УДК 004

СОВЕРШЕНСТВОВАНИЕ МЕР ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ДИСТАНЦИОННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ

Карпов А.С.,
студент, Финансовый университет,
Москва, Россия
makspaks@mail.ru

Аннотация. *Цель данной работы — исследовать современные методы защиты информации в дистанционном банковском обслуживании (ДБО), а также предложить возможные направления совершенствования безопасности информации в ДБО. Задачи данной работы были построены на необходимости проанализировать систему дистанционного банковского обслуживания и ее компоненты, определить ключевые нормативно-методические документы, регламентирующие информационную безопасность, ее проблемы в ДБО. Результатом исследования следует считать рекомендации по обеспечению информационной безопасности в ДБО.*

Ключевые слова: *дистанционное банковское обслуживание; информационная безопасность; персональные данные; проблемы информационной безопасности при ДБО.*

IMPROVEMENT OF INFORMATION SECURITY MEASURES AT REMOTE BANK SERVICE

Karpov A.S.,
student, Financial University,
Moscow, Russia
makspaks@mail.ru

Abstract. *The purpose of this work was to research modern methods of protecting information in remote bank service, as well as suggesting possible directions for improving the security of information at remote bank services. The tasks of this work were based on the need to analyze the remote banking system and its components, identify key regulatory and methodological documents that regulate information security of remote services, information security problems in remote banking services. The results of this work are recommendations for information security of remote banking services.*

Keywords: *remote bank service; information security; personal data; problems of information security in remote banking.*

Научный руководитель: ***Дворянкин С.В.,*** *доктор технических наук, профессор, заместитель заведующего кафедрой информационной безопасности, Финансовый университет, академик РАЕН.*

Современный темп жизни ускоряется, потребность в получении различных услуг на расстоянии возрастает во всех сферах общества. Сегодня для того, чтобы быть эффективным и продуктивным, требуется умение распределять время. По этой причине дистанционные услуги постепенно проникают во все слои жизнедеятельности человека. Одной из сфер, в которую дистанционное обслуживание проникло достаточно уверенно, является банковская.

Дистанционное банковское обслуживание (ДБО) представляет собой тенденцию модернизации в сфере обслуживания. Стараясь обеспечить клиента всеми необходимыми и основными услугами, которые предоставляет банк на расстоянии, ДБО становится главным способом связи между клиентом и банком. Помимо преимуществ, для клиентов, заключающихся в удобстве и быстроте получения услуг, дистанционное обслуживание сокращает расходы банков на операционную деятельность.

Взаимодействие клиента и банка через среду ДБО означает, что в ней циркулирует конфиденциальная информация, в частности персональные данные (ПДн) клиентов, и данные, относящиеся к банковской тайне. Соответственно через ДБО злоумышленник может получить доступ к конфиденциальной информации, что повлечет за собой убытки различного рода как для клиента, так и для банка. Необходимо обеспечить информационную безопасность циркулирующих данных. Задачей информационной безопасности всегда являлось сохранение как уже указанной конфиденциальности, так и целостности, и доступности информации. Это в полной мере относится и к ДБО.

Прежде чем переходить к конкретизации, а именно — совершенствованию мер защиты информации в ДБО, надлежит разобраться в основах, которые непосредственно связаны с задачей этой работы. Определившись, что информация при дистанционном обслуживании требует защиты, следующим действием будет установление мер обеспечения информационной безопасности. Основными средствами информационной безопасности для организаций являются меры, которые условно можно разделить на три основных направления:

1. Организационно-правовые.
2. Программно-аппаратные.
3. Технические.

Условность разделения заключается в комплексном подходе к информационной безопасности, при котором все ее аспекты связаны между собой. Далее станет очевидно, что разновидности ДБО не однородны и представляют различные технологии. По этой причине меры, которые необходимо применять для информационной безопасности ДБО, разнообразны. Следовательно, способы, которыми пользуются злоумышленники для достижения своих целей, будут отличаться в зависимости от вида дистанционного обслуживания.

Для более ясного представления введем определение ДБО — предоставление банком услуг клиенту на расстоянии, чаще всего с использованием сети Интернет. Существуют несколько видов дистанционного обслуживания, которые классифицируются по типу программно-аппаратного средства: банкоматы, система «Клиент-банк», мобильный банкинг (см. *рисунок*).

Виды ДБО

Целью развития различных видов дистанционного обслуживания является постепенный отказ от географически распределенных отделений банка и перекладывание функций на ДБО. Остановимся на каждом виде дистанционного обслуживания из-за необходимости ясно осознавать, что является объектом информационной безопасности. Дистанционное обслуживание при помощи банкоматов является первой из разработанных технологий предоставления услуг на расстоянии. Есть возможность выделить несколько типов такого вида ДБО:

- банкоматы;
- платежные терминалы;
- информационные киоски.

Отличие платежных терминалов и информационных киосков от банкоматов заключается в предоставляемых услугах, причем полнофункциональными принято считать банкоматы, которые позволяют использовать широкий спектр услуг. В отличие от банкоматов, право на установку которых имею лишь банки и коммерческие организации, платежные терминалы может установить индивидуальный предприниматель. Главным является то, что банкомат оперирует со счетом клиента, а платежный терминал — с внесенными в него средствами. Простейшим примером информационных киосков являются аппараты по присуждению номера в очереди при выборе запрашиваемой услуги в отделении банка.

Следующим видом дистанционного обслуживания является система «Клиент-банк», в которой доступ к банковским услугам происходит с использованием персональных компьютеров клиентов. Существует две разновидности системы «Клиент-банк», которые различаются предоставляемым функционалом и возможностями. Система «Банк-клиент», или «толстый клиент», представленная клиентским приложением на персональном клиенте, предоставляет наиболее полный функционал услуг банка. Программа хранит на устройстве данные и информацию, относящуюся к операциям клиента. Чаще всего таким видом ДБО пользуются организации различного рода, в то время как физические лица предпочитают выбирать облегченную версию, получение доступа к функционалу которой осуществляется через интернет-браузер. Интернет-банкинг, или «тонкий клиент», не требует от пользователя установки специфичного программного обеспечения (ПО) и позволяет воспользоваться услугами банка, пройдя авторизацию на сайте.

Последним и набирающим все большую популярность из-за удобства доступа и функциональности является мобильный банкинг или «Телефон-банк». Мобильный банкинг предоставляет услуги дистанционного обеспечения при помощи мобильных устройств и телекоммуникационных технологий. К мобильному банкингу относится телефонный банкинг и СМС-банкинг. Телебанк представляет собой приложение на основных мобильных операционных системах, через который пользователь взаимодействует с банком. На раннем этапе развития телефонный банкинг предоставлял пользователю только информационные услуги и не обладал функционалом, сравнимым с клиентскими программами для персональных компьютеров. С развитием технологий телефонный банкинг обрастает новым функционалом, которым обладают системы «Клиент-банк». СМС-банкинг чаще всего стал использоваться как дополнительный способ безопасности и информирования клиентов, используется в дополнение к другим видам дистанционного обслуживания.

Получив общие представления о разновидности технологий дистанционного обслуживания, мы убедились, что подходы к оказанию услуг разнообразны и способы обеспечения безопасности информации, применимые для одного вида ДБО, могут не сработать при другой технологии.

Проблемы безопасности информации при использовании банкоматов в большей степени связаны с мошенничеством, а именно — со скиммингом. Установка специального оборудования на банкоматы мошенниками для считывания информации с вставленных клиентами карт или для видеозаписи набираемых PIN-кодов позволяет злоумышленникам получить доступ к ПДн и счетам владельцев.

В отличие от мошенничества с кредитными картами в банкоматах, вопрос безопасности информации в системах «Банк-клиент» надлежит разделить на проблему безопасности приложения и средства доступа. Угрозы без-

опасности информации в системе «Клиент-банк» относятся к разному роду уязвимостям. Согласно исследованию[1], проведенному компанией Positive Technologies, актуальные уязвимости можно распределить по нескольким категориям:

1. Недостатки реализации механизмов защиты.
2. Недостатки конфигурации.
3. Уязвимости в коде приложений.
4. Устаревшее ПО[2].

Исследование заключалось в анализе существующих ДБО систем и их уязвимостей. Важно отметить, что уязвимостям безопасности также подвержено оборудование, которое использует дистанционное приложение, т.е. персональные компьютеры. В частности, уязвимости клиентских программ классического ДБО актуальны и для телебанка.

Мобильные системы ДБО под управлением iOS по-прежнему обладают более высоким уровнем защищенности по сравнению с системами под Android, где 75% систем подвержены критически опасным уязвимостям. Однако треть уязвимостей, обнаруженных в приложениях для iOS, характеризуются высокой степенью риска. Эти недостатки связаны с хранением и передачей важных данных в открытом виде. Каждое приложение на базе Android содержит 3,8 уязвимости, что примерно соответствует уровню 2013 и 2014 гг. (3,7). Для iOS-приложений данный параметр равен 1,6, что значительно лучше результата предыдущих лет, когда на каждое приложений приходилось 2,3 уязвимости[3].

Следующим шагом надлежит установить методы защиты информации, применяемые в ДБО. Уязвимости, которые могут быть реализованы злоумышленниками, различаются для каждого из способов обслуживания, из-за чего необходимо использование различных методов обеспечения безопасности информации.

Особенностью безопасности информации в ДБО является построение защиты, которое необходимо реализовать как клиенту, так и банку. В случае использования банкомата со стороны клиента потребуются определенные шаги для обеспечения безопасности данных, а именно: бдительность при взаимодействии с банкоматом, зрительный поиск следящих устройств и накладных устройств на считыватель карт и клавиатуру, набор PIN-кода с ограниченным для посторонних обзором. Со стороны банка производятся периодические мероприятия по контролю банкоматов на наличие мошеннического оборудования, установка оборудования активного и пассивного обнаружения скиммингом. Также в поддержание информационной безопасности банкоматов со стороны банка устанавливается безопасное соединение между устройством и сервером обработки запросов банкомата. Защита «толстого клиента» основывается на обеспечении безопасности рабочей станции и локальной вычислительной сети (ЛВС). Проблемы несанкционированного доступа (НСД) к рабочей станции, с которой происходит взаимодействие с ДБО, осуществляется организационными и программно-аппаратными средствами. Многофакторная аутентификация внедрена в системы «Клиент-банк» и мобильный банкинг для уменьшения рисков НСД. Антивирусные системы, в том числе системы класса endpoint[4], защищают от проникновения и инициализации вредоносного программного обеспечения (ВПО), целью которого может являться хищение платежной информации, идентификационных данных, нарушение функционирования бизнес-процесса ДБО. Сетевая безопасность ЛВС строится на межсетевых экранах и системах IPS/IDS. Надежность информационной безопасности (ИБ) интернет-банкинга должна строиться на защищенном соединении, которое шифрует передаваемый трафик. Для

[1] Уязвимости приложений финансовой отрасли. Positive Technologies. URL: http://www.ptsecurity.com/upload/ptru/analytics/Financial-Vulnerability-2016-rus.pdf

[2] Уязвимости приложений финансовой отрасли // Positive Technologies. 2016. URL: http://www.ptsecurity.com/upload/ptru/analytics/Financial-Vulnerability-2016-rus.pdf (дата обращения: 01.04.2017).

[3] Positive research 2016 // Positive Technologies. 2016. URL: http://www.ptsecurity.com/upload/ptru/analytics/Positive-Research-2016-rus.pdf (дата обращения: 12.04.2017).

[4] Endpoint system — антивирусные системы, обладающие расширенным функционалом по защите персональных компьютеров и серверов.

это используется стек протоколов SSL/TLS. Со стороны банка должны существовать идентичные шаги по обеспечению безопасности ЛВС. Для контроля транзакций в системе дистанционного обслуживания банками внедряются и применяются антифрод-системы, которые анализируют активность пользователей и блокируют подозрительные транзакции и операции, основываясь на проанализированных данных активности.

Любые меры безопасности должны быть подкреплены нормативно-методической базой для четкого регулирования понятий требования и правил. Сферу дистанционного банковского обслуживания в России регулируют как национальные нормативные и законодательные нормы, так и международные стандарты. Международными стандартами, которые обеспечивают информационную безопасность дистанционного обслуживания, являются EMV и PCI DSS.

PCI DSS — международный стандарт безопасности данных в индустрии платежных карт. Стандарт представляет собой набор требований к компаниям, которые взаимодействуют с платежными системами Visa и MasterCard. Стандарт обязывает организации проходить регулярные проверки на соответствие требованиям.

Требования стандарта PCI DSS распространяются на все компании, которые обрабатывают, хранят или передают данные о держателях платежных карт (банки, процессинговые центры, сервис-провайдеры, e-commerce и т.п.). Причем требования относятся только к тем информационным системам компании, в которых обрабатывается или хранится информация о платежных картах, а также к системам, которые с ними взаимосвязаны[5].

EMV — международный стандарт, определяющий безопасность финансовых операций по банковским картам с чипом. Этот стандарт используется международными платежными системами VISA и MasterCard.

Стандарт EMV определяет физическое, электронное и информационное взаимодействие между банковской картой и платежным терминалом для финансовых операций[6].

Национальная нормативно-законодательная база по защите информации при ДБО в России представлена законами, постановлениями, приказами, стандартами и другими рекомендательными документами. Стоит отметить, что существуют три главных регулятора: Федеральная служба по техническому и экспортному контролю (ФСТЭК), Федеральная служба безопасности и Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Центральный банк Российской Федерации (ЦБ РФ) является органом, который регулирует кредитную систему страны. Как уже было ранее сказано, в ДБО циркулирует конфиденциальная информация, Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» дает общие представления о необходимости соблюдения конфиденциальности, в частности ст. 16. «Защита информации» описывает основные понятия и принципы, которым должны следовать операторы информационных систем и обладатели информации в части ее защиты. Следующим законодательным актом, регулирующим ИБ данных, является Федеральный закон № 152-ФЗ «О персональных данных», определяющий, что является ПДн, регламентирующий обработку и хранение таких данных, определяющий, какие информационные системы являются информационными системами персональных данных (ИСПДН). Наличие ПДн определяют системы ДБО, как ИСПДН, а операторы перевода денежных средств — как оператора ПДн. Соответственно операторы обязаны соблюдать требования по обеспечению конфиденциальности ПДн. В соответствии со ст. 19 152-ФЗ Правительство Российской Федерации издало постановление № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в котором определены возможные угрозы безопасности ПДн трех типов, закрепляются 4 уровня защищенности ПДн.

[5] Сертификация по PCI DSS // Digital Security. URL: https://dsec.ru/services/certification/certification-according-to-pci-dss/ (дата обращения: 22.05.2017).

[6] EMV. URL: https://ru.wikipedia.org/wiki/EMV (дата обращения: 02.05.2017).

Из-за специфики сферы деятельности ЦБ РФ выпускает документы по информационной безопасности для организаций банковской сферы. Так, правовой статус положения № 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» закрепляется Федеральным законом № 161-ФЗ «О национальной платежной системе». Положение 382-П в вопросе защиты ДБО предъявляет набор требований к оператору перевода денежных средств с использованием систем дистанционного обслуживания. В обязанности оператора входит обеспечение процессов идентификации, аутентификации и авторизации клиентов в системе, разработка ПО, обеспечивающего защиту от НСД, информирование пользователей систем ДБО о ложных ресурсах и ПО, имитирующие ресурсы оператора. Положение также вводит требования к информационной безопасности банкоматов, обязуя операторов по переводу денежных средств к поддержанию безопасности на требуемом уровне.

Постановление Правительства РФ № 584 утверждает положение «О защите информации в платежной системе».

Положение устанавливает требования к защите информации о средствах и методах обеспечения информационной безопасности, персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемой операторами по переводу денежных средств, банковскими платежными агентами (субагентами), операторами платежных систем и операторами услуг платежной инфраструктуры в платежной системе (далее соответственно — информация, операторы, агенты)[7].

ЦБ РФ разработан комплекс документов под название «Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации». Стандарт носит рекомендательный характер, но при заявлении организации о присоединении, организация обязывается выполнять требования по ИБ в соответствии со стандартом. По состоянию на 1 июля 2016 г., 511 организаций банковской системы Российской Федерации приняли решение о введении в действие СТО БР ИББС[8].

Совершенствование защиты информации представляется в необходимости выполнение следующих действий:

- введение единых требований к информационной безопасности в системах ДБО;
- повышение информационной грамотности клиентов в вопросе безопасного использования и взаимодействия с системами ДБО и платежными картами;
- внедрение ограничительных механизмов на операции, как функция для пользователей;
- отказ банковских организаций от хранения конфиденциальной информации на серверах в открытом виде;
- шифрование потоков данных при установлении соединения между устройством системы ДБО и процессами банка.

Проблемы защиты информации при дистанционном обслуживании не являются нерешаемыми. Банкам следует заполучить специалистов по ИБ систем и процессов ДБО для уменьшения уязвимостей, связанных с программным кодом приложений. Принять во внимание стандарт СТО БР ИББС, который позволяет повысить эффективность ИБ. Существуют инциденты ИБ, которые возможно избежать, если пользователь будет знать, что от него требуется для сохранения его данных конфиденциальными. Согласно 161-ФЗ оператор перевода денежных средств обязан возместить пользователю средства, переведенные в результате несанкционированной транзакции. Поэтому информирование клиентов о соблюдении правил информационной безопасности при взаимодействии с ДБО является желательным для оператора.

[7] Постановление Правительства РФ от 13.06.2012 № 584 «Об утверждении Положения о защите информации в платежной системе». URL: http://base.garant.ru/70189962/ (дата обращения: 22.05.2017).

[8] Список организаций БС РФ, информация о принятии решения о введении в действие Комплекса БР ИББС, в которых получена Банком России по состоянию на 01.07.2016. URL: http://www.cbr.ru/credit/Gubzi_docs/spisok.pdf.