцируют получателей отправить свои аутентификационные данные злоумышленникам или предлагают пройти по ссылке на мошеннический сайт. Однако безопасность можно рассматривать как состояние, при котором уровень риска использования сервиса приемлем как для пользователя, так и для владельца. Качество предоставляемой услуги ДБО для банков – это вопрос привлечения клиентов. Качество определяется, прежде всего, объемом предоставляемых услуг, удобством использования, доступностью и защищенностью. Именно защищенность становится все более весомым критерием при выборе системы ДБО и в немалой степени влияет на выбор банка.

Список литературы

1. Абдулаева З.Л. Проблемы внедрения электронной цифровой подписи в Республике Дагестан [Текст]. Материалы X научно-практической конференции «Ключевые вопросы в современной науке – 2014», г. София, Болгария. – С. 15–18.

2. Издание о высоких технологиях // [Электронный ресурс] / Режим доступа: http://www.cnews.ru

3. Издание – Электронная энциклопедия Wikipedia // [Электронный ресурс] / Режим доступа: http://www.wikipedia.org

4. Интернет-журнал TadViser // [Электронный ресурс] // Режим доступа: http://www.tadviser.ru

5. Интернет-журнал Computerra // [Электронный ресурс] / Режим доступа: http://www.computerra.ru