Проблемы безопасности электронной коммерции в сети Интернет

Абдеева Зульфия Рашидовна
аспирантка 1 года обучения
Башкирский государственный университет, экономический факультет, г.Уфа, РБ
E–mail: *zulfia92007@yandex.ru*

Безопасность является ключевым вопросом для внедрения электронной коммерции. Основным препятствием, возникающим на пути развития рынка Интернет-платежей, является психологический фактор, связанный с осознанием угрозы потенциального мошенничества. Люди до сих пор не рассматривают Интернет как безопасную среду, чему способствуют объективная информация о степени безопасности работы в Интернете. Опросы показывают, что более всего люди боятся потенциальной угрозы получения кем-либо их персональных данных при работе через Интернет. По данным платежной системы VISA около 23% транзакций с банковскими картами так и не производятся из-за боязни клиента ввести запрашиваемую электронным магазином персональную информацию о клиенте. В результате, люди главным образом используют Интернет в качестве информационного канала для получения интересующей их информации [3,240].

***

Мошенничество может быть совершено также путем отказа от операций, сделанных при помощи электронных денег. Например, при дистанционных операциях, совершаемых при помощи телефона или компьютерных сетей, пользователь может заявить, что не разрешал проводить операцию. Это, в свою очередь, может привести к финансовым потерям торгового предприятия или эмитента электронных денег [8].

***

При достаточно обширном списке мер, предпринимаемых для обеспечения безопасных расчетов в сети Интернет, многое зависит от самого пользователя. Часто причиной мошеннического доступа к счету пользователя Интернет-банкинга является невнимательность и неосторожность самого пользователя. Поэтому, чтобы избежать возможных проблем, владельцу учетной записи необходимо беречь данные доступа к ней. Необходимо периодически изменять пароли для доступа в систему и не использовать Интернет-банкинг на непроверенных компьютерах [9].

Доля интернет-торговли неуклонно растет из года в год, увеличиваются обороты от продажи товаров и услуг в сети, пропорционально растет и количество мошеннических операций, но мало кто хочет отказываться от получаемых выгод, поэтому всех участников процесса все больше волнует безопасность проведения платежей и расчетов [4, 48].

Одним из эффективных направлений защиты информации является криптография или криптографическая информация, широко применяемая в различных сферах деятельности в государственных и коммерческих структурах [1,1].

***

Но все же решить проблему обеспечения надежности информационной безопасности исключительно с помощью технических средств и программного обеспечения невозможно. По мнению специалистов, защита корпоративных информационных систем зависит от ряда факторов: на 30% – от применяемых технических решений; на 40% – от проводимых в учреждении организационных мероприятий и на 30% – от морально-нравственного состояния общества и общекультурного уровня пользователя.

Более половины кредитных организаций не имеют специалистов по информационной безопасности. Некоторые банки администрируют задачи филиалов с удаленных и головных офисов. Но эти мероприятия носят фрагментарный характер, поэтому задачи по обеспечению безопасности практически не решаются. Особенно не защищены филиалы, где системы часто не настроены, внутренние сети, как правило,

соединены с внешними, неправильно эксплуатируются межсетевые экраны и средства АРМ-клиента – Банка России. На откуп специалистам IT функции безопасности передают 42% банковских подразделений. Но для них это направление работы является непрофильным, носит второстепенный и фрагментарный характер [7, 84].

Необходимо помнить, что проблемы безопасности онлайновых услуг связаны также и с отсутствие нормативно-правовой базы: закона об электронно-цифровой подписи, комплекта нормативных актов прямо регулирующих права и обязанности участников оборота онлайновых финансовых услуг, гарантий по выполнению распоряжений отданных в электронной форме, толкования подобных операций соответствующими контролирующими и надзорными ведомствами, все эти обстоятельства тормозят развитие электронных банковских услуг. Сегодня вопросы обеспечения безопасности онлайновых банковских операций каждый банк решает в отдельности путём использования профессиональных средств защиты. Однако банкам потребуется немало времени и усилий, прежде чем они смогут заручиться доверие таких средств защиты у значительной массы клиентов [6, 69-81].

Литература

1. ГОСТ Р 34.10-94 Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
2. Букин М. Активная безопасность ДБО // Банковские технологии. — 2010 — №10.
3. Голдовский И. Безопасность платежей в Интернете — СПб: Питер, 2001.
4. Гончаров В.В. Безопасность и защита интернет-платежей // Расчеты и операционная работа в коммерческом банке. — 2010 — №4.
5. Калемберг Д. Токен является ключевым элементом информационной безопасности в новых условиях // Банковские технологии. — 2010 — №1.
6. Кочергин Д. А. Развитие онлайновых банковских услуг в экономически развитых странах и России — Известия Санкт-Петербургского государственного университета экономики и финансов. – СПб.: Изд-во СПбГУЭиФ, 2001. – № 2.
7. Тимошкин А.В. Эволюция финансового контроля теневой экономики. Защита информации и технологий – условие стабильности банковской системы // Банковское дело. — 2009 — №6.
8. Горюков Е.В., Котина О.В. Электронные деньги: развитие, направления использования в современной банковской практике (окончание) http://bankir.ru/tehnologii/s/elektronnie-dengi-razvitie-napravleniya-ispolzovaniya-v-sovremennoi-bankovskoi-praktike-okonchanie-1373402/
9. Резниченко Е. Безопасность Интернет-банкинга: практические аспекты http://www.prostobank.ua/internet_banking/stati/