**РЕФЕРАТ**

**по дисциплине «Интернет-маркетинг»**

**по теме «Платежные системы в Интернете»**

**1. 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.

**2. Российские платежные системы**

В российской части Интернета существует ряд платежных систем, практически в полной мере охватывающий круг функций, выполняемых западными платежными системами:

1. CyberPlat (www.cyberplat.ru) - универсальная межбанковская система платежей через Интернет. Система разработана специалистами банка "Платина" (www.platina.ru) и фирмой "Инист" (www.inist.ru). Фактически CyberPlat является одной из первых российских систем, производящих электронные платежи через Интернет в режиме подключения.

Основные свойства системы CyberPlat:

интегрированностъ. Система объединяет различные инструменты для ведения бизнеса в Интернете: CyberCheck - подсистема обслуживания транзакций класса В2В; CyberPOS - подсистема обслуживания транзакций класса В2С для платежей по пластиковым картам международных и российских платежных систем; Inetnet-Banking - подсистема управления счетом в банке-участнике системы через Интернет;

мулътибаиковостъ. Система допускает участие неограниченного количества банков, открыта для взаимодействия с любыми другими платежными системами и обеспечивает поддержку множества процессинговых центров;

универсальность. Система позволяет использовать различные платежные инструменты: пластиковые карты международных и российских платежных систем, в том числе Visa, Europay, Diners Club, JCB, American Express, скретч-карты E-port, а также платежи непосредственно с банковских счетов плательщиков в банках-участниках системы на любой банковский счет.

Assist Система Интернет-платежей Assist (www.assist.ru) позволяет в реальном времени с любого компьютера, подключенного к Интернету, осуществлять авторизацию и проведение платежей, совершаемых при помощи кредитных карт или с лицевых счетов клиентов поставщиков услуг Интернета и другого программного обеспечения, кроме браузера, пользователю устанавливать не требуется. Платежная система Assist впервые была запущена в эксплуатацию компанией "Рексофт" в рамках проекта "Озон" в апреле 1998 г. Полный коммерческий запуск системы состоялся в апреле 1999 г. В 2000 г. Assist подключился к "Альфа-Банку" и банкам, обслуживаемым процессингом "СТБ-Кард". Развитие системы Assist было направлено на расширение числа банков-клиентов системы и предоставление новых услуг. С помощью платежной системы Assist "Альфа-Банк" впервые в России применил технологию SET для проведения платежей через Интернет. При выделении Assist в отдельную компанию в апреле 2002 г. был расширен отдел технической поддержки и создана группа мониторинга транзакций по кредитным картам. Также была создана и отработана специализированная методика дополнительного фрод-мониторинга, предлагаемая Интернет-магазинам. В течение 2002-2003 гг. Assist удалось подключить все пять ведущих российских систем электронной наличности, таких как WebMoney, Яндекс.Деньги, Rapida, e-port и CreditPilot. Таким образом, к стандартному набору кредитных карт (VISA, MasterCard, DINERS CLUB) добавились электронные кошельки, позволяющие решить вопрос микроплатежей.

ЭлИТ-Карт (www.elit.ru/card/) является совместным проектом уже упоминавшейся выше компании "АйТи" и АКБ "Автобанк". "АйТи" выполняет функции технологической компании и обеспечивает интеграцию системы ЭлИТ-Карт с торговыми системами Интернета. "Автобанк" выполняет эквайринговое обслуживание организаций. Система предназначена для проведения через Интернет платежей по пластиковым картам мировых платежных систем, в том числе Visa, MasterCard, EuroCard, American Express, UnionCard и др.

4. Instant (www.paybot.com/defaultrus.asp) разработана компанией "Интерфейс" (www.interface.ru) совместно с американской фирмой PayBot (www.paybot.com). Платежная система предоставляет возможность:

оплачивать в режиме реального времени международными пластиковыми карточками товары или услуги, исключая пересылку данных о пластиковых карточках от клиентов продавцам;

оплачивать в режиме реального времени любые услуги и товары с виртуальных счетов покупателя в платежной системе;

проверять в режиме реального времени продавцу услуг или товаров поступление платежа или наличие транзакции по карточке и отпускать продукт покупателю;

получать продавцу оплату за услуги или товары на счет в его банке без необходимости открытия нового банковского счета;

получать продавцу оплату за услуги или товары на его счет как от клиентов - владельцев виртуальных счетов покупателя в платежной системе, так и от клиентов - держателей международных пластиковых карточек, зарегистрированных в платежной системе;

использовать CyberMall - встроенный электронный магазин для того, чтобы быстро и просто организовать продажу продукта;

благодаря несложному интерфейсу обеспечивать интеграцию платежной системы с любым сторонним программным обеспечением электронной коммерции;

продавцу самостоятельно регистрировать держателей международных пластиковых карт, обеспечивая в дальнейшем безопасное использование карточек для платежей в его адрес;

банкам регистрировать держателей международных пластиковых карт как из числа своих клиентов, так и держателей карт, эмитированных сторонними банками. Это позволяет обеспечивать рост числа операций по пластиковым карточкам, предоставлять клиентам - держателям карточек и клиентам - продавцам услуг и товаров новый вид обслуживания - безопасные операции с пластиковыми карточками в Интернете.

Платежная система базируется на использовании персональных счетов покупателя (Current Account), карт покупателя (Customer Card) и счетов продавца (Merchant Account), доступных только пррг предъявлении идентификатора счета (Account Id) и пароля (Password). Любая компания, желающая продавать через Интернет свои товары или услуги (Интернет-провайдеры, провайдеры сотовой связи, информационные агентства, периодические издания, разработчики программного обеспечения), может воспользоваться данным сервисом для того, чтобы в режиме реального времени получать платежи от своих клиентов и автоматически предоставлять им свои продукты немедленно после оплаты. Каждый продавец Интернет-услуг, других телекоммуникационных услуг либо информационных продуктов может разместить их описание и ссылку (link) для их получения в CyberMall, CyberMall функционирует по принципу DVP (Delivery Versus Payment - поставка против оплаты) - ссылка на продукт предоставляется после его оплаты.

Банки, желающие увеличить объемы операций по пластиковым картам, могут стать регистраторами пластиковых карт в платежной системе.

Для этого подключения покупателя к системе необходимо следующее.

Если предполагается оплата со своего виртуального счета в платежной системе, то необходимо открыть виртуальный счет покупателя в платежной системе (Current Account), обязательно записав при этом идентификатор счета (Account Id) и пароль (Password). Это можно сделать сразу на сайте системы, воспользовавшись функцией "Открыть счет покупателя".

Чтобы пополнить свой виртуальный счет покупателя, покупатель должен послать требуемую сумму на реальный банковский счет финансового оператора (FinOp), которого он выбрал при открытии счета. Банковские реквизиты SYSTEM FinOp приведены на странице сайта "Пополнить ваш счет". Финансовые операторы должны обеспечить покупателей и продавцов необходимой информацией о своих банковских реквизитах. Если ваш банк или провайдер услуг не является Instant FinOp, необходимо выбрать SYSTEM FinOp.

Если предполагается оплата с личной международной пластиковой карточки, необходимо зарегистрировать карточку в платежной системе, обязательно записав при этом идентификатор карты (Card Id) и пароль (Password). Для этого на сайте имеется функция "Регистрация карты". После регистрации необходимо будет подтвердить регистрационные данные, предъявив карточку и паспорт в банке или у продавца, зарегистрированного в платежной системе. Если продавец, услугами которого вы будете пользоваться, согласен принимать неподтвержденные карточки, то подтверждать зарегистрированные карточки не обязательно, но очень желательно. После этого можно оплачивать товары и услуги в режиме реального времени.

Подключение к системе продавца товаров или поставщика услуг организуется следующим образом.

Сначала необходимо открыть виртуальный счет продавца (Merchant Account), воспользовавшись функцией "Открыть счет продавца", обязательно записав при этом идентификатор счета (Account Id) и Пароль (Password). Продавцы получают от финансового оператора (FinOp), выбранного при открытии счета, на свои банковские счета собранные от покупателей средства. Финансовые операторы должны обеспечить покупателей и продавцов необходимой информацией о своих банковских реквизитах. Если банк иди провайдер услуг продавца не является Instant! FinOp, необходимо выбрать SYSTEM FinOp.

Далее, если предполагается прием оплаты как от владельцев счетов, так и от держателей пластиковых карт, необходимо заключить договор с банком-эквайрером, который будет обрабатывать транзакции по пластиковым карточкам. В случае, если уже имеется право приема пластиковых карточек, можно использовать платежную систему для перепроцессинга операций с кредитными карточками, обеспечивая безопасный прием карточек и генерацию транзакций для существующего банка.

Каждый владелец счета покупателя или счета карты может в режиме реального времени:

получать выписки с балансом счета и детальной историей проведенных операций;

переводить деньги на счета продавцов товаров и услуг и на счета покупателей;

переводить деньги со счета покупателя на свой счет в своем банке (например, на счет своей пластиковой карты);

получать услуги и товары немедленно после оплаты через Интернет.

Каждый владелец счета продавца может в режиме реального времени:

получать оплату за услуги или товары без необходимости открытия нового банковского счета как от клиентов - владельцев виртуальных счетов покупателя в платежной системе, так и от клиентов - держателей международных пластиковых карточек, зарегистрированных в платежной системе;

получать выписки с балансом, счета и детальной историей проведенных операций;

получать автоматическую справку о конкретном платеже клиента - это позволяет предоставлять ему товар или услугу немедленно после оплаты - полностью автоматически для информационных товаров или телекоммуникационных услуг;

использовать CyberMall - встроенный электронный магазин для того, чтобы быстро и просто организовать продажу продукта;

использовать простой интерфейс для интеграции платежной системы с любым сторонним программным обеспечением электронной коммерции;

регистрировать держателей международных пластиковых карт, обеспечивая в дальнейшем безопасное использование карточек для платежей в его адрес.

Счет продавца является полностью безопасным - с него невозможно снять деньги через Интернет. Он предназначен только для сбора платежей от клиентов. Перечень продавцов, описание их товаров и услуг, а также функции оплаты и получения товара или услуг представлены на странице "Магазин".

Для визуального подтверждения участника системы продавцы товаров и услуг размещают на своих Web-серверах логотип Instant!

Несмотря на заверения о полной безопасности платежей, разработчики рекомендуют обязательно выполнять правила личной безопасности:

не передавайте ваш пароль другим лицам. Для получения выписки необходимо указать символьный префикс нашего пароля (первые 4 символа). Полный 8-символьный пароль вам необходим только когда вы переводите деньги со своего счета покупателя на счет продавца;

не передавайте ваш полный 10-символьный идентификатор счета другим лицам. Для пополнения вашего счета необходимо указать б-символьный префикс вашего идентификатора счета (первые 6 символов). Полный 10-символьный идентификатор счета вам необходим только тогда, когда вы переводите деньги со своего счета покупателя на счет продавца либо получаете выписку. Шестисимвольный префикс вашего идентификатора счета полностью его идентифицирует;

каждый открытый и остающийся пустым (с нулевым балансом) в течение 30 дней счет покупателя автоматически закрывается. Пожалуйста, держите некоторую сумму на вашем счете покупателя для предотвращения его автоматического закрытия;

после четырех попыток доступа к счету, использующих неправильный пароль, доступ к счету блокируется на 24 ч. Это сделано для предотвращения попыток анализа пароля;

после восьми попыток доступа к счету, использующих неправильный идентификатор счета, доступ для данного удаленного IP-адреса блокируется на 24 ч. Это сделано для предотвращения попыток анализа идентификатора счета. В случае выдачи системой соответствующего сообщения проверьте, не используете ли вы proxy-сервер совместно со многими другими пользователями.

WebMoney Transfer относится к дебетовым системам на основе электронных денег, в качестве которых в системе служат титульные знаки WebMoney, стабильность курса и ликвидность которых обеспечиваются гарантами системы. Учетная система WebMoney Transfer обеспечивает проведение расчетов в реальном времени посредством учетных единиц - титульных знаков WebMoney (WM). Управление движением титульных знаков осуществляется пользователями с помощью клиентской программы WM Keeper.

Системой поддерживается несколько типов титульных знаков, обеспеченных различными активами и хранящихся на соответствующих электронных кошельках:

WMR - эквивалент RUR на R-кошельках;

WME - эквивалент EUR на Е-кошельках;

WMZ - эквивалент USD на Z-кошельках;

WMU - эквивалент UAH на U-кошельках;

WM-C и WM-D - эквивалент WMZ для кредитных операций на С- и D-кошельках.

При переводе средств используются однотипные кошельки, а обмен различных титульных знаков производится в обменных сервисах.

Гарантом по WMR-операциям является ООО "BMP" - компания, представляющая WebMoney Transfer на территории России. Гарантом по WMZ- и WME-операциям выступает компания Amstar Holdings Limited, S.A. Гарантом по WMU-операциям выступает компания ООО "Украинское Гарантийное Агентство" (http://www.guarantor.com.ua).

Для того чтобы стать участником системы WebMoney Transfer, достаточно установить на своем компьютере клиентскую программу WM Keeper и зарегистрироваться в системе, получив при этом WM-идентификатор и приняв соглашения системы. Процесс регистрации также предусматривает ввод персональных данных и подтверждение их достоверности посредством клиентской программы WM Keeper. Эту программу в виде самораспаковывающегося архива, а также учебные пособия по ее применению, можно бесплатно получить на Web-сервере системы.

В системе реализована программа WM-аттестации. Каждый пользователь имеет WM-аттестат - цифровое свидетельство, составленное на основании предоставленных им персональных данных.

С помощью системы WebMoney Transfer пользователи Интернета, находящиеся в любой точке земного шара, могут осуществлять безопасные наличные расчеты в реальном времени: переводить средства другим пользователям, оплачивать товары и услуги в Сети, обсуждать с партнерами условия торговых сделок посредством голосового сервиса, а также защищенной WM-почты.

В системе WebMoney Transfer возможны два типа платежей - обычный и двухфазовый. Обычный платеж рекомендуется для оплаты информации или услуг, т. е. для товара, не требующего физической доставки. Покупатель оплачивает товар. При этом из его кошелька сумма, равная стоимости товара, переводится в кошелек продавца. Затем продавец производит поставку. Двухфазовый платеж рекомендуется для оплаты товаров, требующих физической доставки. В этом случае покупатель переводит деньги продавцу. При этом продавец не может воспользоваться ими до тех пор, пока не выполнит свои обязательства перед покупателем. И если эти обязательства не выполнены по истечении определенного срока (срока протекции сделки), деньги возвращаются в кошелек покупателя.

Получить WM можно следующими способами: у гарантов путем безналичного перевода из любого банка, а также почтовым переводом на расчетный счет гаранта с указанием номера пополняемого кошелька (денежные средства будут автоматически конвертированы в WM и зачислены на указанный при переводе кошелек); через предоплаченную WM-карту (пополнение Z-кошельков); от кого-либо из участников системы в обмен на товары, услуги или лее в обмен на наличные деньги.

С помощью WebMoney Transfer можно совершать покупки в электронных магазинах, создавать собственные магазины, реализующие виртуальные продажи через Интернет, а также производить расчеты с другими участниками системы.

За все операции, связанные с движением электронных денег в систему или из системы, взимается плата в соответствии с действующими тарифами по данным операциям агентов системы. Для Z-кошельков взимается тариф в соответствии с тарифами International Metal Trading Bank (USA). Для R-кошельков взимается тариф в соответствии с тарифами банка, обслуживающего ВМ-Центр.

PayCash (www.paycash.ru) - совместный проект, разрабатываемый банком "Таврический" и группой компаний "Алкор-Холдинг". Система PayCash является средством проведения платежей электронными деньгами через Интернет. Электронные деньги представляют собой "денежные обязательства", хранящиеся на информационном накопителе пользователя и позволяющие владельцу оплачивать услуги и товары и производить денежные переводы через Интернет. Специальная процедура позволяет использовать эти денежные обязательства частями по мере необходимости. Клиент может неоднократно пополнять платежную книжку в банке и выполнять с ее помощью платежи на любую сумму в пределах находящихся на ней средств, не задумываясь о необходимости их размена. Любые изменения состояния платежной книжки делаются только по инициативе владельца и обязательно подтверждаются банком. Неподтвержденные банком изменения через определенное время или по инициативе пользователя отменяются, и на платежной книжке восстанавливается прежняя сумма.

PayCash - единственная российская платежная Интернет-система, основанная на классической технологии цифровой наличности (digital cash), первоначально предложенной Дэвидом Чаумом (David Chaum, система "eCash"). Цифровая наличность - это бессрочные денежные обязательства на предъявителя, эмитированные в форме защищенных цифровых сертификатов, которые могут быть использованы для расчетов через сеть Интернет и обеспечиваются обыкновенными денежными средствами в момент предъявления обязательства его эмитенту.

С теоретической точки зрения существенным недостатком системы Чаума является то, что плательщик и банк вынуждены доверять друг другу. Банк может присвоить предъявленную плательщиком монету, заявляя, что она уже была использована ранее. В свою очередь, мошенник может' предъявлять претензии банку, заявляя, что никакого повторного использования монеты не было, а банк просто хочет украсть ее. Требуется также доверие к продавцу, если монеты передаются ему в открытом виде. Следует отметить, что этот недостаток не является специфическим свойством монет Чаума, но выражает фундаментальное свойство сертификатов на предъявителя. Сертификаты на предъявителя не заключают в себе никакого секрета предъявителя, при помощи которого он мог бы доказывать свои права на сертификат. Таким образом, в системе Чаума возможны конфликты, не разрешимые средствами самой системы. Это приводит к удорожанию платежной системы, так как для обработки таких конфликтов требуются особые организационные меры (страховочные фонды, черные списки и т.п.).

Основной областью применения платежной системы является электронная коммерция. Для того чтобы иметь возможность разрешать конфликты в рамках торговой системы, любая денежная транзакция должна быть привязана к соответствующей товарной транзакции таким образом, чтобы плательщик имел возможность доказывать факт оплаты конкретного товара. Так как в рамках системы Чаума отсутствует внутренняя возможность интегрирования с торговой системой, то это означает, что плательщик, кроме кошелька (клиента платежной системы), должен иметь еще специфического для данной торговой системы покупщика (клиента торговой системы), который будет увязывать денежные транзакции с товарными транзакциями.

Рано или поздно список использованных монет в монетной системе Чаума перестанет помещаться в отведенном для него хранилище. Кроме того, время поиска монет в этом списке растет с ростом списка, хотя и логарифмически. Поэтому, чтобы иметь возможность удерживать размер списка в приемлемых пределах, банк должен ограничивать период оперативной платежеспособности монет. В этом случае использованные монеты, платежеспособный период которых истек, можно удалять из списка. Слишком короткий период оперативной платежеспособности не добавляет платежной системе потребительской привлекательности. Здесь нужно отметить, что скорость роста размера списка использованных монет тем выше, чем шире диапазон и меньше шаг возможных платежей, так как для обеспечения широкого диапазона и малого шага необходимо вводить много номиналов монет. Как следствие, возрастает среднее число монет в одном платеже. Увеличение среднего числа монет в одном платеже пропорционально увеличивает время поиска в списке использованных монет. Постоянный прогресс компьютерной техники постепенно снижает серьезность проблемы большого списка использованных монет. Кроме того, Чаум предложил остроумный способ слепого возврата банком сдачи, что позволяет использовать для платежа всего лишь одну монету.

В системе PayCash клиент расплачивается при помощи данных, которые называются платежной книжкой и отличаются от монеты Чаума тем, что вместо случайного серийного номера используется случайный открытый ключ, а сумма закодирована не с помощью "номинала", а с помощью степени подписывающего отображения. Схема платежей представляет собой систему анонимных счетов с возможностью непрослеживаемого перевода денег (обязательств) с одного счета на другой. Так как виртуальный счет, как правило, обслуживает много платежей, то список виртуальных счетов растет значительно медленнее, чем соответствующий список использованных монет в системе Чаума. Очевидно, что все платежи, проведенные с помощью одной платежной книжки, легко могут быть связаны банком друг с другом через общий виртуальный счет. Это представляет некоторую угрозу для анонимности клиента, так как если один из платежей клиента будет атрибутирован внешними по отношению к системе средствами, то тогда и вся платежная история клиента, связанная с данной платежной книжкой, может быть раскрыта. Для уменьшения этой угрозы клиент может прерывать свою платежную историю, открывая новые платежные книжки и прекращая использовать старые. Кроме того, по истечении срока действия книжки ее платежная история заканчивается. Как часто следует клиенту прерывать свою платежную историю и сколько платежных историй иметь одновременно, зависит от его мнительности и от расценок, установленных банком для различных операций. Высокая стоимость открытия виртуального счета и/или высокая стоимость съема денег на книжку стимулирует среднего пользователя использовать одну и ту же платежную книжку для большего числа платежей, не закрывая полностью возможность для мнительного пользователя ограничивать количество платежей, проведенных с одной книжки. Кроме того, взимание банком платы за открытие виртуального счета защищает его список виртуальных счетов от переполнения, так как каждое место в этом списке оплачивается, а также предоставляет банку дополнительный источник дохода.

Технология слепой подписи, используемая при пополнении платежной книжки, гарантирует лишь несвязываемость счета с книжкой в сеансе пополнения. Однако книжка может быть косвенно связана банком со счетом иными средствами, например по Интернет-адресу их владельца. Банк может также пытаться связать книжку со счетом путем анализа общей суммы денег, переведенных на платежную книжку. Однако этот косвенный способ связывания в значительной степени затруднен тем, что одна и та же платежная книжка может пополняться с разных счетов, и тем, что при платеже владелец платежной книжки не раскрывает банку сразу нею сумму N платежной книжки РауВоок. Кроме того, в платежную систему PayCash встроен модифицированный механизм слепого возврата сдачи Чаума, который может быть использован для реструктуризации сумм на платежных книжках, и в частности для перевода на свежую платежную книжку остатка денег с книжки, предназначенной для удаления, что еще больше уменьшает возможность связывания книжки со счетом. Таким образом, подход, избранный для построения платежной системы PayCash, обеспечивает разумный уровень непрослеживаемости платежей.

Система PayCash предполагает возможность участия в чей неограниченного числа банков, каждый из которых может выпустить собственные электронные деньги, которые могут находиться в одном кошельке, и управление счетами и разных банках будет осуществляться при помощи одного и того же программного обеспечения. Для демонстрационных целей наряду с реально работающим банком в рамках системы PayCash работает демонстрационный банк. Демонстрационный банк оперирует с игрушечными деньгами, которые можно заказать и получить на сайте совершенно бесплатно.

Для работы с игрушечными деньгами необходимо скопировать с сайта http://imoney.com.ua программу Интернет-кошелек и установить в качестве системы демосистему, а в качестве валюты - одну из демонстрационных валют.

При помощи этого банкомата Вы можете быстро зачислить на свои счет в ДемоБанке небольшую сумму игрушечных денег. При этом ДемоБанк удерживает комиссионные в обычном порядке.

Эта страница теряет силу после того, как отослан успешный запрос о зачислении денег, или по истечении 4 минут после ее загрузки или обновления, потому ее следует обновлять по мере необходимости.

Сумма не должна превышать:

300 рубликов 10 доллариков 25 евриков 10 латиков.

В виртуальном банкомате можно положить на открытый счет демовалюту (рублики и долларики). При этом убедитесь, что вносимая демовалюта соответствует валюте открытого счета. В Демомагазине можно приобрести виртуальные товары за демовалюту. При этом во время покупки на компьютере должен быть открыт Кошелек. Инструкции по работе с программой предлагаются на том же сайте.

Необходимо заметить, что система PayCash является единственной электронной системой, работающей с украинской гривной. Основной (российский) сайт грузится по адресу http://www.paycash.ru/, а украинская версия по http:// www.paycash.kiev.ua/. В России система продвигается под брендом Яндекс Деньги.

Чтобы совершить покупку у Вас в компьютере должен быть запущен кошелек и, конечно же, в нем должно быть достаточное количество денег.

Чтобы стать участником системы Яндекс Деньги, совсем не обязательно иметь счет в банке или кредитную карточку. Достаточно бесплатно скачать и установить на свой компьютер специальную программу - Интернет-Кошелек. При этом в платежной системе автоматически будет открыт счет, связанный с данным Кошельком. На этот счет зачисляются любым удобным способом собственные деньги, как и в обычный банк. После этого возможно проводить расчеты и получать деньги в свой Кошелек от кого-либо. Электронные деньги с виртуального счета при желании всегда можно обменять на реальные деньги. Схема работы системы Яндекс Деньги и последовательность взаимодействия с системой следующая:

вы устанавливаете на своем компьютере программу Интернет-Кошелек и кладете деньги на свой счет в процессинговом центре системы Яндекс Деньги. Таким образом у вас в Интернет-Кошельке оказывается электронная наличность;

выбираете товар или услугу в электронном магазине и отсылаете заказ - нажимаете кнопку "купить". Ваш Кошелек в этот момент должен быть запущен. Кошелек продавца (магазина) выставляет вашему Кошельку требование об оплате, содержащее текст контракта (договора купли-продажи). Контракт подписан электронной цифровой подписью продавца;

ваш Кошелек предъявляет вам текст договора. Если вы согласны и у вас достаточно денег на счету, то ваш Кошелек отсылает Кошельку продавца электронные деньги и подписанный вашей электронной подписью договор;

Кошелек продавца предъявляет полученные от вас электронные деньги в процессинговый центр для подтверждения их достоверности;

в случае положительного результата проверки процессинговый центр системы Яндекс Деньги зачисляет соответствующую сумму денег на счет продавца. Сообщение об этом передается Кошельку продавца вместе с "квитанцией" для Вас;

Получив ответ из банка, Кошелек продавца передает сообщение об успешном зачислении денег на его счет и посылает "квитанцию" вашему Интернет-Кошельку. Обратите внимание, что при совершении покупки при помощи системы Яндекс Деньги вместе с электронными деньгами передается и договор купли-продажи между участниками сделки. Во время расчетов этот договор автоматически подписывается электронными цифровыми подписями владельцев кошельков, передающих и принимающих деньги согласно этому договору. Таким образом, у вас, покупателя, остается электронный документ, подтверждающий товарные обязательства продавца, с его электронной подписью.

В России к системе PayCash подключены и успешно функционируют более ста проектов электронной коммерции и прочих компаний (в том числе OZON, Bolero, Molotok.ru, http://colibri.ru/, РОСНО, SpyLOG и проч.), поставляющих различные товары и услуги. Технологические схемы совместной работы между проектом электронной коммерции и PayCash могут варьироваться от использования разнообразных решений по интеграции программного обеспечения PayCash с Web-сайтом клиента до работы через "Центр приема платежей", предоставляющий простое технологическое решение проблемы приема Интернет-платежей. Число частных клиентов PayCash составляет более 30 000. Используя платежную систему PayCash, клиенты могут приобрести книги, видео- и аудиокассеты, CD-диски, программное обеспечение, лекарственные препараты, страховые полисы и многое другое, а также оплатить услуги сотовой и пейджинговой связи, услуги провайдеров услуг Интернет-доступа и IP-телефонии, участие в on-line-аукционах и развлекательных порталах, членские взносы и ряд других услуг.

Заканчивая обзор, следует отметить, что при выборе платежных систем покупатели товаров и услуг электронного рынка руководствуются функциональностью отечественных систем (показатели приведены в табл. 5.1). Что касается продавцов, то они, как правило, стремятся подключить Интернет-магазины ко всем платежным системам с тем, чтобы не потерять продажи из-за субъективных предпочтений покупателей.

Таблица 1 - Сравнение параметров российских платежных систем (по материалам www.ibusiness.ru)

|  |  |  |  |
| --- | --- | --- | --- |
| **Параметр** | **CiberPlat** | **PayCash** | **WebMoney** |
| Тип системы | Банковская | Цифровые наличные | Внебанковская, с высокой степенью гибкости |
| Сфера применения | В2В, В2С, С2С с ограничением | В2В, В2С, С2С | В2В, В2С, С2С |
| Транзакции между пользователями | Не реализована | Реализована | Реализована |
| Правовое пространство | Российская правовая база | Международная система | Международная система |
| Устойчивость к уничтожению | Соответствует надежности банка | Отсутствует, если деньги на кошельке | Деньги потерять невозможно |
| Мультивалютность | За пределами системы | Реализована, но не применяется из-за правовых ограничений | Имеется (в рамках системы - две валюты). На входе-выходе разные мировые валюты |
| Микро платежи | Не зависят от системы | От 0,0001 коп. | От 1 коп. (WMR) или от 1 цента (WMZ) |
| Комиссионные, взимаемые системой | От 0,5% до 4,5% в зависимости от суммы перевода | 1-2%. Минимальный порог не заявлен | 0,8% при транзакциях и выводе денег из системы. Ввод денег в систему - бесплатно. Минимальный уровень - 0,01 WM |
| Прием платежей по кредиткам | Реализован | Не заявлено | Возможность заявлена, но пока не реализована |
| Состыковка с бухгалтерией | + | + | + |
| Анонимность платежей | Невозможна | Возможна | Возможна |
| Удостоверение участников сделки | Обязательно | Возможно | Только по желанию клиентов |
| Кредитование | В рамках CyberCheck | Отсутствует | Поддерживается системой |
| Двухфазные платежи с протекцией сделки | В рамках системы не поддерживаются | Не реализованы | Поддерживаются на уровне системы |
| Ввод денег в систему | Только через банковский счет системы | Наличными (СПб., Москва), банковским переводом, почтовым, телеграфным переводом, через Сбербанк, по предоплаченным картам с ограничениями | Наличными (в 4 странах) банковским, почтовым, телеграфным переводом, через Сбербанк, Western Union, по предоплаченным картам |
| Сохранность денег | Не зависит от системы | При утрате файла-кошелька деньги пропадают | Деньги не уничтожимы |
| Вывод денег из системы | Только через банковский счет системы | Наличными (СПб., Москва), банковским переводом, почтовым, телеграфным переводом, через Сбербанк | Наличными (в 4 странах) банковским, почтовым, телеграфным переводом, через Сбербанк, Western Union |
| Шлюзы в зарубежные банки | Нет | Заявлено, но пока не реализовано | Шлюз в банке 1MB, Черногория |
| Криптография | SSL+RSA  (512 бит) + "Верба" | Собственной разработки | SSL + симметричный собственной разработки 1024 бит + RSA 1048 бит |

**3. 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. В настоящее время наиболее известным источником сертификатов являются компании Thawte и VeriSign (), однако существуют и другие системы сертификации, такие как World Registry (IBM), Cyber Trust (GTE) и Entrust (Nortel). В России дистрибьютором SSL-сертификатов компании Thawte сегодня является "РосБизнесКонсалтинг" (www.rbc.ru).

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.