

Проблемы информационной безопасности, влияющие на развитие системы мобильных платежей



УДК 336.74:004.056(470+571)

В настоящее время вопрос применения мобильных платежей при формировании собственной национальной платежной системы является одним из актуальнейших. Поскольку переход на мобильные платежные системы в России, а также внедрение систем безопасности против их взлома требуют определенных затрат, в нынешних экономических условиях у кредитных организаций должны быть достаточно серьезные мотивы для внедрения новых систем. В то время как снижаются доходы бизнеса, увеличение расходов на внедрение новых систем может представляться нерациональной стратегией. Однако положительной стороной мобильных платежей является то, что они позволят снизить капитальные расходы, при понимании того, что технологии внедрения уже разработаны, их не надо создавать заново. Дальнейшее широкое применение мобильных платежей неразрывно связано с обеспечением необходимого уровня безопасности. В статье рассматриваются основные угрозы, с которыми могут столкнуться потребители при оплате товаров и услуг с помощью мобильного телефона.

Ключевые слова

Мобильные платежи, безопасность, национальная платежная система.

Автор

Лахно Юлия Викторовна — менеджер ФГУП «Международное информационное агентство „Россия сегодня“», аспирант кафедры систем управления бизнес-процессами Российской академии народного хозяйства и государственной службы при Президенте РФ.

По мере того как мобильные телефоны будут трансформироваться в часть платежной системы, потребители все меньше будут нуждаться в наличных денежных средствах. Более того, возможно, отпадет необходимость брать с собой для совершения покупок банковские карты (кредитные/дебетовые). Достаточно будет ввести информацию — текстовый код — в мобильный телефон и установить соответствующие программы (конечно, при наличии у торговых предприятий всего необходимого оборудования для считывания информации), как это уже делается в странах Западной Европы и США.

Для того чтобы мобильные платежи могли действительно широко применяться, необходимо обеспечить соответствующий уровень безопасности, при котором в первую очередь учитывались бы интересы потребителя.

Для понимания проблемы безопасности мобильных платежей в России Центральным банком

По мере того как мобильные телефоны будут трансформироваться в часть платежной системы, потребители все меньше будут нуждаться в наличных денежных средствах.

ным платежам с привязанной банковской картой и посредством Интернета сейчас высока — около 65,8% от всех операций [1]. Количество мошенничеств в IV квартале 2014 г. по сравнению с III кварталом 2014 г. выросло на 42%, а по объему — на 86%. Повышение средней суммы такой операции составило увеличение с 2,6 тыс. до 3,3 тыс. руб. [1]. Данные цифры говорят об уменьшении инцидентов, связанных с банкоматами и платежными терминалами при одновременном росте объемов мобильных и интернет-хищений.

Если клиент не уверен в защищенности своих денежных средств и персональной информации, которую он сообщает оператору или кредитному учреждению, то данная модель платежной системы не сможет развиваться, клиент просто не будет ею пользоваться.

а также сотрудников банков, то есть на так называемый человеческий фактор.

На данный момент наиболее уязвимым звеном информационной безопасности является клиент. Во всем мире ущерб от хищения средств и персональных данных оценивается в миллиарды долларов [2]. Зачастую потребитель сам грубо нарушает требования безопасности, раскрывая персональные данные злоумышленникам. В меньшей степени киберкражи происходят в результате атак хакеров на компьютер клиента.

Нарушение клиентом требований безопасности может быть связано с излишней сложностью инструментов безопасности, ведь данные системы требуют от клиента определенных знаний, дисциплины, следования конкретным и не всегда простым инструкциям. Другим примером атак является провоцирование мошенниками клиентов на совершение определенных действий при помощи различных психологических уловок. Несмотря на то что банки предлагают клиентам ознакомиться с рекомендациями по безопасности, в большинстве случаев клиенты не обращают внимания на это. Решением проблемы может стать повышение финансовой грамотности населения и выстраивание работы таким образом, чтобы соблюдался максимальный уровень защиты при невозможности совершения иного действия. Однако не стоит упускать из виду работу над усовершенствованием систем безопасности, попытки сделать их более простыми и менее зависимыми от человеческого фактора.



собирается статистика инцидентов по всем операторам по переводу денежных средств. Из обзора о несанкционированных переводах денежных средств Центрального банка России 2014 г. следует, что доля мошеннических действий по мобиль-

Человеческий фактор в нарушении безопасности мобильных платежей

В основном действия злоумышленников направлены на банковские системы и на клиентов,

Правовая защита от незаконных действий в области мобильных платежей

Вместе с тем вопросы нормативно-правового обеспечения безопасности мобильных платежей имеют большое значение. Если правовые вопросы осуществления мобильных платежей не будут решены на должном уровне, весь рынок уйдет в интернет-коммерцию, которую очень сложно регулировать на законодательном уровне. Стремление

их возврата, но при условии подачи заявления оператору, ответственному за перевод денежных средств, а также в правоохранительные органы [4].

Зачастую клиенты не знают своих прав. Банки заинтересованы в защите прав потребителей, ведь их задачей является привлечение как можно большего количества клиентов. Если клиент доверяет сервису и знает, что его интересы будут соблюдаться на законодательном уровне, он нач-



многих стран оградить себя от такой неконтролируемой валюты, как биткойн, стимулировало становление и развитие мобильных платежных систем. Финансовый рынок нуждается в обновлении, во внедрении инновационных продуктов, которые могли бы заменить существующие наличные виды расчетов и банковские переводы. В нормативные документы был внесен ряд изменений, регламентирующих использование NFC-технологий, ужесточающих условия предоставления sim-карт (их приобретение теперь в большинстве случаев возможно только при наличии паспорта), а также идентификацию через третьих лиц [3], которыми могут выступать операторы сотовой связи.

В случае же хищения денежных средств в результате мошеннических действий Законом о национальной платежной системе предусматривается возмож-

но нет более активно использовать сервис. Психологический тормоз снимется, появится удовлетворенность обслуживанием, что в дальнейшем обеспечит доходность банковской деятельности. В данном вопросе банкам следует брать на себя максимальную ответственность по защите интересов клиентов. В случае если в банке заявят, что клиент сам несет ответственность за хищение денежных средств, очевидным результатом будет отказ от мобильных платежей.

Бывают случаи, когда банки сознательно снижают уровень безопасности систем мобильного банкинга. Это происходит при конкуренции на рынке и делается в угоду клиенту, чтобы привлечь его удобством использования. Для недопущения подобного необходим минимальный набор принципов, к реализации которых кредитные организации должны стремиться [5].

Внешние атаки на банковские системы

Гораздо серьезнее и по масштабу, и по количеству украденных данных являются атаки на банковские системы. В данном случае мошенники находят слабые места в программном обеспечении и взламывают его. С точки зрения таких атак в группе риска находятся прежде всего мобильные приложения. Большинство обладателей смартфонов скачивают и устанавливают приложения на свои телефоны. Такие приложения могут заранее иметь дефект, а могут быть и нелегальными. Особенно много случаев зафиксировано на платформе *Android* [6]. В данном случае возможен рост фальсификации платежей при онлайн-оплате.

ЦБ РФ предъявляет жесткие требования к банкам по соблюдению информационной безопасности, но, несмотря на это, количество взломов и утечек данных ежегодно растет. Для выполнения требований безопасности необходимо, чтобы банки прописывали их уже при разработке технического задания, а затем тестировали. Лучше обнаружить ошибки в системе на этапе проверки, чем пытаться исправить их уже непосредственно в рабочем процессе [7].

В целом же технически очень сложно проникнуть в систему



Примером атак является провоцирование мошенниками клиентов на совершение определенных действий при помощи различных психологических уловок.

безопасности банка снаружи, поэтому чаще всего применяются атаки на клиентов и сотрудников банка.

Современные средства оплаты требуют повышенной безопасности. Развитие современных технологий стимулирует не только повышение удобства для клиента, но и рост мошеннических операций. В дальнейшем видится только увеличение таких инцидентов, и для того, чтобы противостоять несанкционированным переводам денежных средств, необходимо сфокусировать внимание операторов при сборе статистических данных на Интернет и мобильные платежи.

При этом необходимо предоставлять информацию по каждому направлению отдельно. При постоянном мониторинге и настройке оценки защищенности клиента затраты на безопасность будут окупаться. Опыт западных стран показывает, что эффективность работы повышается в 5 раз при внедрении высоких технологий.

На данный момент видится, что одновременное развитие технологий защиты и повышение грамотности населения может стать ключом к изменению восприятия мобильных платежей.

С ростом доверия потребителей платежи с помощью мобильного телефона перейдут из разряда технических новшеств для молодежи в самостоятельный конкурентоспособный и перспективный инструмент оплаты.

ПЭС 15091/27.07.2015

Источники

1. Обзор о несанкционированных переводах денежных средств. 2014 г. М.: Банк России. 2015 (июнь). С. 10, 17.

2. Сенаторов М. СТО БР ИББС — тот самый фундамент, на котором финансово-кредитные организации могут выстраивать собственные системы информационной безопасности // Национальный банковский журнал NBJ. 2013. № 11 (114).

3. Письмо ЦБ РФ от 28 января 2014 г. № 14-Т — бенефициарный владелец.

4. Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе», ст. 12.

5. Сумманен К. Обеспечивая информационную безопасность, банки должны искать некую золотую середину по принципу «клиенту еще удобно, а мошеннику уже невыгодно» // Национальный банковский журнал NBJ. 2013. № 11 (114) // The best publications 2003–2013. С. 60.

6. Mobil Banking [Электронный ресурс] // Bank Info Security. URL: <http://www.bankinfosecurity.com/mobile-banking-c-106>.

7. Скогорева А. Инфосистема «Джет» предлагает комплексный подход // Национальный банковский журнал NBJ. 2014. С. 106–107.

Safety as the Essential Part of Mobile Payments' Development

Yulia Lakhno

During these days the problem of implantation of the mobile devices into the National payment system is of current interest. As the example of paying particular attention to the mobile services can be the approval of the bill, expanding the law about the National payment system, during the government session of the RF July 9, 2015. The bill will give the opportunity to the telecommunications provider to provide subscribers with the funds to increase the balance of electronic money (EMF). Further widespread use of mobile payments is inextricably linked to the essential security level. The article covers the main directions of threats, with which customers may meet during the payment for goods and services using a mobile phone.

Keywords: mobile payments, safety, national payment system.