

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМАХ – АКТУАЛЬНЫЙ ВОПРОС ЭЛЕКТРОННОЙ КОММЕРЦИИ

М. Я. Мансурова

Узбекистан, Ташкент, ТУИТ

С введением электронной коммерции приоритетным вопросом становится обеспечение безопасности. Безопасность является ключевым вопросом при внедрении систем и форм электронной коммерции. Быстрый рост компьютерной коммерции, сделок в Интернет и других сетях обусловили постановку данного вопроса в числе приоритетных.

Безопасность электронной коммерции - состояние защищенности хозяйствующих субъектов, совершающих коммерческие операции на рынке с помощью технологии электронной коммерции, от угроз материальных потерь, потерь времени или иных потерь.

При решении вопроса безопасности в электронной коммерции на первый план выходит задача обеспечения безопасности в платежных системах. Сформированы основные требования к схемам проведения транзакций электронной коммерции в платежных системах, обеспечивающие необходимый уровень их безопасности. Эти требования сводятся в основном к следующему:

- аутентификация участников покупки (покупателя, торгового предприятия и его обслуживающего банка). Под аутентификацией покупателя (продавца) понимается процедура, доказывающая факт того, что данный владелец карты действительно является клиентом некоторого эмитента-участника (обслуживающего банка-участника) данной платежной системы. Аутентификация обслуживающего банка доказывает факт того, что банк является участником данной платежной системы;
- реквизиты платежной карты (номер карты, срок ее действия, CVC2/CVV2 и т.п.), используемой при проведении транзакции электронной коммерции, должны быть конфиденциальными для торгового предприятия;
- невозможность отказа от транзакции для всех участников транзакции электронной коммерции то есть наличие у всех участников неоспоримого доказательства факта совершения покупки (заказа или оплаты);
- гарантирование магазину платежа за электронную покупку - наличие у торгового предприятия доказательства того, что заказ был им выполнен.

Рассмотрим безопасность в электронной коммерции на примере некоторых платежных систем.

Платежная система CyberPlat. Основное ее достоинство - безопасность, как с финансовой, так и с юридической точки зрения. Во-первых, CyberPlat основана на широко распространенной технологии криптографической защиты информации с помощью цифровой подписи. Эта технология позволяет не только предохранить информацию от «любителей совать нос» в «чужие дела», но и однозначно определить автора любого сообщения, а также убедиться, что сведения не были изменены во время передачи по сети Интернет. Во-вторых, система CyberPlat основана на комплексе юридических договоров, полностью соответствующих законодательству. Это дает продавцам и покупателям твердую уверенность в том, что существует четкая и определенная законом процедура решения всех спорных вопросов, возникающих при расчетах между участниками сделки.

Платежная система Paypal. Электронная платежная система PayPal является на данный момент одной из самых популярных и надежных среди зарубежных платежных систем. К началу 2006 года она обслуживает пользователей из 55 стран.

Для передачи информации используются SSL протоколы с кодовым ключом 128-bit. Вся информация поступает на сервер, который защен как от физического, так и от

электронного взлома. Сервер оснащен брандмауарами и напрямую не подключен к Интернет.

Платежная система CyberCash

Известная компания, работающая на рынке безопасных Интернет-платежей, сейчас активно предлагает всем своим клиентам работу по протоколу SET, пропагандируя его преимущества. Преимущества использования SET сводятся к следующему:

- продавцы защищены от покупок с помощью неавторизованной платежной карточки и от отказа от покупки;
- банки защищены от неавторизованных покупок;
- клиенты не пострадают от перехвата номера кредитки и от покупки у несуществующих продавцов.

Платежная система WebMoney. Система Интернет расчетов, использующая «цифровые наличные». Безопасность гарантируется системой на основе уникальных ключей шифрования, которые действительны в течении одного сеанса. Поэтому при последующих сделках реквизиты предыдущих не являются действительными. Для каждой сделки используются уникальные реквизиты, и попытка использовать их вторично немедленно отслеживается и гасится. Для работы в системе требуется установить бесплатную программу WM Keeper. Напрямую взломать сервер WebMoney или перехватить данные во время транзакций невозможно. Сам WM Keeper устойчив к попыткам несанкционированного доступа. Используются алгоритмы кодирования RSA, RC5, MD4, MD5, SSL. Пользователь WebMoney может чувствовать себя защищенным, если только он сам не клонет на уловки мошенника. Главные требования безопасности, которые вам следует выполнять:

- хранить файл .kwm в надежном месте (желательно на сменном носителе) ;
- помнить пароль на вход и код доступа к .kwm;
- соблюдать общеизвестные рекомендации: не открывать подозрительных вложений в письмах, не скачивать и не запускать сомнительные программы, пользоваться антивирусами.

Система устойчива по отношению к обрывам связи. Если любая операция в системе не была успешно завершена по причине обрыва связи, то система не учитывает данную операцию.

Платежная система ASSIST. В системе ASSIST безопасность платежей обеспечивается использованием SSL протокола для передачи конфиденциальной информации от клиента на сервер системы ASSIST для дальнейшей обработки. Дальнейшая передача информации осуществляется по закрытым банковским сетям высшей степени защиты. Обработка полученных конфиденциальных данных клиента (реквизиты карты, регистрационные данные и т.д.) производится в процессинговом центре. Таким образом, никто, даже продавец, не может получить персональные и банковские данные клиента, включая информацию о его покупках, сделанных в других магазинах.

Для повышения безопасности заказов информация о банковских картах клиента не сохраняется на сервере. Обработка карточных данных ведется на безопасном высокотехнологичном сервере процессинговой компании. Для защиты информации от несанкционированного доступа на этапе передачи от клиента на сервер системы ASSIST используется протокол SSL 3.0, сертификат сервера (128 bit) выдан компанией Thawte - признанным центром выдачи цифровых сертификатов.

Ведение электронной коммерции в открытых сетях требует эффективных и надежных механизмов, гарантирующих безопасность всех ее участников. Эти механизмы должны обеспечивать конфиденциальность, аутентификацию (то есть возможность для каждой стороны в заключаемой сделке удостовериться в личности другой стороны) и гарантию того, что стороны впоследствии не смогут отрицать своего участия в сделке. Поскольку признанные механизмы поддержки безопасности основаны на сертификации

третьей стороной, глобальная электронная коммерция требует наличия глобальных сертификационных систем.

Однако, расширение использования электронных денег неизбежно, по той простой причине, что, несмотря на некоторые недостатки, они обладают такими неоспоримыми преимуществами, как удобство, высокая скорость совершения финансовых операций, простота использования, обеспечение полного контроля за платежами и их высокая безопасность, анонимность, возможность передачи третьим лицам. Кроме того, системы электронных платежей также значительно расширяют возможности небольших организаций, чьи расходы на операции с наличными деньгами значительно выше по сравнению с цифровыми, включая их хранение и транспортировку. Использование сети Интернет уже сейчас позволяет продавцам обеспечить себе выход на рынки с более низкими издержками на маркетинг и рекламу. Экономия, которую обеспечивает переход к электронным деньгам, выглядит очень заманчиво для банков, поскольку себестоимость любых электронных транзакций в несколько раз ниже обычных.

Для Республики Узбекистан задача развития электронной коммерции является одной из приоритетных. Для устойчивого развития электронной коммерции правительством республики была совершенствована нормативно-правовая база. А именно были разработаны и введены в действие Законы Р.Уз. «Об электронном документообороте», «Об электронной цифровой подписи», «Об электронной коммерции». Пересмотрен Закон Р.Уз. «Об информатизации». Внесены изменения и дополнения в Законы Р.Уз «О стандартизации», «О сертификации продукции и услуг», «О телекоммуникациях», «Об электронных платежах» от 16.12.2005 года, Постановлением Кабинета Министров №120 от 12 июня 2007 г. «О мерах по дальнейшему совершенствованию проведения платежей при осуществлении электронной коммерции» и др. Также внесены изменения в «Гражданский кодекс», «Уголовно-процессуальный кодекс». Принятие указанных законов позволит урегулировать вопросы, связанные с процедурами заключения и регистрации сделок.

Литература:

1. Информационная безопасность в электронной коммерции. (Республиканский семинар «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения.» УзАСИ. Ташкент: 24 октября, 2007 г. с. 46) Сборник докладов. Мансурова М.Я.
2. Актуальные проблемы безопасности в электронной коммерции. –(Ж. Алока дунёси, Ташкент: 2007, №3, с. 52) Сборник докладов. Исаходжаева М.Я, Мансурова М.Я.
3. <http://www.cyberplat.ru>
4. <http://www.webmoney.ru>
5. <http://www.assist.ru>
6. «Merchant's Guide to E-commerce Payment Gateways» доктор Ральф Ф. Вильсон (<http://www.wilsonweb.com>)
7. Необходимость платежных систем Интернет. Основные требования Е-commerce.ru.