**СОДЕРЖАНИЕ**

Введение

1. Системы электронных платежей и их классификация

1.1 Основные понятия

1.2 Классификация электронных платёжных систем

1.3 Анализ основных электронных платёжных систем, используемых в России

2. Средства защиты систем электронных платежей

2.1 Угрозы, связанные с использованием систем электронныхплатежей

2.2 Технологии защиты электронных платежных систем

2.3 Анализ технологий на соответствие базовым требованиям к системам электронных платежей

Заключение

Библиографический список

**ВВЕДЕНИЕ**

Узкоспециальная, мало кому интересная еще лет 10 назад тема электронных платежей и электронных денег в последнее время стала актуальной не только для бизнесменов, но и конечных пользователей. Модные слова "e-business", "e-commerce" знает, наверное, каждый второй, кто хоть изредка читает компьютерную или популярную прессу. Задача дистанционной оплаты (перевода денег на большие расстояния) из разряда специальных перешла в повседневные. Однако обилие информации по этому вопросу вовсе не способствует ясности в умах граждан. Как из-за сложности и концептуальной непроработанности проблемы электронных расчетов, так и в силу того, что многие популяризаторы работают зачастую по принципу испорченного телефона, на бытовом-то уровне все, конечно, понятно каждому. Но это до тех пор, пока не настанет черед практического освоения электронных платежей. Вот тут-то и обнаруживается непонимание того, насколько уместно использование электронных платежей в тех или иных случаях.

Между тем задача приема электронных платежей становится все более актуальной для тех, кто собирается заниматься коммерцией с использованием Интернета, а равно и для тех, кто собирается совершать покупки через Сеть. Эта статья предназначена и тем, и другим.

Основной проблемой при рассмотрении систем электронных платежей для новичка является многообразие их устройства и принципов работы и то, что при внешней похожести реализации в их глубине могут быть сокрыты достаточно разные технологические и финансовые механизмы.

Стремительное развитие популярности глобальное сети Интернет привело к возникновению мощного импульса развития новых подходов и решений в самых различных областях мировой экономики. Новым течениям поддались даже такие консервативные системы, как системы электронных платежей в банках. Это выразилось в появлении и развитии новых систем платежей - систем электронных платежей через Интернет, главное преимущество которых заключается в том, что клиенты могут осуществлять платежи (финансовые транзакции), минуя изнурительные и иногда технически трудноосуществимый этап физической транспортировки платежного поручения в банк. Банки и банковские учреждения также заинтересованы во внедрении данных систем, так они позволяют повысить скорость обслуживания клиентов и снизить накладные расходы на осуществление платежей.

В системах электронных платежей циркулируют информация, в том числе и конфиденциальная, которая требует защиты от просмотра, модификации и навязывании ложной информации. Разработка соответствующих технологий защиты, ориентированных на Интернет, вызывает серьезные затруднения в настоящее время. Причина этого в том, что архитектура, основные ресурсы и технологии сети Internet ориентированы на организацию доступа или сбора открытой информации. Тем не менее, в последнее время появились подходы и решения, свидетельствующие о возможности применения стандартных технологий Интернет в построении систем защищенной передачи информации через Интернет.

Целью РГР является анализ систем электронных платежей и разработка рекомендаций по использованию каждой из них. Исходя из поставленной цели, сформулированы следующие этапы выполнения РГР:

1. Определить основные задачи систем электронных платежей и принципы их функционирования, их особенности.
2. Проанализировать основные системы электронных платежей.
3. Проанализировать угрозы, связанные с использованием электронных денег.
4. Проанализировать средства защиты при использовании электронных платежных систем.
5. Разработать рекомендации по использованию электронных платёжных систем.

**1. СИСТЕМЫ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ И ИХ КЛАССИФИКАЦИЯ**

**1.1 Основные понятия**

Электронные расчеты. Начнем с того, что правомерно говорить о появлении электронных расчетов как вида безналичных расчетов во второй половине ХХ века. Говоря иначе, передача информации о платежах по проводам существовала давно, но приобрела принципиально новое качество, когда на обоих концах проводов появились компьютеры. Информация передавалась с помощью телекса, телетайпа, компьютерных сетей, появившихся в то время. Качественно новый скачок выражался в том, что скорость осуществления платежей значительно возросла и появилась возможность их автоматической обработки.

В дальнейшем возникли также и электронные эквиваленты других видов расчетов — наличных платежей и иных платежных средств (например, чеков).

Электронные платежные системы (ЭПС). Электронной платежной системой мы называем любой комплекс специфических аппаратных и программных средств, позволяющий проводить электронные расчеты.

Существуют различные способы и каналы связи для доступа к ЭПС. Сегодня самым распространенным из этих каналов является Интернет. Усиливается распространение ЭПС, доступ к которым осуществляется с помощью мобильного телефона (через SMS, WAP и другие протоколы). Менее распространены другие способы: по модему, по телефону с тональным набором, по телефону через оператора.

Электронные деньги. Расплывчатый термин. Если внимательно рассмотреть то, что за ним кроется, легко понять, что электронные деньги — это некорректное название "электронной наличности", а также электронных платежных систем как таковых.

Это недоразумение в терминологии обусловлено вольностью перевода терминов с английского языка. Поскольку электронные расчеты в России развивались гораздо медленнее, чем в Европе и Америке, мы вынуждены были пользоваться прочно внедрившимися терминами. Безусловно, имеют право на жизнь такие названия электронной наличности, как "цифровая наличность" (e-cash), "цифровые деньги" (digital money), "электронная наличность" (digital cash)2.

В целом термин "электронные деньги" ничего конкретного не означает, поэтому в дальнейшем мы будем стараться избегать его использования.

Электронная наличность:

— это появившаяся в 90-х годах прошлого века технология, позволяющая проводить электронные расчеты, не привязанные впрямую к переводу денег со счета на счет в банке или другой финансовой организации, то есть напрямую между лицами — конечными участниками платежа. Другим важнейшим свойством электронной наличности является обеспечиваемая ею анонимность платежей. Авторизационный центр, удостоверяющий платеж, не имеет информации о том, кто конкретно и кому переводил деньги.

Электронная наличность представляет собой один из видов электронных расчетов. Единица электронной наличности — не что иное, как финансовое обязательство эмитента (банка или другого финансового учреждения), по сути своей схожее с обычным векселем. Расчеты с помощью электронной наличности появляются там, где становится неудобным использование других систем оплаты. Наглядный пример — нежелание покупателя сообщать сведения о своей кредитной карточке при оплате товара в Интернете.

Определившись с терминологией, мы можем перейти к следующему этапу нашего разговора — поговорим о классификации ЭПС. Поскольку ЭПС опосредуют электронные расчеты, в основу деления ЭПС положены различные виды этих расчетов.

Кроме того, в этом вопросе очень важную роль играет программная и/или аппаратная технология, на которой базируется механизм ЭПС.

**1.2 Классификация электронных платёжных систем**

Электронные платежные системы можно классифицировать, основываясь как на специфике электронных расчетов, так и на базе конкретной технологии, лежащей в основе ЭПС.

Классификация ЭПС в зависимости от вида электронных расчетов:

1. По составу участников платежа (таб. 1).

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
| Вид электронных расчетов | Стороны платежа | Аналог в традиционной системе денежных расчетов | Пример ЭПС |
| Платежи банк-банк | Финансовые институты | нет аналогов | SWIFT |
| Платежи B2B | Юридические лица | Безналичные расчеты между организациями | Cyberplat |
| Платежи С2B | Конечные потребители товаров и услуг и юридические лица - продавцы | Наличные и безналичные платежи покупателей продавцам | WebmoneyPaycashCyberplatAssistE-portКредит-пилотEaccessPhonepayRapida |
| Платежи C2C | Физические лица | Прямые расчеты наличными между физическими лицами, почтовый, телеграфный перевод | WebmoneyPaycashAnelikContactRapida |

Мы не будем в дальнейшем рассматривать те ЭПС, которые призваны обслуживать электронные расчеты вида "банк—банк". Такие системы чрезвычайно сложны, они затрагивают в большей степени технологические аспекты функционирования банковской системы, и широким массам наших читателей они, скорее всего, неинтересны.

Дополнительно следует отметить, что существует еще один тип платежей, логически не совсем вписывающийся в таблицу 1. По формальным признакам он полностью попадает в область С2В, но тем не менее не может быть обеспечен средствами широко распространенных ЭПС этого вида. Для микроплатежей характерна крайне небольшая (центы или доли цента) стоимость товара. Самый характерный для всех популярных статей пример системы, реализующей микроплатежи, — это продажа анекдотов (по центу за штуку). Для осуществления микроплатежей подходят такие системы, как Eaccess и Phonepay.

1. По виду проводимых операций (таб. 2).

Таблица 2

|  |  |  |
| --- | --- | --- |
| Вид электронных расчетов | Где используются | Пример ЭПС |
| Операции по управлению банковским счетом | Системы "клиент банк" с доступом через модем, Интернет, мобильный телефон и т.п. | Операции по управлению банковским счетом Системы "клиент |
| Операции по переводу денег без открытия банковского счета | Системы перевода денег по компьютерным сетям, аналогичные почтовым и телеграфным переводам | AnelikWestern UnionMoney GramContactRapida |
| Операции с карточными банковскими счетами | Дебетовые и кредитные пластиковые карточки | Cyberplat (Cyberpos) |
| Операции с электронными чеками и другими неденежными платежными обязательствами | Закрытые системы межкорпоративных платежей | Cyberplat (Cybercheck) |
| Операции с электронной (квази) наличностью | Расчеты с физ. лицами, электронные аналоги жетонов и предоплаченных карт, используемых в качестве денежных суррогатов для оплаты товара | PaycashWebmoney |

Необходимо отметить, что системы вида "клиент — банк" известны достаточно давно. Доступ к своему счету в банке можно было получить с помощью модема. За последнее десятилетие появились новые возможности управления своим счетом с помощью Интернета, через удобный для пользователя web-интерфейс. Эта услуга получила название "Интернет-банкинга" и не внесла ничего принципиально нового в платежные системы вида "клиент-банк". Кроме того, существуют иные возможности доступа к банковскому счету, например, с помощью мобильного телефона (WAP- банкинг, SMS-банкинг). В связи с этим в данной статье мы не будем специально останавливаться на подобного рода ЭПС, отметим только, что сейчас в России услуги Интернет-банкинга предоставляют около 100 коммерческих банков, используя более 10 различных ЭПС.

Классификация ЭПС в зависимости от используемой технологии:

Одним из важнейших качеств ЭПС является устойчивость ко взлому. Пожалуй, это наиболее обсуждаемая характеристика подобных систем. Как видно из таблицы 3, при решении проблемы безопасности системы большинство подходов к построению ЭПС основывается на секретности некой центральной базы данных, содержащей критичную информацию. В то же время некоторые из них добавляют к этой секретной базе данных дополнительные уровни защиты, основанные на стойкости аппаратуры.

В принципе, существуют и другие технологии, на основе которых могут строиться ЭПС. Например, не так давно в СМИ прошло сообщение о разработке ЭПС, основанной на CDR-дисках, встроенных в пластиковую карточку. Однако подобные системы не получили широкого распространения в мировой практике, в связи с чем мы не будем заострять на них внимание.

Таблица 3

|  |  |  |
| --- | --- | --- |
| Технология | На чем основана устойчивость системы | Пример ЭПС |
| Системы с центральным сервером клиент банк, перевод средств | Секретность ключей доступа | Телебанк (Гута-банк),"Интернет Сервис Банк" (Автобанк)Anelik |
| Смарт карты | Аппаратная устойчивость смарт карты к взлому | Mondex, АККОРД |
| Магнитные карты и виртуальные кредитки | Секретность баз данных, содержащих авторизационную информацию (номера карт, PIN коды, имена клиентов и т.д.) | Assist, Элит |
| Скрэч-карты | Секретность базы данных с номерами и кодами скрэч-карт | E-port, Creditpilot, Webmoney, Paycash, Rapira |
| Файл/кошелек в виде программы на компьютере пользователя | Криптографическая стойкость протокола обмена информацией | PaycashWebmoney |
| Оплачиваемый телефонный звонок | Секретность центральной базы данных с pin-кодами и аппаратная устойчивость интеллектуальной телефонной сети | Eaccess, Phonepay |

**1.3 Анализ основных электронных платёжных систем, используемых в России**

В настоящее время в российском Интернете используется достаточно много электронных платежных систем, хотя не все они получили широкое распространение. Характерно, что практически все западные платежные системы, используемые в Рунете, привязаны к кредитным картам. Некоторые из них, например, PayPal, официально отказываются работать с клиентами из России. Наибольшее распространение на сегодняшний день получили следующие системы:

1) CyberPlat

2) Assist

3) Paycash

4) Webmoney

CyberPlat относится к системам смешанного типа (с точки зрения любой из вышеприведенных классификаций). По сути дела, можно сказать, что внутри этой системы под одной крышей собраны три отдельные: классическая система "клиент-банк", позволяющая клиентам управлять счетами, открытыми в банках-участниках системы (11 российских банков и 1 латвийский); система CyberCheck, позволяющая проводить защищенные платежи между юридическими лицами, подключенными к системе; и система Интернет-эквайринга, то есть обработки платежей, принимаемых с кредитных карт — CyberPos. Среди всех систем Интернет-эквайринга, имеющихся на российском рынке, CyberPlat обеспечивает обработку наибольшего количества видов кредитных карт, а именно: Visa, Mastercard/Eurocard, American Express7, Diners Club, JCB, Union Card, объявлено о скором подключении к системе STB-card и АККОРД-кард/Башкард. Неофициально сотрудники компании утверждали, что прорабатывают возможность стыковки и с другими российскими карточными системами. Вдобавок к перечисленному компания CyberPlat обеспечивает обработку скрэтч-карт платежной системы E-port и объявила о готовящемся вводе в строй шлюза с системой Paycash.

В настоящее время для повышения уровня защиты от платежей с ворованных кредитных карт компания производит разработку специализированной технологии PalPay, состоящей в том, что продавцу предоставляется возможность проверить, действительно ли покупатель имеет доступ к банковскому счету, связанному с кредитной картой, или только знает ее реквизиты. Официально о введении этой технологии в эксплуатацию еще не объявлено.

Большой интерес для организации работы с корпоративными партнерами представляет система CyberCheck. Ее основной особенностью (по сравнению с приемом платежей по кредитным картам) является невозможность отказа плательщика от совершения платежа постфактум. Другими словами, получение подтверждения о платеже из CyberCheck столь же надежно, как и получение такого подтверждения из банка, где размещен счет продавца. Все эти характеристики делают CyberPlat, пожалуй, наиболее продвинутой и интересной для продавцов ЭПС российского Интернета.

Система Assist в части обработки платежей с кредитных карт является во многом функциональным аналогом CyberPlat. В Москве ее интересы представляет "Альфа-банк". Всего к системе подключено 5 банков. Подсистема Интернет-эквайринга позволяет принимать платежи с карт Visa, Mastercard/Eurocard, STB-card. По состоянию на сентябрь прием платежей из других карточных систем, заявленных на сервере системы Assist, реально не обеспечивался. Впрочем, по неофициальной информации, в ближайшее время будет возможен прием карт Diners Club, дебетовых карт Cirrus Maestro и Visa Electron. Интересно, что такой тип карт обычно не принимается эквайринговыми компаниями, однако в силу своей дешевизны эти карты весьма распространены. Обычно отказ от приема дебетовых карт мотивируется соображениями безопасности. Возможно, ASSIST сумеет обойти эту проблему, использовав протокол SET, о поддержке которого было объявлено компанией буквально на днях. В отличие от традиционного способа оплаты по пластиковым карточкам в Интернете, допускающего возможность отказа владельца карточки от совершенного с нее платежа (charge-back), протокол SET гарантирует достоверность транзакции, существенно уменьшая риск для продавца.

Объявленный на сайте Assist способ расчетов с помощью электронных сертификатов, покупаемых у Интернет-провайдера, достаточно интересен как открывающий провайдерам новые направления бизнеса, однако, по имеющимся сведениям, из-за правовых сложностей до последнего времени реально никем не использовался. Тем не менее, опять же по неофициальной информации, это положение дел скоро изменится — уже осенью 2001-го мы, возможно, увидим, первую практическую реализацию этого способа расчетов.

Кроме упомянутых в описаниях карточных систем CyberPlat и Assist, существуют и другие, получившие определенное распространение на рынке. Discover/NOVUS имеет широкое распространение в Северной Америке и может быть интересен тем электронным магазинам, которые работают на западную аудиторию. Нам неизвестны отечественные эквайринговые компании, которые обрабатывали бы карты этой системы, однако имеется ряд предложений от посредников, представляющих интересы западных эквайеров. Среди российских карточных систем, после STB и Union Card, наиболее заметны на рынке "Золотая корона", "Сберкард" (Сбербанк), "Universal Card" и "ICB-card" (Промстройбанк), а также уже упоминавшиеся выше АККОРД кард/Башкард. "ICB-card" обрабатывается парой небольших эквайринговых компаний, прием платежей через Интернет с карт "Золотой короны" и "Сберкард" якобы обеспечивается напрямую эмитентами и/или связанными с ними компаниями, а в случае с Universal Card, похоже, не обеспечивается никем.

Paycash и Webmoney позиционируются их разработчиками как системы электронной наличности, однако при ближайшем рассмотрении только Paycash может по праву претендовать на такой статус.

Разработка Paycash была инициирована банком "Таврический", но в настоящее время к системе подключены и другие банки, например, "Гута-банк".

С технологической точки зрения, Paycash обеспечивает практически полную имитацию расчетов наличными. Из одного электронного кошелька (специализированной программы, устанавливаемой клиентом на свой компьютер) деньги могут быть переведены в другой, при этом обеспечивается анонимность платежа по отношению к банку. Система получила достаточно широкое распространение в России и в настоящее время предпринимает попытки выхода на мировой рынок.

Узким местом Paycash является процедура по перечислению денег в электронный кошелек. До последнего времени единственным способом сделать это было — пойти в отделение банка и перевести деньги на счет системы. Правда, были и альтернативы — для пользователей системы "Телебанк" Гута-банка, существовала возможность перевести деньги со счета в Гута-банке, не выходя из дома, но в ряде случаев, по всей видимости, проще переводить их непосредственно на счет продавца — электронного магазина, не используя Paycash в качестве посредника. Также можно было переводить деньги через Western Union или почтовым/телеграфным переводом, но привлекательность этого пути ограничивалась высоким уровнем комиссии. Для жителей Петербурга существует совсем уж экзотическая возможность — вызвать за деньгами курьера на дом. Замечательно, но, увы, не все мы живем в Северной столице.

Возможность перечисления денег в Paycash с кредитных карт по сей день отсутствует. Это связано с тем, что компании, поддерживающие работу карточных систем, обеспечивают своим клиентам возможность так называемого "charge back" — отказа от совершения платежа "задним числом". "Charge back" является механизмом, защищающим владельца кредитной карточки от мошенников, которые могут воспользоваться ее реквизитами. В случае такого отказа бремя доказательства того, что товар действительно был поставлен настоящему владельцу карточки и что платеж должен быть совершен, падает на продавца. Но в случае с Paycash такого рода доказательство в принципе невозможно — по вполне очевидным причинам. Упомянутый выше шлюз с CyberPlat, находящийся в стадии разработки, предназначен в том числе и для решения этой проблемы.

Пока же, чтобы расшить это узкое место в системе, PayCash предпринял два довольно разумных хода — выпустил предоплаченные скрэтч-карты и обеспечил прием платежей через систему переводов Contact, чьи тарифы значительно ниже почтовых (2,2% против 8%).

Система Webmoney — один из "пионеров" на рынке электронных платежей в России. В настоящее время она имеет международный характер. По некоторым сведениям, Webmoney имеет представителей не только в странах — республиках бывшего СССР, но и в дальнем зарубежье. Оператором системы является автономная некоммерческая организация "ВМ-центр".

Режим функционирования Webmoney очень напоминает работу с электронной наличностью, только внимательный и придирчивый анализ позволяет убедиться, что на самом деле Webmoney не обеспечивает полной анонимности платежей, то есть они не являются закрытыми от самих владельцев системы. Впрочем, практика работы Webmoney показала, что это ее свойство идет скорее на пользу, позволяя в некоторых случаях бороться с мошенничеством. Более того, в качестве отдельного платного сервиса "ВМ-центр" предлагает сертификацию юридического и физического лица, естественно, лишающую его анонимности по отношению к другим участникам системы. Эта возможность необходима прежде всего тем, кто хочет организовать честный электронный магазин и намеревается убедить потенциальных покупателей в своей надежности. Webmoney позволяет открывать счета и переводить средства в двух валютах: рублях и долларах.

Для доступа к системе используется программа "электронный кошелек". Дополнительными возможностями системы являются передача коротких сообщений с кошелька на кошелек, а также кредитные операции между владельцами кошельков. Впрочем, по нашему мнению, мало кто согласится кредитовать анонимов через Интернет, не имея возможности принудительно взыскивать кредит в случае его невозврата.

В отличие от Paycash, Webmoney изначально обеспечивала возможность как передачи обычных наличных в кошелек, так и обналичивание содержимого кошельков без утомительных процедур заполнения платежных поручений в банке, но достаточно странным, с юридической точки зрения, способом. Вообще, юридическое обеспечение Webmoney в части ее работы с организациями долгое время вызывало много нареканий.

Это было причиной того, что в то время как конечные пользователи активно устанавливали себе "кошельки", многие электронные магазины отказывались от использования этой ЭПС. Правда, в настоящее время эта ситуация несколько выправилась, да и активная маркетинговая позиция владельцев Webmoney приводит к тому, что имидж системы постоянно улучшается. Одной из интересных особенностей этой маркетинговой стратегии явилось то, что почти сразу после ее выхода на рынок всем желающим была предоставлена возможность зарабатывать деньги в этой системе (кое-кто, может быть, вспомнит проект "Гвозди" и его более позднего развития — visiting.ru). Так же, как и Paycash, Webmoney выпускает предоплаченные скрэтч-карты, предназначенные для ввода денег в систему.

Две системы, основанные на скрэтч-картах: E-port (Автокард-холдинг) и "КредитПилот" ("Кредитпилот.ком"), похожи как близнецы-братья. И та, и другая предполагают, что покупатель сначала купит скрэтч-карточку с секретным кодом где-то в широкой сети распространения или заказав курьером на дом, после чего начнет расплачиваться в Интернете при помощи этого кода с магазинами, принимающими платежи этих систем. E-port дополнительно предлагает возможность создания "виртуальных" скрэтч-карт путем перечисления денег на счет компании через банк или через систему "Webmoney".

Система Rapida, начавшая работать с сентября 2001 года, так же, как и две предыдущие, предлагает ввод денег на счет пользователя через скрэтч-карты или платеж в банке-участнике системы. Дополнительно заявлены возможность работы в режиме "Клиент-банк" и перевода денег на счета юридических лиц, не являющихся участниками системы, а также физическим лицам без открытия банковского счета. Доступ к системе предоставляется не только через Интернет, но и по телефону, с использованием тонального набора номера. В целом система выглядит технологически совершенной и весьма интересной, но пока что прошло недостаточно времени после ее запуска в эксплуатацию, чтобы можно было рассуждать о перспективах.

ЭПС, позволяющие производить оплату тем же путем, каким она вносится за междугородные звонки (постфактум, на основании счета, приходящего с телефонной компании), впервые появились в США и предназначались для оплаты доступа к порноресурсам. Однако в связи с систематическими мошенническими действиями многих владельцев таких систем они не снискали популярности среди покупателей, да и продавцы ими были не особо довольны, т. к. эти системы норовили существенно задерживать платежи.

Две отечественные реализации подобной концепции — Phonepay и Eaccess — находятся в самом начале своего пути. И та, и другая системы предполагают, что клиент для совершения платежа должен совершить звонок на определенный междугородный номер в коде 8-809 (предоставляемый, по всей видимости, компанией "МТУ-информ), после чего ему будет продиктована роботом некая ключевая информация. В случае Eaccess это pin-код, используемый для доступа к платному информационному ресурсу, а в случае с Phonepay — универсальная "цифровая монетка", состоящая из 12 цифр одного из пяти жестко заданных в системе номиналов. Глядя на сайты систем, можно отметить, что e-access все-таки постепенно развивается, увеличивая количество подключенных к системе магазинов, а Phonepay так и не подключил к своей системе ни одного магазина, не принадлежащего разработчикам.

На мой взгляд, подобные системы в России имеют вполне определенные перспективы, связанные с легкостью доступа к ним конечного пользователя, однако сфера их применения будет ограничиваться продажей информационных ресурсов. Длительная задержка в получении платежей (система перечислит их магазину не ранее, чем покупатель оплатит телефонный счет) делает торговлю материальными ценностями с использованием этих ЭПС довольно невыгодным занятием.

Наконец, следует упомянуть еще один вид ЭПС — специализированные системы переводов между физическими лицами, конкурирующие с традиционными почтовыми и телеграфными переводами. Первыми эту нишу заняли такие зарубежные системы, как Western Union и Money Gram. По сравнению с традиционными переводами они обеспечивают большую скорость и надежность платежа. В то же время они обладают рядом существенных недостатков, главным из которых является высокая стоимость их услуг, доходящая до 10% от суммы перевода. Другая неприятность заключается в том, что эти системы не могут быть использованы легально для систематического приема платежей за товар. Однако тем, кто хочет просто пересылать деньги родным и близким, имеет смысл обратить свое внимание на эти системы, а также на их отечественные аналоги (Anelik и Contact). Пока что ни Paycash, ни Webmoney не в состоянии составить им конкуренцию, так как получить на руки наличные, вытащив их из электронного кошелька где-нибудь в Австралии или Германии, не представляется возможным. В ЭПС Rapida заявлена такая возможность, но пока что на сайте отсутствуют какие-либо подробности, да и география офисов системы не идет ни в какое сравнение с уже имеющимися на рынке системами.

Владельцам электронных магазинов, по всей видимости, следует думать прежде всего о приеме денег с кредитных карт и систем электронных наличных — Webmoney и Paycash. По совокупности потребительских характеристик, по нашему мнению, конкуренции с CyberPlat не выдерживает ни одна из имеющихся на российском рынке систем приема платежей с кредитных карт. Все прочие системы подлежат факультативному использованию, особенно если помнить, что тот же самый E-port вовсе не обязательно устанавливать отдельно, т. к. его карты обслуживаются CyberPlat.

**2. СРЕДСТВА ЗАЩИТЫ СИСТЕМ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ**

**2.1 Угрозы, связанные с использованием систем электронных платежей**

Рассмотрим возможные угрозы разрушающих действий злоумышленника по отношению к данной системе. Для этого рассмотрим основные объекты нападения злоумышленника. Главным объектом нападения злоумышленника являются финансовые средства, точнее их электронные заместители (суррогаты) - платежные поручения, циркулирующие в платежной системе. По отношению к данным средствам злоумышленник может преследовать следующие цели:

1. Похищение финансовых средств.

2. Внедрение фальшивых финансовых средств (нарушение финансового баланса системы).

3. Нарушение работоспособности системы (техническая угроза).

Указанные объекты и цели нападения носят абстрактный характер и не позволяют провести анализ и разработку необходимых мер защиты информации, поэтому в таблице 4 приводится конкретизация объектов и целей разрушающих воздействий злоумышленника.

Таблица 4 Модель возможных разрушающих действий злоумышленника

|  |  |  |
| --- | --- | --- |
| Объект воздействия | Цель воздействия | Возможные механизмы реализации воздействия. |
| HTML-страницы на web-сервере банка | Подмена с целью получение информации, вносимой в платежное поручение клиентом. | Атака на сервер и подмена страниц на сервере.Подмена страниц в трафике.Атака на компьютер клиента и подмена страниц у клиента |
| Клиентские информационные страницы на сервере | Получение информации о платежах клиента (ов) | Атака на сервер.Атака на трафик.Атака на компьютер клиента. |
| Данные платежного поручения, вносимые клиентом в форму | Получение информации, вносимой в платежное поручение клиентом. | Атака на компьютер клиента (вирусы и т.д.).Атака на данные поручения при его пересылке по трафику.Атака на сервер. |
| Частная информация клиента, расположенная на компьютере клиента и не относящаяся к системе электронных платежей | Получение конфиденциальной информации клиента.Модификация информации клиента.Выведение из строя компьютера клиента. | Весь комплекс известных атак на компьютер, подключенный к сети Интернет.Дополнительные атаки, которые появляются в результате использования механизмов платежной системы. |
| Информация процессингового центра банка. | Раскрытие и модификация информации процессингового центра и локальной сети банка. | Атака на локальную сеть, подключенную к Интернет. |

Из данной таблицы вытекают базовые требования, которым должна удовлетворять любая система электронных платежей через Интернет:

Во-первых, система должна обеспечивать защиту данных платежных поручений от несанкционированного изменения и модификации.

Во-вторых, система не должна увеличивать возможности злоумышленника по организации атак на компьютер клиента.

В-третьих, система должна обеспечивать защиту данных, расположенных на сервере от несанкционированного чтения и модификации.

В-четвертых, система должна обеспечивать или поддерживать систему защиты локальной сети банка от воздействия из глобальной сети.

В ходе разработки конкретных систем защиты информации электронных платежей, данная модель и требования должны быть повергнуты дальнейшей детализации. Тем не менее, для текущего изложения подобная детализация не требуется.

**2.2 Технологии защиты электронных платежных систем**

Некоторое время развитие WWW сдерживалось тем, что html-страницы, являющиеся основой WWW, представляют собой статический текст, т.е. с их помощью сложно организовать интерактивный обмен информацией между пользователем и сервером. Разработчики предлагали множество способов расширения возможностей HTML в этом направлении, многие из которых так и не получили широкого распространения. Одним из самых мощных решений, явившихся новым этапом развития Интернет, стало предложения компании Sun использовать в качестве интерактивных компонентов, подключаемых к HTML-страницам Java-апплетов.

Java-апплет представляют собой программу, которая написана на языке программирования Java, и откомпилирована в специальные байт-коды, которые являются кодами некоторого виртуального компьютера - Java-машины - и отличны от кодов процессоров семейства Intel. Апплеты размешаются на сервере в Сети и загружаются на компьютер пользователя всякий раз, когда происходит обращение к HTML-странице, которая содержит в себе вызов данного апплета.

Для выполнения кодов апплетов стандартный браузер включает в себя реализацию Java-машины, которая осуществляет интерпретацию байт-кодов в машинные команды процессоров семейства Intel (или другого семейства). Заложенные в технологию Java-апплетов возможности, с одной стороны, позволяют разрабатывать мощные пользовательские интерфейсы, организовывать доступ к любым ресурсам сети по URL, легко использовать протоколы TCP/IP, FTP и т.д., а, с другой стороны, лишают возможности осуществить доступ непосредственно к ресурсам компьютера. Например, апплеты не имеют доступа к файловой системе компьютера и к подключенным устройствам.

Аналогичным решением по расширению возможностей WWW является и технология компании Microsoft - Active X. Самыми существенными отличиями данной технологии от Java является то, что компоненты (аналоги апплетов) - это программы в кодах процессора Intel и то, что эти компоненты имеют доступ ко всем ресурсам компьютера, а также интерфейсам и сервисам Windows.

Еще одним менее распространенным подходом к расширению возможностей WWW является подход, основанный на использовании технологии встраиваемых модулей Plug-in for Netscape Navigator компании Netscape. Именно эта технология и представляется наиболее оптимальной основой для построения систем защиты информации электронных платежей через Интернет. Для дальнейшего изложения рассмотрим, как с помощью данной технологии решается проблема защиты информации Web-сервера.

Предположим, что существует некоторый Web-сервер и администратору данного сервера требуется ограничить доступ к некоторой части информационного массива сервера, т.е. организовать так, чтобы одни пользователи имели доступ к некоторой информации, а остальные нет.

В настоящее время предлагается ряд подходов к решению данной проблемы, в частности, многие операционные системы, под управлением которых функционирует серверы сети Интернет, запрашивают пароль на доступ к некоторым своим областям, т.е. требуют проведения аутентификации. Такой подход имеет два существенных недостатка: во-первых, данные хранятся на самом сервере в открытом виде, а, во-вторых, данные передаются по сети также в открытом виде. Таким образом, у злоумышленника возникает возможность организации двух атак: собственно на сервер (подбор пароля, обход пароля и.т.) и атаки на трафик. Факты реализации подобных атак широко известны Интернет-сообществу.

Другим известным подходом е решению проблемы защиты информации является подход, основанный на технологии SSL (Secure Sockets Layer). При использовании SSL между клиентом и сервером устанавливается защищенный канал связи, по которому передаются данные, т.е. проблема передачи данных в открытом виде по сети может считаться относительно решенной. Главная проблема SSL заключается в построении ключевой системы и контроле над ней. Что же качается проблемы хранения данных на сервере в открытом виде, то она остается нерешенной.

Еще одним важным недостатком описанных выше подходов является необходимость их поддержки со стороны программного обеспечения и сервера, и клиента сети, что не всегда является возможным и удобным. Особенно в системах ориентированных на массового и неорганизованного клиента.

Предлагаемый автором подход основан на защите непосредственно html-страниц, которые являются основным носителем информация в Internet. Существо защиты заключается в том, что файлы, содержащие HTML-страницы, хранятся на сервере в зашифрованном виде. При этом ключ, на котором они зашифрованы, известен только зашифровавшему его (администратору) и клиентам (в целом проблема построения ключевой системы решается так же, как в случае прозрачного шифрования файлов).

Доступ клиентов к защищенной информации осуществляется с помощью технологии встраиваемых модулей Plug-in for Netscape компании Netscape. Данные модули представляют собой программы, точнее программные компоненты, которые связаны с определенными типами файлов в стандарте MIME. MIME – это международный стандарт, определяющий форматы файлов в Интернет. Например, существуют следующие типы файлов: text/html, text/plane, image/jpg, image/bmp и т.д. Кроме того, стандарт определяет механизм задания пользовательских типов файлов, которые могут определяться и использоваться независимыми разработчиками.

Итак, используются модули Plug-ins, которые связаны с определенными MIME-типами файлов. Связь заключатся в том, что при обращении пользователя к файлам соответствующего типа, браузер запускает связанный с ним Plug-in и этот модуль выполняет все действия по визуализации данных файла и обработке действий пользователя с этим файлов.

В качестве наиболее известных модулей Plug-in можно привести модули, проигрывающие видеоролики в формате avi. Просмотр данных файлов не входит в штатные возможности браузеров, но установив соответствующий Plug-in можно легко просматривать данные файлы в браузере.

Далее, все зашифрованные файлы в соответствии с установленным международным стандартом порядком определяются как файлы MIME типа. "application/x-shp". Затем в соответствии с технологией и протоколами Netscape разрабатывается Plug-in, который связывается с данным типом файлов. Этот модуль выполняет две функции: во-первых, он запрашивает пароль и идентификатор пользователя, а во-вторых, он выполняет работу по расшифрованию и выводу файла в окно браузера. Данные модуль устанавливается, в соответствии со штатным, установленным Netscape, порядком на браузеры всех компьютеров клиентов.

На этом подготовительный этап работы завершен система готова к функционированию. При работе клиенты обращаются к зашифрованным html-страницам по их стандартному адресу (URL). Браузер, определяет тип этих страниц и автоматически запускает разработанный нами модуль, передав ему содержимое зашифрованного файла. Модуль проводит аутентификацию клиента и при успешном ее завершении расшифровывает и выводит на экран содержимое страницы.

При выполнении всей данной процедуры у клиента создается ощущение “прозрачного” шифрования страниц, так как вся описанная выше работа системы скрыта от его глаз. При этом все стандартные возможности, заложенные в html-страницах, такие как использование картинок, Java-апплетов, CGI-сценариев - сохраняются.

Легко видеть, что при данном подходе решаются многие проблемы защиты информации, т.к. в открытом виде она находится только на компьютерах у клиентов, по сети данные передаются в зашифрованном виде. Злоумышленник, преследуя цель получить информацию, может осуществить только атаку на конкретного пользователя, а от данной атаки не может защитить ни одна системы защиты информации сервера.

В настоящее время, автором разработаны две системы защиты информации, основанные на предлагаемом подходе, для браузера Netscape Navigator (3.x) и Netscape Communicator 4.х. В ходе предварительного тестирования установлено, что разработанные системы могут нормально функционировать и под управлением MExplorer, но не во всех случаях.

Важно отметить, что данные версии систем не осуществляют зашифрование ассоциированных с HTML-страницей объектов: картинок, апплетов сценариев и т.д.

Система 1 предлагает защиту (шифрование) собственно html-страниц, как единого объекта. Вы создаете страницу, а затем ее зашифровываете и копируете на сервер. При обращении к зашифрованной странице, она автоматически расшифровывается и выводится в специальное окно. Поддержки системы защиты со стороны программного обеспечения сервера не требуется. Вся работа по зашифрованию и расшифрованию осуществляется на рабочей станции клиента. Данная система является универсальной, т.е. не зависит от структуры и назначения страницы.

Система 2 предлагает иной подход к защите. Данная система обеспечивает отображение в некоторой области Вашей страницы защищенной информации. Информация лежит в зашифрованном файле (не обязательно в формате html) на сервере. При переходе к Вашей странице система защиты автоматически обращается к этому файлу, считывает из него данные и отображает их в определенной области страницы. Данные подход позволяет достичь максимальной эффективности и эстетической красоты, при минимальной универсальности. Т.е. система оказывается ориентированной на конкретное назначение.

Данный подход может быть применен и при построении систем электронных платежей через Интернет. В этом случае, при обращении к некоторой странице Web-сервера происходит запуск модуля Plug-in, который выводит пользователю форму платежного поручения. После того как клиент заполнит ее, модуль зашифровывает данные платежа и отправляет их на сервер. При этом он может затребовать электронную подпись у пользователя. Более того, ключи шифрования и подписи могут считываться с любого носителя: гибких дисков, электронных таблеток, смарт-карт и т.д.

**2.3 Анализ технологий на соответствие базовым требованиям к системам электронных платежей**

Выше мы описали три технологии, которые могут быть использованы при построении платежных систем через Интернет: это технология, основанная на Java-апплетах, компонентах Active-X и встраиваемых модулях Plug-in. Назовем их технологии J, AX и P соответственно.

Рассмотрим требование об неувеличении возможностей атак злоумышленника на компьютер. Для этого проанализируем один из возможных типов атак - подмену злоумышленником соответствующих клиентских модулей защиты. В случае технологии J - это апплеты, В случае AX - погружаемые компоненты, в случае P - это включаемые модули Plug-in. Очевидно, что у злоумышленника существует возможность подменить модули защиты непосредственно на компьютере клиента. Механизмы реализации данной атаки лежат за пределами данного анализа, тем не менее, необходимо отметить, что реализация данной атаки не зависит от рассматриваемой технологии защиты. И уровень защищенности каждой технологии совпадает, т.е. все они одинаково неустойчивы к данной атаке.

Самым уязвимым местом в технологиях J и AX, с точки зрения подмены, является их загрузка из Интернет. Именно в этот момент злоумышленник может осуществить подмену. Более того, если злоумышленнику удается осуществить подмену данных модулей на сервере банка, то он получает доступ ко всем объемам информации платежной системы, циркулирующие в Интернет.

В случае технологии P опасности подмены нет, так как модуль не загружается из сети - он постоянно хранится на компьютере клиента.

Последствия подмены различны: в случае J-технологии злоумышленник может только похитить вводимую клиентом информацию (что является серьезной угрозой), а в случае, Active-X и Plug-in злоумышленник может получить любую информацию, к которой имеет доступ, работающий на компьютере клиент.

В настоящее время автору неизвестны конкретные способы реализации атак по подмене Java-апплетов. Видимо данные атаки плохо развиваются, так как результирующие возможности по похищению информации практически отсутствуют. А вот атаки на компоненты Active-X широко распространены и хорошо известны.

Рассмотрим требование о защите информации, циркулирующей в системе электронных платежей через Интернет. Очевидно, что в этом случае технология J уступает и P и AX в одном очень существенном вопросе. Все механизмы защиты информации основаны на шифровании или электронной подписи, а все соответствующие алгоритмы основаны на криптографических преобразованиях, которые требуют введения ключевых элементов. В настоящее время длина ключевых элементов составляет порядка 32-128 байт, поэтому требовать введения их пользователем с клавиатуры практически невозможно. Возникает вопрос как их вводить? Так как технологии P и AX имеют доступ к ресурсам компьютера, то решение данной проблемы очевидно и хорошо известно - ключи считываются из локальных файлов, с флоппи-дисков, таблеток или smart-карт. А вот в случае технологии J такой ввод невозможен, значит приходится либо требовать от клиента ввода длинной последовательности неосмысленной информации, либо, уменьшая длину ключевых элементов, снижать стойкость криптографических преобразований и следовательно снижать надежность механизмов защиты. Причем данное снижение является очень существенным.

Рассмотрим требование о том, что система электронных платежей должна организовывать защиту данных, расположенных на сервере от несанкционированного чтения и модификации. Данное требование вытекает из того, что система предполагает размещение на сервере конфиденциальную информацию, предназначенную для пользователя. Например, перечень отправленных им платежных поручений с отметкой о результатах обработки.

В случае технологии P данные информация представляется с виде html-страниц, которые зашифровываются и размещаются на сервере. Все действия выполняются в соответствии с описанным выше (шифрование html-страниц) алгоритмом.

В случае технологий J и AX данная информация может быть размещена в некотором структурированном виде в файле на сервере, а компоненты или апплеты должны выполнять операции по считыванию и визуализации данных. Все это в целом приводит к увеличению суммарного размера апплетов и компонентов, и, следовательно, к уменьшению скорости загрузки соответствующих страниц.

С точки зрения данного требования технология P выигрывает благодаря большей технологичности, т.е. меньших накладных расходах на разработку, и большей устойчивости к подмене компонентов при их прохождении по сети.

Что же касается последнего требования о защите банковской локальной сети, то оно выполняется за счет грамотного построения системы межсетевых экранов (брандмауэров) и от рассматриваемых технологий не зависит.

Таким образом, выше был проведен предварительный сравнительный анализ технологий J, AX и P, из которого вытекает, что технологию J следует применять в том случае, если сохранение степени защищенности компьютера клиента существенно важнее стойкости криптографических преобразований, использующихся в системах электронных платежей.

Технология Р представляется наиболее оптимальным технологическим решением, лежащим в основе систем защиты информации платежей, так как она сочетает в себе мощность стандартного приложения Win32 и защищенность от атак через сеть Интернет. Практической и коммерческой реализацией проектов с использованием данной технологией занимается, например, компания "Российские финансовые коммуникации".

Что же касается технологии AX, то ее использование представляется неэффективным и неустойчивым к атакам злоумышленников.

**ЗАКЛЮЧЕНИЕ**

Электронные деньги все более явно начинают становиться нашей повседневной реальностью, с которой, как минимум, уже необходимо считаться. Конечно, никто в ближайшие лет пятьдесят (наверное) не отменит обычные деньги. Но не уметь управляться с электронными деньгами и упускать те возможности, которые они с собой несут, - значит добровольно возводить вокруг себя «железный занавес», который с таким трудом раздвигался за последние полтора десятка лет. Многие крупные фирмы предлагают оплату своих услуг и товаров через электронные расчеты. Потребителю же это значительно экономит время.

Бесплатное программное обеспечение для открытия своего электронного кошелька и для всей работы с деньгами максимально адаптировано для массовых компьютеров, и после небольшой практики не вызывает у рядового пользователя никаких проблем. Наше время – время компьютеров, Интернет и электронной коммерции. Люди, обладающие знаниями в этих областях и соответствующими средствами, добиваются колоссальных успехов. Электронные деньги – деньги, получающие все более широкое распространение с каждым днем, открывающие все больше возможностей для человека, имеющего доступ в Сеть.

Цель расчетно-графической работы выполнены и решены следующие задачи:

1. Определены основные задачи систем электронных платежей и принципы их функционирования, их особенности.
2. Проанализированы основные системы электронных платежей.
3. Проанализированы угрозы, связанные с использованием электронных денег.
4. Проанализированы средства защиты при использовании электронных платежных систем.
5. Разработаны рекомендации по использованию электронных платёжных систем.

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. Антонов Н.Г., Пессель М.А. Денежное обращение, кредит и банки. -М.: Финстатинформ, 2005, стр. 179-185.
2. Банковский портфель - 3. -М.: Соминтэк, 2005, стр. 288-328.
3. Михайлов Д.М. Международные расчеты и гарантии. М.: ФБК-ПРЕСС, 2008, стр. 20-66.
4. Поляков В.П., Московкина Л.А. Структура и функции центральных банков. Зарубежный опыт: Учебное пособие. - М.: ИНФРА-М, 2006.
5. Гайкович Ю.В, Першин А.С. Безопасность электронных банковских систем. — М: Единая Европа, 2004 г.
6. Демин В.С. и др. Автоматизированные банковские системы. — М: Менатеп-Информ, 2007 г.
7. Крысин В.А. Безопасность предпринимательской деятельности. — М:Финансы и статистика, 2006 г.
8. Линьков И.И. и др. Информационные подразделения в коммерческих структурах: как выжить и преуспеть. — М: НИТ, 2008 г.
9. Титоренко Г.А. и др. Компьютеризация банковской деятельности. — М: Финстатинформ, 2007 г.
10. Тушнолобов И.Б., Урусов Д.П., Ярцев В.И. Распределенные сети. — СПБ: Питер, 2008 г.
11. Novell NetWare. Руководство пользователя, 2008 г.
12. Аглицкий И. Состояние и перспективы информационного обеспечения российских банков. — Банковские технологии, 2007 г. №1.