Министерство образования и науки Украины

Севастопольский национальный технический университет

Контрольная робота

по теме:

**«Электронные платежные системы в Интернет и их особенности»**

Выполнил: ст. гр. МО-52з

Еловенкова Е.С.

г. Севастополь

2010 г.

**Электронные платежные средства**

Платежная система в Интернете - это система проведения расчетов между финансовыми, коммерческими организациями и пользователями Интернета в процессе покупки/ продажи товаров и услуг через Интернет. В системе электронной коммерции платежи совершаются при соблюдении ряда условий:

соблюдение конфиденциальности;

сохранение целостности информации;

покупатели и продавцы должны быть уверены, что все стороны, участвующие в сделке, являются теми, за кого они себя выдают. Процесс удостоверения сторон называют аутентификацией;

возможность оплаты любыми доступными покупателю платежными средствами;

наличие средств у покупателя (авторизация);

гарантии рисков продавца. Осуществляя торговлю в Интернете, продавец подвержен множеству рисков, связанных С отказами от товара и недобросовестностью покупателя. Величина рисков должна быть согласована с поставщиком услуг платежной системы и другими организациями, включенными в торговые цепочки, посредством специальных соглашений;

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.

Лидирующее положение среди существующих платежных систем занимают системы на основе пластиковых карт и прежде всего кредитных карт. Большинство транзакций в Интернете совершаются с использованием именно этого вида платежа.

Пластиковая карта - это персонифицированный платежный инструмент, предоставляющий возможность безналичной оплаты товаров, и услуг, а также получения наличных средств в отделениях банков и банкоматах. Одна из основных функций пластиковой карты - обеспечение идентификации Использующего ее лица как субъекта платежной системы.

На сегодняшний день наиболее распространенными является карты с магнитной полосой, которая располагается на обратной стороне и, согласно стандарту ISO 7811, состоит из трех дорожек: первые две предназначены для хранения идентификационных данных, на третью можно записывать информацию (например, текущее значение лимита дебетовой карты). Однако из-за невысокой надежности многократно повторяемого процесса записи/считывания запись на магнитную полосу, как правило, не практикуется, и такие карты используются только в режиме считывания информации.

Гарантом выполнения платежных обязательств, возникающих в процессе обслуживания пластиковых карт, является выпустивший их банк-эмитент. Поэтому карты на протяжении всего срока действия остаются собственностью банка, а клиенты - держатели карт - получают их лишь в пользование. Характер гарантий банка-эмитента зависит от платежных полномочий, предоставляемых клиенту и фиксируемых классом карты. При выдаче карты клиенту осуществляется ее персонализация - на нее заносятся данные, позволяющие идентифицировать карту и ее держателя, а также осуществить проверку платежеспособности карты при приеме ее к оплате или выдаче наличных денег. Процесс утверждения продажи или выдачи наличных по карте называется авторизацией. Для ее проведения точка обслуживания делает запрос платежной системе о подтверждении полномочий предъявителя карты и его финансовых возможностей. Наиболее распространена автоматическая авторизация, когда карта помещается в POS-терминал (POS - Point Of Sale), данные считываются с карты, кассиром вводится сумма платежа, а держателем карты со специальной клавиатуры -секретный ПИН-код (ПИН - персональный идентификационный номер). После этого терминал осуществляет авторизацию либо устанавливая связь с базой данных платежной системы (авторизация в режиме подключения), либо осуществляя дополнительный обмен данными с самой картой (авторизация в автономном режиме). В случае выдачи наличных денег процедура носит аналогичный характер с той лишь особенностью, что деньги выдаются специальным устройством - банкоматом, который и проводит авторизацию.

Банк-эмитент, как правило, не занимается деятельностью, обеспечивающей прием пластиковых карт предприятиями торговли и сферы услуг. Эти задачи решает банк-эквайер, осуществляющий весь спектр операций по взаимодействию с точками обслуживания карт: обработку запросов на авторизацию; перечисление на расчетные счета точек средств за товары и услуги, предоставленных по картам; прием, сортировку и пересылку документов (бумажных и электронных), фиксирующих совершение сделок с использованием карт; распространение стоп-листов (перечней карт, операции по которым по тем или иным причинам приостановлены) и др.

Кроме того, банк-эквайер может осуществлять выдачу наличных по картам как в своих отделениях, так и через принадлежащие ему банкоматы. Банк может совмещать функции эквайера и эмитента. Следует отметить, что основными, неотъемлемыми функциями банка-эквайера являются финансовые функции, связанные с выполнением расчетов и платежей точкам обслуживания. Что же касается перечисленных выше технических атрибутов его деятельности, то они могут быть делегированы эквайером специализированным сервисным организациям - процессинговым центрам.

Использование кредитных карт для проведения платежей через Интернет связано с определенными техническими недостатками. Сделки, относящиеся в международной классификации к типу mail order/telephone order (mo/to), были достаточно распространены еще в предшествующие Интернету времена в странах с развитыми карточными платежными системами, но в силу специфики товаров, выставляемых на продажу в Интернете, оказались слабозащищенными от мошенничества, будучи просто перенесенными в Интернет. При оформлении сделок mo/to с получением номера карты вне Мнтернета у продавца всегда есть возможность провести аутентификацию (определение личности) клиента при доставке товара. Правила торговли по картам предполагают обязательную аутентификацию покупателя как держателя предъявленной карты, будь то платеж в магазине с прокатыванием карты, когда кассир удостоверяется в том, что берет оплату именно с держателя карты, или доставка товара по заказу, сделанному по телефону, когда служба доставки несет ответственность за доставку товара именно заказчику в полной мере соблюдение этих правил в Интернете невозможно.

Частичным решением указанных проблем может быть использование протоколов (программы) шифрования SSL и SET, который является сегодня наиболее защищенным, но в силу различных причин еще не получил достаточного распространения.

Еще одним из ограничений использования пластиковых карт является ограничение на нижний предел производимых покупок, составляющий около 3~5 долл. Так как за проведение каждой транзакции эмитент карты берет порядка 1,5-3% от суммы транзакции, но не менее 20 центов, то производить оплату товаров в нижнем ценовом диапазоне становится невыгодно.

Попытки кардинально устранить недостатки платежных систем в Интернете на основе кредитных карт привели к разработке альтернативных видов платежных систем - так называемых дебетовых систем, наиболее широкое распространение среди которых получили сегодня "электронные деньги". Дебетовые схемы платежей в Интернете построены аналогично их традиционным прототипам: чековым и обычным денежным схемам. В схему вовлечены две независимые стороны - эмитенты и пользователи. Под эмитентом понимается субъект, управляющий платежной системой. Он эмитирует электронные денежные единицы. Пользователи систем выполняют две главные функции: производят и принимают платежи через Интернет, используя выпущенные электронные единицы.

1. Электронные чеки - являются аналогом обычных бумажных чеков. Чек является предписанием плательщика своему банку перечислить деньги со своего счета на счет предъявителя чека. Отличие состоит лишь в том, что электронный чек имеет цифровую форму и подписывается не собственноручной подписью плательщика, а его электронной подписью. В остальном суть остается той же. В общем случае система, оперирующая электронными чеками, имеет три субъекта: чекодатель, плательщик по чеку (эмитент), получатель (предъявитель чека). Чекодатель выписывает электронный чек, передает его получателю, а тот уже предъявляет чек эмитенту (например, банку). Эмитент, проверив чек, осуществляет перевод со счета чекодателя на счет получателя.

Оборот чеков организован в российской платежной системе WebMoney Чекодатель (ООО "BMP"), имея счет в банке, эмитирует электронные чеки (далее - ЭЧ). Уполномоченный агент (ООО "Гарантийное Агентство") выполняет работу, связанную с вводом-выводом чеков. Чеки приобретаются пользователями у уполномоченного агента за деньги или могут быть получены от любого другого пользователя в момент перевода внутри системы. При этом, для того чтобы иметь возможность вводить или выводить чеки через уполномоченного агента, пользователь должен акцептовать "Договор продажи ценных бумаг". Это называется "авторизовать R-кошелек". Данное действие доступно, как и раньше, на сайте WM-банкинга. С неавторизованных кошельков можно вести расчеты (отправлять и получать переводы) внутри системы WebMoney, но ввод или вывод осуществлять нельзя.

Приобретая у уполномоченного агента электронные чеки чекодателя, пользователь пополняет свой R-кошелек. При переводе чеков другому участнику системы ему передается право собственности на принадлежащие электронные чеки. Аналогично, уполномоченный агент производит выкуп чеков, принадлежащих пользователям. Это операция вывода чеков из системы, которые погашаются банком чекодателя ("ГРАДОбанком"), и соответствующая сумма переводится на счет получателя в "ГРАДОбанке" или в любом другом банке. При этом ООО "BMP" как чекодатель гарантирует перед пользователем надлежащее и своевременное погашение. Эти гарантии закрепляются "Соглашением об использовании чеков в электронной форме". Данный документ акцептуется пользователем в момент создания R-кошелька.

2. Электронные деньги - полностью моделируют реальные деньги. При этом эмиссионная организация - эмитент - выпускает их электронные аналоги, называемые в разных системах по-разному. Далее они покупаются пользователями, которые с их помощью оплачивают покупки, а затем продавец погашает их у эмитента. При эмиссии каждая денежная единица заверяется электронной подписью, которая проверяется выпускающей структурой перед погашением. Электронные деньги представляют собой электронные денежные обязательства выпустившей их стороны и с юридической точки зрения не являются настоящими деньгами. Применяющийся же термин "деньги" показывает, что электронные деньги в значительной степени наследуют свойства реальных наличных денег. Некоторые системы позволяют получать электронную наличность анонимно, чтобы нельзя было определить связь между покупателем и деньгами. Это осуществляется с помощью метода слепой подписи. Стоит еще отметить, что при использовании электронных денег отпадает необходимость в аутентификации, поскольку система основана на выпуске денег в обращение.

Однако до сих пор не выработана единая система конвертирования разных видов электронных денег. Поэтому только сами эмитенты могут гасить выпущенную ими электронную наличность. С другой стороны, наличные электронные деньги могут не только обеспечить необходимый уровень конфиденциальности и анонимности, но и не требуют связи с центром для подтверждения оплаты. В связи с этим стоимость транзакции сводится к минимуму, и такие системы могут быть эффективно использованы для обеспечения микроплатежей - платежей менее одного доллара, где традиционные системы на основе кредитных карт экономически невыгодны. По общему мнению, именно микроплатежи могут обеспечить основной оборот продаж информации в Интернете.

Среди компаний, развивающих системы цифровых наличных, можно назвать NetCash, Citibank, DigiCash, Mondex, в России - WebMoney и PayCash.

Система Cash фирмы DigiCash предназначена для представления денежных купюр различного достоинства в цифровой форме. В этом виде электронная монета (как последовательность цифр) может быть послана по Интернету, продиктована по телефону, послана по факсу или в письме. Цифровая монета в виде последовательности данных может сохраняться пользователем на жестком диске своего компьютера и передаваться по Сети или электронной почте. Продавец, получив через Интернет цифровую монету, предъявляет ее в банк для авторизации. После авторизации соответствующая цифровой монете сумма заносится на расчетный счет продавца.

3. Электронные деньги на базе смарт-карт. Смарт-карты (Smart Card) - пластиковые карты со встроенным микропроцессором, по виду похожие на обычные кредитные карты. Смарт-карта, по своей сути, представляет собой микрокомпьютер и содержит все соответствующие основные аппаратные компоненты: центральный процессор, оперативную и постоянную память.

Часть информации, записанной на карте, может быть доступна только внутренним программам, что вместе со встроенными криптографическими средствами делает микропроцессорную карту высокозащищенным инструментом, который может быть использован в финансовых приложениях, предъявляющих повышенные требования к защите информации. Смарт-карты рассматриваются в настоящее время как наиболее перспективный вид пластиковых карт. Их вычислительные возможности позволяют использовать, например, одну и ту же карту в операциях с авторизацией в режиме подключения и как электронный кошелек. Широкое внедрение в системах VISA и Europay/MasterCard в течение десятилетия позволит полностью вытеснить карты с магнитной полосой. Самым крупным проектом внедрения смарт-карт в России является проект Сбербанка России - сберкарт. Эта система предлагает использовать смарт-карты как для традиционных расчетов, так и для расчетов через Интернет с помощью специального устройства - считывателя карт, подключаемого к компьютеру через USB или СОМ-порт. Основными барьерами на пути широкого распространения смарт-карт в качестве платежного инструмента в Интернете сегодня является достаточно низкое их распространение по сравнению с обыкновенными магнитными картами, а также то, что для их применения в качестве инструмента оплаты через Интернет требуется наличие периферийного устройства для персонального компьютера.

**Обзор платежных систем, наиболее распространенных в Украине**

С помощью электронной валюты возможно, к примеру, скупиться в электронном интернет - магазине, пополнить счет у мобильного оператора или за спутниковый интернет, переводить деньги в США или получить на свой электронный кошелек гонорар за удаленную работу, не отрываясь от компьютера и не выстаивая длинные очереди в банках. С компьютера возможно оплачивать коммунальные услуги, внести абонплату за кабельное телевидение и еще много чего другого.

Электронные интернет - деньги - это очередной промежуточный этап на пути совершенствования платежных средств, уже прошедших внушительный путь от натурального обмена и бизоновых шкур до бумажных банкнот и пластиковых карт. Электронные валюты настолько динамично развиваются, что большинство банков уже включили в длинный перечень своих услуг и операции с электронными интернет - валютами.

Для использования виртуальных деньг, как правило, применяются «электронные кошельки», которые нужно рассматривать в качестве аналога обычных денег или банковского счета. Работа такого кошелька, как правило, требует установки на компьютер специального программного обеспечения.

В большинстве случаев, операции с электронными деньгами осуществляются через сайты электронных платежных систем, каждый из которых имеет собственную электронную валютную единицу, свои правила обслуживания и комиссионные. Количество существующих электронных виртуальных валют на данный момент подсчитать практически не возможно. Для заработка в интернете вполне достаточно выбрать для себя две - три платежные системы и пользоваться только их услугами. На крайний случай, всегда есть возможность обменять валюту одной платежной системы на валюту другой и наше время это так же просто, как в обычном «обменнике» купить евро за гривны или доллары за рубли. Сайты, расположенные в зоне "ua" и подключенные к торговым системам, принимают к оплате виртуальные деньги с помощью платежных систем WebMoney, iMoney, UkrMoney и E-Gold. Электронные деньги этих платежных систем являются в настоящее время самыми распространенными в Украине.

Самой популярной платежной системой в Украине является российская система WebMoney, организованная в ноябре 1998 года. Кроме долларовых, евровых и рублевых кошельков, украинцам будет доступен еще и «родной» вариант - в гривнах. Интересы WebMoney в Украине представляет «Украинское гарантийное агентство», которое является гарантом системы по платежам в WM (в валюте WMU - электронный эквивалент гривны). При регистрации система предлагает пройти процедуру аттестации и получить персональный сертификат, благодаря которому любой участник платежной системы WM сможет просмотреть доступную информацию о предполагаемом партнере по сделке в WebMoney. Любой сертифицированный участник системы характеризуется показателем business level - рейтингом уровня деловой активности, что в некотором роде показывает степень доверия системы WM к этому партнеру. Это очень полезная информация, особенно, когда вы новичок и еще «не освоились» в платежной системе WebMoney и опасаетесь недобросовестных партнеров по сделкам.

Украинская платежная система Интернет.Деньги (iMoney) основана на технологии PayCash, как и российская система Яндекс.Деньг. Ее участником может стать только житель Украины, предоставив системе основную информацию о себе - Ф.И.О., паспортные данные. Только в этом случае вновь открытый счет является «счетом с достаточной идентификацией пользователя». Обладателю такого счета доступны абсолютно все возможности системы iMoney. Эта платежная интернет система является очень гибким инструментом, так как предлагает наличие сразу нескольких тарифных пакетов, в зависимости от направлений пользователя в работе с электронными платежами. iMoney не принимает банковские переводы из-за рубежа и не выводит деньги на счета в иностранных банках. Для этих операций необходимо воспользоваться интернет - обменниками (например, ROBOXchange) и провести платеж в национальной валюте страны-получателя. Несомненно, вышеуказанные ограничения для участников системы не позволяют iMoney развиваться столь же быстро и динамично, как платежной системе UkrMoney.

Платежная интернет - система UkrMoney родилась в мае 2006 года, однако очень быстро развивается - уже в настоящий момент ее поддерживают 222 украинских интернет - магазина и эта цифра продолжает стремительно расти, а ведь еще три месяца назад их было всего 156. В отличие от платежной системы iMoney, UkrMoney позволяет производить регистрацию нерезидентам Украины. И еще одно несомненное достоинство этой системы - в ней допускаются анонимные счета. Но есть и минусы - общий баланс на таком счете не должен превышать 1000 гривен - до предоставления паспортных данных. Начальная регистрация абсолютно бесплатна. Системой открываются для пользователя три счета - гривневый, в долларах и евро. Но разрешено иметь любое количество счетов, заплатив по 1 гривне за каждый дополнительно открытый счет. Таким образом, можно «обойти» ограничение на размер средств на счету, создав вместо одного несколько счетов. Все аккаунты в UkrMoney, как заявляют владельцы этой платежной системы, обеспечены реальными счетами в Украинском коммерческом банке «ПриватБанк», стратегическом партнере UkrMoney.

Ресурс E-Gold.com, взявший старт в 1996 году в США, доступен для любого жителя Украины по причине своей анонимности. В этой мировой платежной системе открывают аккаунт вне зависимости от страны вашего проживания. Единственная проблема - невозможно на прямую, за гривны, приобрести доллары E-Gold, решается благодаря существованию в интернете многочисленных пунктов обмена интернет - валют. Денежные средства клиентов E-Gold вложены в драгоценные металлы (в основном - в золото), поэтому остаток на счете колеблется в зависимости от состояния цен на драгметаллы на мировых валютных рынках. «Хитрость» здесь еще и в том, что хранение денежных средств в E-Gold рассматривается как инвестиция в драгоценные металлы (не секрет, что цены на драгметаллы в последние годы стабильно растут). Анонимность счетов и финансовых операций уже не раз играла против компании, когда в начале 2007 года было начато судебное преследование правительства США владельцев компании E-Gold относительно участия ее клиентов в отмывании «грязных денег». Несмотря на то, что вина компании так и не была доказана, акции E-Gold серьезно упали в момент обнародования этой информации (хотя сейчас все приходит в «норму»). Размер комиссионного сбора за обналичку или конвертацию E-Gold в другие электронные валюты вырос в несколько раз, но сейчас начинает постепенно снижаться.

Однако платежная интернет - система E-Gold все же очень актуальна для украинцев, желающих заработать в иностранных партнерских программах. Это связанно с малодоступностью других зарубежных электронных платежных систем, в частности PayPal и Moneybookers, хотя компания PayPal с 2006 года начала принимать платежи от жителей Украины и России. Правда, работает PayPal несколько «однобоко» - послать платеж другим участникам системы PayPal вы можете, а вот они вам - нет. (А вот платежная система Moneybookers вообще включила Украину в «черный список» - не на должном уровне организована борьба с электронным мошенничеством, поэтому клиентов из Украины в настоящее время Moneybookers не обслуживает и не понятно, когда будет обслуживать). Но это уже не так! Подробности в статье Платежная система Moneybookers отменила санкции против Украины.

Активный серфер Интернета имеет счета в нескольких платежных системах - никаких ограничений нет. Также допускается наличие любого количества электронных «кошельков» в одной платежной системе. Благодаря существованию системы интернет - обменников, можно практически мгновенно переводить деньги из одной системы в другую. Обменные сервисы для электронных валют работают примерно таким же образом, как и «наземные» пункты обмена реальных валют. За каждую такую операцию обменник взимает небольшой процент с ее объема - свои «комиссионные». Вся процедура происходит в окне браузера, так что устанавливать программное обеспечение нужды нет. На мой взгляд, наиболее популярный в сети обменный сервис - ROBOXchange и GalaExchange (хотя у каждого могут быть свои предпочтения). Замечу, что не стоит гнаться за самым низким процентом - с высокой вероятностью вы просто наткнетесь на обман. Лучше заплатить лишний доллар, чем вообще лишиться всех своих средств.

По оценкам экспертов, доля электронного мошенничества составляет 1-2% от объема всех операций. Некоторая часть относится к категории «психологических вирусов», когда вас с помощью обмана добровольно «вынуждают» расстаться с деньгами. Но в большинстве случаев основатели платежных систем успешно противодействуют электронному «лохотрону». В целях безопасности используются сложные и различные пароли как для входа в платежную систему и просмотра ваших отчетов, так и для осуществления платежей. Например, система интернет банка «Приват24» использует для этих целей мобильный телефон, пароль от вашего аккаунта вы получаете в виде SMS. Для шифрования данных применяются специальные криптографические протоколы и алгоритмы. В настройках аккаунта можно ограничить вход в систему только с назначенных вами IP-адресов. От автоматического подбора паролей или их перехвата на сайтах-близнецах платежных систем клиенты должны ввести случайно сгенерированный проверочный номер и присланный на ваш Email специальный пин - код, например, как в системе E-Gold. Кроме выше перечисленных мер, каждая платежная система имеет в своем арсенале и другие средства электронной защиты.

Ввод в платежную систему реальных денег осуществляется несколькими способами - конвертация средств из другой системы, оплата ваучером (чаще всего пластиковой предоплаченной картой), внесение наличных через отделение банка, оплата кредитной картой или sms - кой, через мобильный телефон. Вывести электронные деньги можно путем опять же конвертации, перевода средств на кредитную карту, через банковский перевод, получения на-личных в кассе оператора системы. Преимущества и недостатки того или иного способа ввода-вывода напрямую зависят от суммы, условий конфиденциальности счета, размера комиссии и степени комфортности для пользователя.

Низкая стоимость платежей делает привлекательным применение электронных валют для выполнения микроплатежей, где обычные безналичные расчеты малоприменимы. Сравните, к примеру, тарифы на перевод денег «Укрпочтой» (комиссия 1,5-4,5%), банковским переводом (комиссия 1,5-7%) с тарифами на обналичивание электронных денег (комиссия 2-3%). И еще одно неоспоримое преимущество - анонимность (для транзакции не нужно идти в банк, заполнять бланки, теряя при этом свои документы и т. д.). И последнее - операции в режиме он-лайн в большинстве случаев происходят в течение нескольких минут, экономя ваше время. С другой стороны, основной минус - это довольно ограниченная сфера использования электронных денег.

Не забывайте, что электронные платежи слабее защищены от мошенничества, чем при стандартных безналичных платежах. Кроме того, перемещение электронных денег гарантируется лишь самой платежной системой, государство не дает никаких гарантий на ваши взаиморасчеты. Хотя в нашей стране государство вообще не дает ни каких гарантий, ни на что! Какие гарантии от разорения имеют у нас вкладчики «наземных» банков? Исходя из вышесказанного - электронные деньги не стоит использовать для крупных платежей или как средство накопления. Но что касается микроплатежей, то более удобной формы их осуществления не существует.

Время электронных денег наступит тогда, когда в Украине, да и не только, а вообще в странах СНГ получат широкое распространение электронные интернет - магазины и сервисы, когда они станут серьезными конкурентами крупным оф-лайновым торговым сетям. Это время не за горами, свое слово должен сказать потребитель, который «ищет там, где дешевле». Наступит время, когда увеличение количества пользователей и борьба за клиента между существующими системами приведут к существенному снижению тарифов и электронные платежи станут для нас таким же обыденным делом, как и езда на автомобиле!

**Сравнение платежных систем, доступных для жителей Украины.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Сравнение | WebMoney | UkrMoney | iMoney | E-Gold |
| Открытие счета | Бесплатно | Бесплатно | 5 грн | Бесплатно |
| Первоначальный взнос | Бесплатно | Бесплатно | 0,01-100 грн\* | Бесплатно |
| Неснижаемый остаток | Бесплатно | Бесплатно | 10 грн | Бесплатно |
| Комиссия на транзакции внутри системы  | 0,8%, но не менее $0,01 | 0,7%, но не менее $0,03 | 0,5% - входящие, 0% - исходящие | 1%, но не менее $0,5 |
| Комиссия на ввод средств в систему | 0% | 0% | 0% | 0% |
| Комиссия на вывод средств из системы | 0,8%, но не более $50 | 1% (с помощью Maestro) | 1%\* | 1%, но не более $0,5 |
| Количество счетов с 1 аккаунта | 4 | Неограниченн о | До 100 | 4 |
| Открытие счета в гривне | Да | Да | Да | Нет |
| Анонимные счета | Нет, персонализация счета обязательна | Макс. до 1000 грн (или эквивалент) | Нет | Да |
| Номинал ваучеров\*\* | 50,100,200 | 10,30,50,100 (электронные) | 50,100,200, | Номинал ваучеров\*\* |
| Интернет - карты | Нет | Maestro, Visa | Нет | Нет |
| Украинские банки-партнеры | «ПриватБанк», «УкрПромБанк» | «ПриватБанк» «Надра», | «VAB Банк» | Нет |

\* В зависимости от тарифного пакета.

\*\* Без учета комиссии торговых агентов (иногда доходит до 8-10%).

**Безопасность платежей в Интернете**

Функционирование платежных систем в Интернете возможно только при обеспечении условий безопасности. Понятие "безопасность информации" можно определить как состояние устойчивости информации к случайным или преднамеренным воздействиям, исключающее недопустимые риски ее уничтожения, искажения и раскрытия, которые приводят к материальному ущербу владельца или пользователя информации. Решение проблемы безопасности основывается на криптографических или шифровальных системах, обеспечивающих:

конфиденциальность - информация должна быть защищена от несанкционированного доступа как при хранении, так и при передаче. Доступ к информации может получить только тот, для кого она предназначена. Обеспечивается шифрованием;

аутентификацию - необходимо однозначно идентифицировать отправителя, при однозначной идентификации отправитель не может отказаться от послания. Обеспечивается электронной цифровой подписью и сертификатом;

целостность - информация должна быть защищена от несанкционированной модификации как при хранении, так и при передаче. Обеспечивается электронной цифровой подписью.

Любая система шифрования работает по определенной методологии, которая включает один или несколько алгоритмов шифрования (математических формул), ключей, используемых этими алгоритмами, а также системы управления ключами. Наиболее распространены алгоритмы, объединяющие ключ с текстом. Основная проблема шифрования состоит в безопасной процедуре генерации и передаче ключей участникам взаимодействия.

На практике существуют два основных типа криптографических алгоритмов: классические, или симметричные, алгоритмы, основанные на использовании закрытых, секретных ключей, когда и шифрование, и дешифрирование производятся с помощью одного и того же ключа; ассиметричные - алгоритмы с открытым ключом, в которых используются один открытый и один закрытый ключ.

Алгоритмы симметричного шифрования используют ключи не очень большой длины и могут быстро шифровать большие объемы данных. Порядок использования систем с симметричными ключами выглядит следующим образом.

Безопасно создается, распространяется и сохраняется симметричный секретный ключ. Отправитель использует симметричный алгоритм шифрования вместе с секретным симметричным ключом для получения зашифрованного текста. Отправитель передает зашифрованный текст. Симметричный секретный ключ никогда не передается по незащищенным каналам связи. Для восстановления исходного текста получатель применяет к зашифрованному тексту тот же самый симметричный алгоритм шифрования вместе с тем же самым симметричным ключом, который уже есть у получателя.

Характеристики симметричных шифров регламентируются стандартами: ГОСТ № 28147-89 РФ, DES (Data Encryption Standard) США и др.

Суть асимметричных криптосистем состоит в том, что каждым адресатом генерируются два ключа, связанные между собой по определенному правилу. Хотя каждый из пары ключей подходит как для шифрования, так и для дешифрирования, данные, зашифрованные одним ключом, могут быть расшифрованы только другим ключом.

Криптографические системы с открытым ключом используют так называемые необратимые, или односторонние, функции. Понятие односторонней функции было введено в теоретическом исследовании о защите входа в вычислительные системы. Функция f(x) называется односторонней (one-way function), если для всех значений х из ее области определения легко вычислить значения у = fix), но вычисление обратного значения практически не осуществимо. Известно несколько криптосистем с открытым ключом. Наиболее разработана на сегодня система RSA, предложенная еще в 1978 г. Этот алгоритм стал мировым стандартом де-факто для открытых систем и рекомендован МККТТ (Международный консультативный комитет по телефонии и телеграфии).

Шифрование передаваемых через Интернет данных позволяет защитить их от посторонних лиц. Однако для полной безопасности должна быть уверенность в том, что второй участник транзакции является тем лицом, за которое он себя выдает. В бизнесе наиболее важным идентификатором личности заказчика является его подпись. В электронной коммерции применяется электронный эквивалент традиционной подписи - цифровая подпись (в России закон о цифровой подписи принят в январе 2003 г.). С ее помощью можно доказать не только то, что транзакция была инициирована определенным источником, но и то, что информация не была испорчена во время передачи. Как и в шифровании, технология электронной подписи использует либо секретный ключ (в этом случае оба участника сделки применяют один и тот же ключ), либо открытый ключ (при этом требуется пара ключей - открытый и личный). И в данном случае более простые в использовании методы с открытым ключом (такие как RSA) более популярны.

Основной проблемой криптографических систем является распространение ключей. Асимметричные методы более приспособлены для открытой архитектуры Интернета, однако и здесь использование открытых ключей требует их дополнительной защиты и идентификации для определения связи с секретным ключом. Без такой дополнительной защиты злоумышленник может выдать себя за отправителя подписанных данных или за получателя зашифрованных данных, заменив значение открытого ключа или нарушив его идентификацию. В этом случае каждый может выдать себя за другое лицо. Все это приводит к необходимости верификации открытого ключа. Для этих целей используются электронные сертификаты.

Электронный сертификат представляет собой цифровой документ, который связывает открытый ключ с определенным пользователем или приложением. Для заверения электронного сертификата используется электронная цифровая подпись доверенного центра - Центра сертификации (ЦС). Исходя из функций, которые выполняет ЦС, он является основным компонентом всей инфраструктуры открытых ключей (ИОК или PKI - Public Key Infrastructure). Используя открытый ключ ЦС, каждый пользователь может проверить достоверность электронного сертификата, выпущенного ЦС, и воспользоваться его содержимым. Для того чтобы сертификатам можно было доверять, независимая организация, выполняющая функции ЦС и являющаяся источником сертификатов, должна быть достаточно авторитетной.

Технология цифровых сертификатов работает следующим образом. Чтобы воспользоваться сертификатом, потенциальный покупатель должен прежде всего получить этот сертификат у надежного источника сертификатов. Для этого ему необходимо каким-то образом доказать подлинность своей личности, возможно, явившись в эту организацию и предъявив соответствующий документ, а также передать источнику сертификатов копию своего открытого ключа. Когда после этого он захочет что-либо купить через Интернет, ему будет достаточно добавить к заказу свою электронную подпись и копию сертификата. Отдел обслуживания покупателей фирмы, в которой он совершил покупку, проверяет сертификат, чтобы убедиться, что к заказу приложен подлинный открытый ключ, а также выясняет, не аннулирован ли сертификат.

Гарантами безопасности платежных систем являются стандарты безопасности. Наиболее распространенными стандартами безопасности виртуальных платежей являются протокол SSL (Secure Socket Layer), обеспечивающий шифрование передаваемых через Интернет данных и стандарт SET (Secure Electronic Transactions), разработанный компаниями Visa и MasterCard и обеспечивающий безопасность и конфиденциальность совершения сделок при помощи пластиковых карт.

Протокол SSL - стандарт, основанный на криптографии с открытыми ключами. Протокол обеспечивает защиту данных, передаваемых в сетях TCP/IP по протоколам приложений за счет шифрования и аутентификации серверов и клиентов. Это означает, что шифруется вся информация, передаваемая и получаемая Web-браузером, включая URL-адреса, все отправляемые сведения (такие как номера кредитных карт), данные для доступа к закрытым Web-сайтам (имя пользователя и пароль), а также все сведения, поступающие с Web-серверов. Три основные функции безопасности, гарантированные в SSL, основаны на криптографии с открытым ключом.

Одной из основных причин медленного роста электронной коммерции является озабоченность покупателей надежностью средств, применяемых при выполнении платежей в Интернете с использованием кредитных карт. Описанный выше протокол SSL позволяет решить часть названных проблем безопасности, однако его роль в основном ограничивается обеспечением шифрования передаваемых данных. Поэтому для комплексного решения перечисленных выше проблем была разработана спецификация и создан набор протоколов, известные как стандарт SET (Secure Electronic Transaction - Безопасные электронные транзакции).

В основе системы безопасности, используемой стандартом SET, лежат стандартные криптографические алгоритмы DES и RSA. Инфраструктура SET построена в соответствии с инфраструктурой открытого ключа (Public Key Infrastructure - PKI) на базе сертификатов, соответствующих стандарту Х.509 организации по стандартизации (ISO). Главная особенность SET - регламентация использования системы безопасности, которая устанавливается международными платежными системами.

Требования Visa и Europay к процессинговому центру на основе SET включают, во-первых, традиционные требования к процессингу пластиковых карт (защита помещений, контроль над доступом, резервное энергоснабжение, аппаратная криптография и т.п.); во-вторых, специфические дополнения - межсетевые экраны (firewalls) для защиты каналов Интернета.

Такой подход позволяет использовать единые методики оценки рисков при проведении электронных платежей вне зависимости от способа аутентификации клиента (традиционная карта с магнитной полосой, смарт-карта или цифровой сертификат). Это позволяет участникам платежной системы разрешать спорные ситуации по отработанным механизмам и сконцентрироваться на развитии своего электронного бизнеса.

Для получения актуальной информации о распространении SET, включая информацию о банках, имеющих сертификаты Visa и Europay/MasterCard, и торговых/сервисных компаниях, принимающих SET-платежи, можно обратиться на сайт set-sites.com или сайты международных платежных систем.

**Список использованной литературы**

1. Веляевский И.К. Маркетинговое исследование: информация, анализ, прогноз. М.: Финансы и статистика, 2006.
2. Головеров Д.В., Кемрадж А.С. и др. Правовые аспекты использования Интернет-технологий. М.: Книжный мир, 2008.
3. Данько Т.П., Дьяконова Л.Я., Завьялова Н.В., Сагинова О.В. и др. Электронный маркетинг: Учеб. пособие. М.: ИНФРА-М, 2007.
4. Раздьяконов Н. и др. Jump In: Учеб. пособие для слушателей курсов "Амадеус". М.; СПб.: Amadeus Russia, 2007.
5. Успенский И. Энциклопедия Интернет-бизнеса. СПб.: Питер, 2006.
6. Холмогоров В. Интернет-маркетинг. Краткий курс. СПб.: Питер, 2008.
7. Хорошилов А.В., Селетков С.Я. Мировые информационные ресурсы. СПб.: Питер, 2004.
8. http://www.marketingpower.com/welcome.php - сайт американской маркетинговой ассоциации (АМА).
9. http://www.ram.ru/ - сайт российской ассоциации маркетинга (РАМ).
10. http://www.e-commerce.ru/ - Интернет-ресурсы информационно-консалтингового центра по электронному бизнесу.
11. http://www.e-management.ru/ - консультационный центр развития электронного бизнеса.