УДК 336.717:004.78

ЗАЩИТА ИНФОРМАЦИИ В ИНТЕРНЕТ-ПЛАТЕЖНЫХ СИСТЕМАХ

Рассмотрены механизмы обеспечения целостности и аутентичности банковской информации в Интернет- платежных системах

С.П. Евсеев
Кандидат технических наук, доцент*
Контактный тел. (057)702-18-31
e-mail: Evseev_serg@inbox.ru

О.Г. Король
Преподаватель*
Контактный тел. (057)702-18-31
e-mail: korol_o@mail.ru
*Кафедра информационных систем
Харьковский национальный экономический университет
проспект Ленина 9-а, г. Харьков, Украина, 61001

А.С. Жученко
Кандидат технических наук, доцент
Кафедра «Транспортная связь»
Украинская государственная академия железнодорожного транспорта
ул Фейербаха, 7, г. Харьков, Украина, 61000.
Контактный тел. (097) 219-07-50
e-mail: rtcp@mail.ru

Введение

Стремительное развитие электронной коммерции привело к разработке множества самых различных электронных платежных систем, функциональные возможности которых постоянно расширяются и усложняются. Одним из самых прогрессирующих направлений развития платежных систем являются Интернет-платежные системы (ИПС), позволяющие производить мгновенные и безналичные транзакции, используя виртуальные счета и электронные деньги [1-3]. Увеличение объемов обрабатываемых и передаваемых данных в ИПС, вовлечение банков в электронную коммерцию требует новых подходов к обеспечению информационной безопасности ИПС. Целью статьи является исследование принципов построения и анализ основных угроз безопасности ИПС, обоснование общих требований к применяемым методам и механизмам защиты информации.

Принципы построения и основные угрозы безопасности ИПС

ИПС – система проведения расчетов между финансовыми, бизнес-организациями и Интернет-пользователями в процессе покупки/продажи товаров и услуг через Интернет. Именно платежная система позволяет превратить службу по обработке заказов или электронную витрину в полноценный магазин со всеми стандартными атрибутами: выбрав товар или услугу на сайте продавца, покупатель может осуществить платеж, не отходя от компьютера [4-10].

В системе электронной коммерции платежи совершаются при соблюдении ряда условий:

1. Соблюдение конфиденциальности. При проведении платежей через Интернет покупатель хочет, чтобы его данные (например, номер кредитной карты) были известны только организациям, имеющим на это законное право.

2. Сохранение целостности информации. Информация о покупке никем не может быть изменена.

3. Аутентификация. Покупатели и продавцы должны быть уверены, что все стороны, участвующие в сделке, являются теми, за кого они себя выдают.

4. Средства оплаты. Возможность оплаты любыми доступными покупателю платежными средствами.

5. Авторизация. Процесс, в ходе которого требование на проведение транзакции одобряется или отклоняется платежной системой. Эта процедура позволяет определить наличие средств у покупателя.

6. Гарантии рисков продавца. Осуществляя торговлю в Интернет, продавец подвержен множеству рисков, связанных с отказами от товара и недобросовестностью покупателя. Величина рисков должна быть согласована с провайдером платежной системы и другими организациями, включенными в торговые цепочки, посредством специальных соглашений.

7. Минимизация платы за транзакцию. Плата за обработку транзакций заказа и оплаты товаров, естественно, входит в их стоимость, поэтому снижение цены транзакции увеличивает конкурентоспособность. Важно отметить, что транзакция должна быть оплачена в любом случае, даже при отказе покупателя от товара.

Все указанные условия должны быть реализованы в платежной системе Интернет. Таким образом, все платежные системы по имеющейся схеме платежей можно разделить на:

дебетовые (работающие с электронными чеками и цифровой наличностью);

кредитные (работающие с кредитными карточками).

Дебетовые схемы платежей построены аналогично их оффлайновым прототипам: чековым и обычным денежным. В схему (см. рис. 1) вовлечены две независимые стороны: эмитенты и пользователи. Под эмитентом понимается субъект, управляющий платежной системой. Он выпускает некие электронные единицы, представляющие платежи (например, деньги на счетах в банках). Пользователи систем выполняют две главные функции. Они производят и принимают платежи в Интернет, используя выпущенные электронные единицы. Примерами дебетовых систем являются: система Assist – платежная система, позволяющая пользователям производить электронные платежи в режиме реального времени; Яндекс. Деньги (бывшая PayCash).

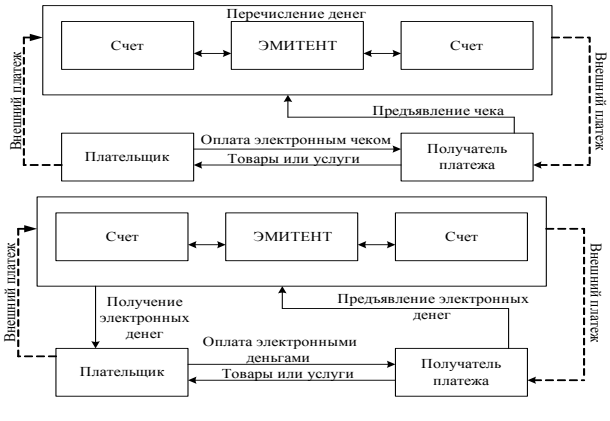

Рис. 1. Дебетовые схемы платежей с помощью электронных чеков и денег

Интернет-кредитные системы (см. рис. 2) являются аналогами обычных систем, работающих с кредитными картами.

Отличие состоит в проведении всех транзакций через Интернет, и как следствие, в необходимости дополнительных средств безопасности и аутентификации (“виртуальные” платежные системы: WebMoney, Рапида, E-port, КредитПилот, банковские – FakturaPAY и CyberCheck).

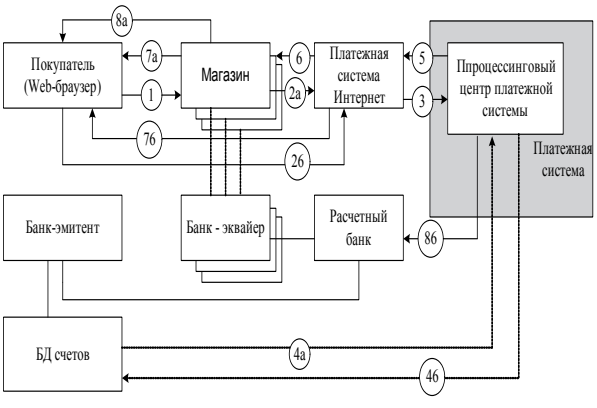

Рис. 2. Общая схема платежей в интернет-кредитной системе

Таблица 1

Способы нанесения ущерба	Объекты воздействий			
	Оборудование	Программы	Данные	Персонал
Раскрытие (утечка) информации	Хищение носителей информации, подключение к линии связи, несанкционированное использование ресурсов	Несанкционированное копирование перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашение, халатность
Потеря целостности информации	Подключение, модификация, спец. вложения, изменение режимов работы, несанкционированное использование ресурсов	Внедрение “троянских коней” и “жучков”	Искажение, модификация	Вербовка персонала, “маскарад”
Нарушение работоспособности автоматизированной системы	Изменение режимов функционирования, вывод из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение

Существующие на данный момент электронные платежные системы по типу доступа к электронному счету можно разделить на 2 большие группы:

– требующие установки на компьютер пользователя дополнительного программного обеспечения;

– платежные системы имеющие веб-интерфейс;

Основными преимуществами электронных платежных систем являются [9]:

– доступность – любой пользователь имеет возможность открыть собственный электронный счет;

– мобильность – независимости от места своего нахождения пользователь может осуществлять любые финансовые операции со своим счетом;

– простота использования – для открытия и использования электронного счета не требуется специальных знаний;

– оперативность - перевод средств со счета на счет происходит в считанные минуты.

Вместе с тем, актуальными остаются проблемы безопасности в электронных системах, традиционно являющиеся одним из ключевых вопросов финансового бизнеса.

Кроме того, для всех этих предложений пока не разработана жесткая система стандартов, которые так же повлияли бы на развитие и принятие электронных платежных систем.

Классификация видов нарушений работоспособности таких систем и несанкционированного доступа к информации по объектам воздействия и способам нанесения ущерба безопасности приведена в табл.1.

Для обеспечения защиты от нарушений Интернет-платежные системы должны иметь собственную систему защиты информации, отвечающую современным требованиям.

Анализ требований информационной безопасности ИПС

Поскольку Интернет одновременно является и чрезвычайно эффективным коммуникативным средством и средой, вызывающей достаточно большое недоверие у пользователей, безопасность электронных платежей является весьма серьезным критерием успеха конкретной системы и использующего ее электронного бизнеса. Важно, чтобы при любой реализации в системе не оставалось плохо защищенных участков, способных привести к крупномасштабному мошенничеству [10]. Поэтому основными требованиями по информационной безопасности являются:

– исключения возможности списания средств с аккаунта плательщика третьими лицами;

– обеспечение возможности легитимного подтверждения плательщиком перед третьими лицами (например, судом) факта совершения платежа, его получения получателем и назначения данного платежа (например, получения товара надлежащего качества);

– обеспечение возможности легитимного подтверждения получателем перед третьими лицами факта получения платежа и его назначения;

– обеспечение возможности легитимного подтверждения эмитентом факта проведения всех авторизованных транзакций по данному аккаунту действительным владельцем данного аккаунта;

– обеспечение гарантий, что перемещаемая с аккаунта сумма не будет украдена в момент передачи и попадет точно и исключительно по назначению;

– исключение возможностей подделки квитанций эмитента пользователям;

– обеспечение разрешения всех спорных вопросов между эмитентом и пользователями исключительно электронным образом с помощью сообщений с цифровой подписью;

– обеспечение возможности разрешения спорных вопросов между пользователями без участия эмитента; система в целом должна быть устойчива к мошенническим действиям, в том числе - в случае форс-мажорных обстоятельств.

Интернет в целом, и любые платежи всегда тесно связаны с понятием конфиденциальности. Поэтому необходимо, чтобы платежная система сама по себе не навязывала пользователям никаких нарушений конфиденциальности, а предоставление расширенной и дополнительной информации всегда оставлялось на усмотрение пользователя. Таким образом, требования по конфиденциальности включают в себя:

– исключение возможности получения информации о действиях пользователей сторонними наблюдателями;

– обеспечение необходимой степени анонимности плательщика для получателя платежа;

– исключение возможности получения эмитентом информации о назначении платежа;

– исключение возможности получения эмитентом информации о том, с каким из поступлений на аккаунт получателя связано каждое из списаний с аккаунта плательщика.

Требования к реализации обычно направлены на простоту и надежность работы системы, поскольку отказы в таких решениях могут привести к большим финансовым потерям сторон. Требования по реализации следующие:

– Система должна быть простой - как с точки зрения пользователей, так и для разработчиков. Простота системы удешевляет и ускоряет ее реализацию и техническую поддержку, способствует расширению сообщества применяющих ее организаций и привлекает потребителей.

– Система должна базироваться на хорошо проверенной и надежной технологии, что также будет залогом простоты ее реализации и уверенности в достаточном уровне безопасности.

– Система должна иметь возможность работать с пользователями извне организации, использующей данную платежную систему, так как очевидно, что множество потенциальных пользователей не являются сотрудниками этой организации.

– Помимо изложенных выше требований, к любой платежной системе применимы традиционные для любой онлайновой системы требования по гибкости, масштабируемости и эффективности.

– Для обеспечения безопасности в Интернет-платежных системах используется технология протокола SSL и электронная цифровая подпись на основе криптографического алгоритма RSA с длиной ключа в 1024 бита.

Вместе с тем, доминирование в Интернете традиционных платежных систем (со своими стандартами

защиты электронных транзакций) не только препятствует дальнейшему развитию электронной коммерции, но и угрожает полностью остановить ведение определенных видов е-бизнеса. Результаты исследований, информационные сообщения подтверждают это мнение [11].

Количество онлайновых подложных транзакций, осуществляемых при помощи кредитных/дебетовых карт, в 12 раз выше, нежели в оффлайне. Эта разница выливается в дополнительные потери, которые наносят ощутимый урон прибыльности электронной коммерции. В результате исследования, объектами которого стали 165 обычных, интернет- и смешанных магазинов, было выявлено, что 1.15% всех онлайновых покупок являются подложными в сравнении с 0.06-0.09% в оффлайне. При этом 64% от всех chargebacks (операция принудительного возврата компанией-эмитентом незаконно списанных средств на карточный счет клиента), связанных с онлайновым бизнесом, являются следствием подложных транзакций, в то время как в оффлайне только 44% от всех chargebacks связаны с подлогом.

Недоверие покупателей к онлайновым платежным системам является основным препятствием для развития электронной коммерции в различных странах. Почти 40% всех интернет-пользователей заявили, что боязнь "засветить" свою кредитную/дебетовую карту в Интернете является основным сдерживающим от совершения онлайновых покупок фактором. Таким образом, повышение безопасности платежных систем является ключевым моментом для привлечения клиентов и повышения доверия покупателей к электронной коммерции. В целом, 28% пользователей Интернет считают, что основным способом снижения риска является совершение коммерческих операций на известных сайтах, а 22% предпочли бы купить понравившийся товар в оффлайновом магазине.

В 2003 году случаи мошенничества с кредитными/дебетовыми картами составят 14% от общего числа электронных транзакций. Безопасность электронных платежей с использованием кредитных карт стала основным барьером в развитии онлайновых покупок для 79% пользователей, 73% потребителей обеспокоены небезопасностью интернет-торговли, а 83% не решаются проводить онлайновые транзакции. Усложнение процесса аутентификации электронных расчетов, сомнения по поводу доставки и ее высокая стоимость заставляют многих потенциальных покупателей закрывать страницы с бланками заказа.

По мнению аналитиков, электронный бизнес не получит достаточного развития до тех пор, пока Интернет-продавцы не предоставят своим клиентам безопасные каналы для проведения платежных операций. Английское агентство по оценке кредитоспособности Experian провело исследование, которое показало, что 57% из 800 компаний, занимающихся коммерческой деятельностью в Интернет, не сообщают властям о случаях финансового мошенничества, а половина из них считают, что полиция вообще не интересуется такими ситуациями. До судебного разбирательства доходит лишь в 9% случаев, и таким образом 9 из 10 онлайновых преступлений остаются не только безнаказанными, но и незамеченными. 20% Интернет-продавцов заявляют, что незаконные операции составляют 1% от общего объема продаж, в то время как некоторые называют цифру в 10%. Почти половина всех респондентов заявила, что они не могут быть до конца уверены в том, что их клиент действительно является тем, за кого он себя выдает, и лишь 15% компаний используют в своей деятельности автоматические системы, проверяющие подлинность карты. По мнению компании EuroDebit, основной проблемой, с которой сегодня столкнулась электронная коммерция, является безопасность платежей. И ситуация, в которой пользователи хотят совершать покупки, но опасаются мошенничества со стороны продавца, будет продолжаться, пока доверие к системам электронных расчетов не вырастет [11].

Выводы

Проведенные исследования показали, что на сегодняшний день применяемые протоколы защиты информации не обеспечивают безопасность банковских транзакций в ИПС, в первую очередь, не обеспечивается выполнение современных возросших требований по аутентичности и целостности банковской информации. Недооценка проблем, связанных с безопасностью информации в ИПС, может привести к огромным финансовым потерям. Отсутствие стандартизированных протоколов обеспечения информационной безопасности ИПС, эксплуатация в практике однотипных массовых программно-технических средств (например, IBM-совместимые персональные компьютеры, операционные системы — Windows, Unix, MS DOS, Netware и т.д.) создает в определенной мере благоприятные условия для злоумышленников. Таким образом, разработка перспективных механизмов обеспечения безопасности банковской информации является актуальной задачей.

Литература

1. В. Столлингс Криптография и защита сетей: принципы и практика, 2-е изд. : пер. с англ. – М.: издательский дом «Вильям», 2001. – 672 с.
2. Євсеєв С.П., Чевардин В.Е., Радковский С.А. Механизмы обеспечения аутентичности банковских данных во внутриплатежных системах коммерческого банка. / Збірник наукових статей ХНЕУ. – Харків: ХНЕУ. – 2008. – Вип. 6. – С. 40-44.
3. Кузнецов А.А., Король О.Г., Ткачев А.М. Анализ механизмов обеспечения безопасности банковской информации во внутриплатежных системах коммерческого банка / Збірник наукових статей "Управління розвитком", ХНЕУ. № 6 – Х.: 2008. – С. 28 – 35.
4. http://www.cryptopro.ru
5. http://e-signature.com.ua
6. http://www.ict.com.ua
7. http://www.vano-zhuk.narod.ru
8. http://bezpeka.ladimir.kiev.ua
9. http://www.infocity.kiev.ua
10. http://www.i2.ru
11. http://www.paycash.ru