УДК 336.717

ПРИМЕНЕНИЕ ДИСТАНЦИОННОГО БАНКИНГА: РИСКИ СОВЕРШЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И ПУТИ ИХ МИНИМИЗАЦИИ

Зиниша О.С.,
к. э. н., доцент
ФГБОУ ВО «КубГАУ имени И. Т. Трубилина»,
Краснодар, Россия

Стрельникова Т.О.,
студент
ФГБОУ ВО «КубГАУ имени И. Т. Трубилина»,
Краснодар, Россия

Аннотация

В данной статье авторами рассматривается одна из наиболее динамично развивающихся сфер банковской системы – дистанционный банкинг. По итогам проведенного исследования было выявлено, что быстрое развитие и масштабное внедрение систем дистанционного обслуживания имеет положительные моменты и для банка, и для клиента, но такая растущая популярность сопровождается и определенными рисками. Несмотря на то, что банки постоянно совершенствуют систему безопасности дистанционного обслуживания клиентов, мошенники изобретают новые пути обхождения этой системы.

Ключевые слова: дистанционный банкинг, фишинг, скиммингговые устройства, биометрическая идентификация.

THE USE OF REMOTE BANKING: THE RISKS OF COMMITTING UNAUTHORIZED ACCESS AND WAYS TO MINIMIZE THEM

Zinisha O.S.,
candidate of Economic Sciences, associate Professor
Kuban State Agrarian University named by I.T. Trubilin,
Krasnodar, Russia

Strelnikova T.O.,
student of the faculty of Economics
Kuban State Agrarian University named by I.T. Trubilin,
Krasnodar, Russia

Annotation

The article deals with one of the most dynamically developing spheres of the banking system – remote banking. According to the results of the study, the rapid development and large-scale implementation of remote service systems has positive aspects for both the bank and the client, but this growing popularity is accompanied by certain risks. Despite the fact that banks are constantly improving the security system of remote customer service, fraudsters are inventing new ways to circumvent this system.

Keywords: remote banking, phishing, skimming devices, biometric identification.

Одной из основных тенденций развития мировой экономики является виртуализация хозяйственных процессов. Широкое распространение получила сетевая экономика, основной характеристикой которой является осуществление предпринимательской деятельности при помощи глобальной информационной

сети. Так называемая «интернетизация» охватила все сферы общественной жизни людей: банковская система не стала исключением. Необходимость более эффективного решения новых задач, связанных с обеспечением безбумажных, менее затратных технологий обслуживания клиентов с высокой пропускной способностью, характеризующихся значительным уровнем централизации банковских процессов, повышенными требованиями к безопасности систем. Таким универсальным решением и выступает дистанционный банкинг.

Дистанционный банкинг представляет собой совокупность методов предоставления банковских услуг клиенту, оказываемых посредством служб сети Интернет – дистанционно [5]. Применение дистанционного банкинга в полной мере обеспечивает реализацию одного из ключевых принципов работы с населением в банковской сфере – простоты и удобства оказания услуг. Иначе говоря, большую часть операций с клиентом обслуживающий банк может осуществить без его присутствия: необходимо лишь распоряжение, направленное клиентом удаленным образом [3].

Возникновение и становление дистанционного банкинга ознаменовало принципиально новый этап в развитии банковской сферы. Система дистанционного обслуживания обеспечила реализацию упрощенной схемы взаимодействия банка с клиентом, что обусловило ее популярность среди российского населения. Однако такое повсеместное распространение спровоцировало и определенные риски, заключающиеся в осуществлении мошеннических операций с целью хищения конфиденциальных данных клиентов банка и последующей кражей средств с их счетов. Итак, перейдем к рассмотрению проблем, связанных с внедрением дистанционного обслуживания в банковской сфере России.

Самым распространенным видом мошеннических операций, применяемых на территории России, является фишинг. Данный термин образуется от сочетания английских слов «fishing» и «password», которое

можно перевести как «ловля пароля». Сущность данного вида мошеннической операции сводится к созданию фишингового сайта – страницы, являющейся зеркальным отображением Интернет-ресурса официального источника. Чтобы клиент банка смог перейти на фишинговый сайт и ввести данные своей банковской карты, злоумышленники, как правило, отправляют письмо на адрес электронной почты. При этом текст переданного сообщения должен вызвать интерес или беспокойство пользователя, чтобы он действительно перешел по закрепленной ссылке и ввел личные данные. Например, подобным образом действует группировка «WhiteBear»: она использует целевые фишинговые письма для доставки жертвам зараженных PDF-файлов [6 с. 5].

Второй тип мошеннических операций – это установка вредоносных программ. Как и применение фишинга, хакеры направляют электронные письма сотрудникам банка от имени клиентов. Открытие письма сопровождается заражением компьютера вирусом, которое записывает и сохраняет данные клиентов банка в базе данных.

Согласно отчету «Лаборатории Касперского» за 2017 год, банковское вредоносное программное обеспечение расширило набор применяемых инструментов. Так, в 2017 году было выявлено несколько новых методов кражи денежных средств клиентов банка. Одна из них получила название «FakeToken». Работа данного троянца заключается в перекрытии мобильного приложения банка фишинговыми сайтами, предназначенными для кражи данных банковской карты пользователя. Также в июле 2017 года была обнаружена еще одна вредоносная программа – Svpeng. Она запрашивала у клиента банка право использовать специальные возможности, а затем выдавала себе разрешения для отправки SMS-сообщений, совершения звонков и др. Используя эти специальные возможности, программа беспрепятственно получала данные, вводимые через интерфейсы мобильных приложений [6, с. 27].

Однако действия мошенников не ограничиваются атаками в Интернет-среде. Банковские терминалы и автоматы также являются объектом нападения. Для похищения персональных данных владельца банковской карты применяются скимминговые устройства, а сам процесс называется «скиммингом».

Сущность скимминга заключается в считывании данных с магнитной полосы, расположенной на банковской карте, при помощи скиммера. Скиммер представляет собой конкретную часть банковского автомата, которая производит операцию фиксирования данных с пластиковой карты. Он крепится непосредственно к банкомату, причем заметить наличие дополнительного устройства сможет лишь наблюдательный человек [4].

Итак, владелец пластиковой карты вставляет ее в банковский автомат, не подозревая о наличии кардридера, установленного мошенником. В это время, скимминговое устройство начинает считывать данные с магнитной полосы банковской карты. После получения всех данных, необходимых для ввода, злоумышленники создают дубликат пластиковой карты клиента банка. Зная номер карты, имя владельца, а также PIN-код, они беспрепятственно получают доступ к счету жертвы и могут распоряжаться находящимися на ней средствами.

Для того чтобы обезопасить себя от действия скимминговых устройств при использовании банковского терминала, необходимо следовать определенным правилам, которые отображены в таблице 1.

Таблица 1. - Способы защиты от скимминговых устройств [4]

№	Содержание правила
1	Использовать терминалы и банкоматы, расположенные непосредственно в отделениях банка. В этом случае мошенникам будет трудно установить скиммеры.

2	Перед тем как, вставить карту в приемник, необходимо внимательно осмотреть банкомат.
3	Никому не сообщать PIN-код от банковской карты.
4	Подключить услугу SMS-информирования, которая будет оповещать о любой операции, производимой по карте.
5	Установить лимит на выдачу средств в сутки и за одну операцию.
6	При вводе PIN-кода необходимо прикрывать свои пальцы другой рукой

В условиях борьбы за привлечение клиента, банки стремятся преодолеть или минимизировать потери от вышеуказанных мошеннических операций. Для поддержания доверия клиента и, следовательно, своей репутации, они создают всевозможные способы защиты от вмешательства.

Дистанционный банкинг как одно из направлений банковского дела имеет большой потенциал для дальнейшего развития в России. В будущем возможно создание полноценного электронного рынка, на котором можно будет совершать все банковские операции посредством служб Интернет.

Вместе с тем важно отметить, что с увеличением возможностей дистанционного банкинга как одного из наиболее динамично развивающихся банковских сервисов, растут и возможности мошеннических атак, в результате которых совершается хищение денежных средств, находящихся на счете клиента. В этом случае, кредитным организациям приходится разрабатывать меры по контролю над банковскими рисками и управления ими с учетом новых источников и компонентов информационных контуров банковской деятельности и возникновением новых вариантов проявления рисков, связанных с удаленным предоставлением банковских услуг.

Рассмотрим, какие методы защиты денежных средств клиентов применяют российские коммерческие банки на сегодняшний день.

Первый метод – это получение SMS-сообщений о транзакциях, осуществляемых с банковской картой клиента. Такой способ контроля считается наиболее популярным среди граждан РФ, пользующихся услугами коммерческих банков. Для осуществления операции необходимо подтверждение в виде пароля, которое приходит на телефонный номер клиента. Операция не производится до тех пор, пока не будет введен направленный пользователю пароль [2].

Второй метод связан с проведением банковских операций через официальные сайты банков. Речь идет о шифровании данных, которая представляет собой технологию, обеспечивающую безопасность передачи трафика между браузером клиента и веб(ресурсом коммерческого банка. Сущность шифрования данных заключается в том, что при установлении соединения с сайтом перехват данных мошенниками становится невозможным, так как на протокол «http» накладывается защита. Как было указано ранее, хакеры, пытаясь обойти систему шифрования, создают фишинговые сайты, которые во многом схожи с оригиналом, а пользователь, не задумываясь, вводит личные данные [2]. Чтобы избежать этого, пользователю следует посмотреть на адресную строку, а также проверить наличие защищенного соединения, которое представлено в виде зеленого замка.

Говоря о перспективных направлениях защиты данных клиентов банка, следует выделить биометрическую идентификацию, представляющую собой систему распознавания и измерения черт и особенностей, присущих отдельно взятому человеку: это может быть геометрическое строение руки или лица, отпечатки пальцев, сетчатка глаза, тембр голоса и т.д.

Использование биометрической идентификации позволит выйти российским банкам на новый уровень развития дистанционного обслуживания. Было установлено, что деятельность мошенников строится на

невнимательности самих клиентов банка. В результате злоумышленник получает PIN-коды к банковским картам и уже свободно распоряжается денежными ресурсами жертвы. Применение биометрической системы идентификации позволит минимизировать риски, связанные с внедрением и использованием дистанционного обслуживания.

Так, Альфа-банк с 1 ноября 2018 года начал предоставлять возможность доступа к банковской ячейке без присутствия сотрудника банка: клиентам необходимо лишь отсканировать на установленном устройстве рисунок вен ладони. Такая услуга доступна лишь во флагманском офисе по работе с состоятельными клиентами. Управляющий директор «Альфа Private» Катерина Милеева пояснила, что решение о распространении подобной технологии в других отделениях банка будет приниматься на основании анализа использования депозитария во флагманском офисе [1].

Рисунок вен был выбран в качестве критерия биометрической идентификации, потому что этот рисунок не меняется на протяжении жизни человека, в связи с чем отпадает необходимость регулярного обновления базы данных.

По прогнозам консалтинговой компании «J’son & Partners Consulting», которые приводит ЦБ РФ в своем обзоре рынка биометрии, идентификация клиентов по рисунку вен ладони (наряду с голосом и радужной оболочкой глаза) в ближайшие пять-семь лет будет самым быстрорастущим видом идентификации в России [1].

На сегодняшний день российские банки не так активно применяют биометрическую технологию для идентификации клиентов, что связано со значительными инвестициями для установки всех необходимых устройств.

Таким образом, можно сделать вывод, сегодня российские банки отражают большую часть атак и предотвращают многие мошеннические операции благодаря уже существующим средствам, но общество развивается,

меняются потребности клиентов банка. В связи с этим появляется потребность внедрения новых технологий для удовлетворения требований потребителей.

Библиографический список:

1. Альфа-банк начал идентифицировать клиентов по венам на ладони [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/finances/01/11/2018/5bd9950d9a79470031da1a07?utm_source=vk_rbc, свободный. – (дата обращения: 27.11.2018).

2. Виды афер и махинаций с платежными картами - как распознать обман и не стать жертвой мошенников [Электронный ресурс]. – Режим доступа: https://sovets.net/13102-moshennichestvo-s-bankovskimi-kartami.html, свободный. – (дата обращения: 27.11.2018).

3. Особенности развития банковской системы в современной экономике / Гончарова Н.А., Дубровская О.В. // Экономика и управление: актуальные вопросы теории и практики. Материалы VI международной научно-практической конференции. - Саратов, 2017. - С. 41-45.

4. Скимминг в банкоматах [Электронный ресурс]. – Режим доступа: http://www.chclub.ru/skimmingatm, свободный. – (дата обращения: 27.11.2018).

5. Что такое дистанционное банковское обслуживание или интернет банкинг [Электронный ресурс]. – Режим доступа: https://superobmen.org/chto-takoe-distancionnoe-bankovskoe-obsluzhivanie/, свободный. – (дата обращения: 27.11.2018).

6. Kaspersky Security Bulletin 2017. Развитие угроз [Электронный ресурс]. – Режим доступа: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2018/03/09043350/KSB_Review-of-2017_final_RU.pdf, свободный. – (дата обращения: 27.11.2018).

Оригинальность 95%