

Электронные платежи в Интернет.

Ананьев Денис 017гр.
МФТИ, 2004 г.

СОДЕРЖАНИЕ

| | |
|---|-----------|
| ВВЕДЕНИЕ | 3 |
| ГЛАВА 1. СИСТЕМЫ УПРАВЛЕНИЯ СЧЕТОМ ЧЕРЕЗ ИНТЕРНЕТ | 4 |
| Общие сведения | 4 |
| Система “Банк-клиент” | 4 |
| Банковские карты | 4 |
| ГЛАВА 2. ЭЛЕКТРОННЫЕ ДЕНЬГИ (ЭЛЕКТРОННЫЕ ДЕНЕЖНЫЕ ОБЯЗАТЕЛЬСТВА) | 7 |
| Общие сведения | 7 |
| Смарт-карты (smart-cards, chip-cards) | 7 |
| Платежные системы | 8 |
| ЛИТЕРАТУРА | 10 |

Введение

На сегодняшний день с помощью Интернета совершаются миллионы транзакций, имеющих реальное финансовое значение, начиная от покупок газет и кончая крупными сделками на рынке ценных бумаг. Все это можно назвать коммерцией в Интернете, подобно тому как размещение рекламной коммерческой информации, прайс-листов, и других материалов сейчас принято называть е-бизнесом.

Но настоящий электронный бизнес начинается тогда, когда пользователь может совершать покупки не отходя от компьютера. При этом на пути к распространению Интернет-магазинов встает проблема доступности и надежности платежных систем.

На сегодняшний день основными способами оплаты товаров и услуг через Интернет являются:

- управление счетом через Интернет;
- использование электронных денег (электронных денежных обязательств).

Цель данного эссе – рассмотреть существующие в настоящее время способы совершения электронных платежей в Интернет, вскрыть возникающие проблемы, связанные с обеспечением безопасности и надежности проведения электронных платежей, предложить решения этих проблем, а также рассмотреть правовые основы совершения электронных платежей через Интернет.

Глава 1. Системы управления счетом через Интернет

Общие сведения

Управление счетом через Интернет – это средство управления счетом, переданное банком владельцу счета во временное пользование. К данному типу оплаты относятся системы “Банк-клиент” и платежи по банковским картам.

Система “Банк-клиент”

Общие сведения о системе “Банк-клиент”

В основе системы “Банк-клиент” лежит идея управления своим банковским счетом на расстоянии. При этом как покупатель, так и продавец имеют в системе свои счета и процедура оплаты сводится к передачи запроса банку на перевод денег с одного счета на другой. Для использования таких систем нужны специальные программные средства для доступа к счету или управлению через браузер. При этом защита данных пользователей обеспечивается на компьютерах пользователей, а идентификация пользователей в процессе передачи данных происходит по секретным и/или симметричным локальным ключам и/или сертификатам.

Проблемы, возникающие при работе с системой “Банк-клиент”

Основными проблемами системы являются следующие проблемы:

1. информация обо всех платежах хранится в банке и может быть получена и использована как в интересах клиента, так и в интересах других субъектов. Все платежи со счета являются связанными, при этом при персонификации одного платежа персонифицируются и другие (частично решить эту задачу способны анонимные или псевдонимные (номерные) счета).
2. при осуществлении торговли не виртуальными, а “реальными” товарами, часто возникают проблемы, связанные с отсутствием паспорта сделки на проданный товар, наличие которого необходимо при продаже за границу товара стоимостью выше 100\$. Данная проблема связана с тем, что для оформления паспорта сделки необходимо предъявить письменный договор купли-продажи, что невозможно сделать автоматически при торговле через Интернет.
3. при продаже товара зачастую счета продавца и покупателя находятся в разных банках, при этом возникает проблема организации межбанковских расчетов, т.к. банк покупателя должен иметь прямой доступ к базе данных банка продавца, что в свою очередь негативно сказывается на безопасности соответствующих систем.
4. нет ограничений на разовый перевод, т.е. получив доступ к счету, злоумышленник может перевести всю сумму. Наложение же ограничения на разовый перевод, сильно ограничит возможности осуществления денежных переводов для владельца счета.

Банковские карты

Общие сведения о банковских картах.

В настоящее время наибольшее широко используемыми средствами оплаты в Интернете являются банковские карты.

Правила проведения торговых сделок по банковским картам обязывают продавца убедиться в том, что предъявитель карты является ее законным держателем. При оплате покупок через банковскую карту в обыкновенном магазине кассир имеет такую возможность, в случае доставки товара по телефонному или почтовому заказу ответственность за передачу товара заказчику, передавшему данные о банковской карте, несет служба доставки. Соблюдение данных правил при осуществлении сделок в Интернете

в полной мере почти невозможно, особенно в отношении информации, которая может быть получена непосредственно в момент платежа. Интернет-магазин способен проверить лишь платежеспособность карты, но не аутентифицировать владельца.

Таким образом, при предъявлении карты через Интернет, невозможно распознать:

- предъявляется ли “личная” карта владельца для оплаты товара;
- предъявляется ли карта родственника или знакомого с его согласия;
- предъявляются ли данные карты, которые оказались известны без согласия её держателя.

С точки зрения продавца, получившего данные через Интернет, эти операции совершенно одинаковы, и данные карты во всех трех случаях передаются в процессинговый центр, откуда получается информация о платежеспособности карты, и затем снимаются деньги с соответствующего счета в банке, выпустившем карту. Однако последствия этих операций будут различны. В первых двух случаях держатель карты в течение месяца получит выписку по карточному счету и согласится с проведенной операцией. В последнем же случае держатель карты будет опротестовывать операцию, которую он не совершал. И, по правилам карточных платежных систем, опротестованные денежные средства будут сняты с магазина, совершившего операцию. Теперь уже магазин будет доказывать факт совершения покупки банку. При личном визите покупателя в магазин у магазина остается подпись под чеком, или документы службы доставки товара. При продаже же через Интернет, особенно при продаже виртуального товара, подобных документов не остается, и доказательство факта покупки и доставки товара становится весьма трудным и дорогостоящим мероприятием.

В результате, в большинстве случаев мошенничества с банковскими картами потери несет продавец, из-за чего увеличивается риск и стоимость торговых операций через Интернет и уменьшается их привлекательность для магазинов. Это может быть причиной сужения географического региона, обслуживаемого данным интернет-магазином или платежной системой. Что касается держателя карты, то необходимость оспаривать совершенный не им платеж, отнимает его время и деньги.

Проблемы использования банковских карт и возможные решения:

Приведем возможные проблемные ситуации, связанные с использованием банковских карточек, и их возможные решения:

- Злоумышленник имеет доступ к трафику пользователей, а информация о карточке передается открытым текстом, без использования протоколов защиты информации (например, SSL). Чтобы предотвратить подобные возможности для злоумышленников, при передаче данных о карте необходимо пользоваться протоколом SSL. Причем сертификат на SSL протокол должен быть выдан организацией, имеющей устойчивую репутацию, например, RSA Data Security, Thawte, VeriSign, или, как минимум, производителями, включенными в список доверенных при поставке браузера, а не добавленным впоследствии клиентом самостоятельно.
- Информация о карточке попадает в руки злоумышленников при предъявлении данных о карте в поддельный или недобросовестный магазин, собирающий эту информацию для использования в криминальных целях. Подобные случаи не являются редкостью, особенно при посещении специфических сайтов (порнография, азартные игры и т.д.). Для снижения риска попадания в подобную ситуацию рекомендуется покупать товары через Интернет только у фирм с хорошей репутацией, имеющих представительство в Интернете в течение длительного времени.
- Взлом интернет-магазина. Например, в начале января 2000 г. была выкрадена и распространена в Интернет информация о кредитных карточках 300.000 клиентов CD Universe, после того, как компания отказалась выплатить взломщику 100 000\$ в качестве компенсации за неразглашение. От подобной ситуации никто не застрахован, и владелец банковской карточки повлиять на неё никак не может.

Закрытые клубные системы приема карточных платежей

Для снижения рисков операций в Интернете существуют закрытые клубные системы приема карточных платежей. Обычно участники такой системы должны зарегистрироваться специальным образом или разместить средства в специально созданном для этого страховом фонде, для того чтобы их было легко найти для разрешения возникшей спорной ситуации. Т.е. участникам предлагается раскрыть свои персональные данные в обмен на гарантии совершения более безопасных операций через Интернет и обязательства по неразглашению полученной информации. Примером закрытых клубных системы приема карточных платежей являются система Ассист (www.assist.ru) Банка “Платина” и решение от Internet Billing Company (www.ibill.com).

Глава 2. Электронные деньги (электронные денежные обязательства)

Общие сведения

Электронными деньгами принято считать денежные обязательства государства или представляющего его лица, выраженные в электронной форме. Часто под электронными деньгами также понимают выраженные в электронной форме обязательства конкретной банковской или иной структуры. Электронные деньги могут храниться, переноситься и использоваться как в специально разработанных для этого электронных устройствах, так и на обыкновенном персональном компьютере.

Смарт-карты (smart-cards, chip-cards)

Общие сведения о смарт картах

Смарт-карта представляет собой маленький компьютер со своим процессором, памятью, программным обеспечением и системой ввода/вывода информации. Пока смарт-карта используется как дебетовая карта, в которую вносятся записи о списании денег, или информация о клиенте. Работа с наличными цифровыми деньгами на базе смарт-карт обеспечена необходимым уровнем конфиденциальности, при этом при работе с смарт-картами не требуется связь с процессинговым центром для подтверждения оплаты, так как, в отличие от подобных систем на базе компьютеров, файлы-деньги не могут быть скопированы или стерты с диска целенаправленно или по неосторожности.

Смарт-карта Mondex

Смарт-карта Mondex представляет собой микрокомпьютер с тактовой частотой 10 МГц, состоящий из 8-ми битного CPU, 16-ти килобайтного ROM, 512-ти байтного RAM, и 8 килобайт энергонезависимой памяти (EEPROM) для хранения данных. Загрузка электронных денег на карточку Mondex осуществляется при помощи специализированных банкоматов для загрузки электронной наличности или при помощи телефонов (в том числе мобильных), совместимых с Mondex. Передача денег с карты на карту осуществляется при помощи специально разработанного устройства – бумажника. Для определения остатков на карте также существует карманный считыватель. Безопасность системы Mondex обеспечивается на программно-аппаратном уровне механизмами аутентификации и криптозащиты, при этом алгоритмы и принципы работы этих механизмов не опубликованы.

Первый крупномасштабный проект платежной схемы Mondex был реализован в г. Суиндон, Великобритания, в июле 1995 года. На данный момент Mondex поддерживают такие компании как AT&T, Dean Witter Discover, MasterCard, Michigan National Bank и др.

Сберкарт

Одним из крупнейших проектов внедрения смарт-карт в России является проект Сбербанка России – Сберкарт, использующая смарт-карты BGS Smartcard AG. Данная система позволяет использовать смарт-карты не только для традиционных расчетов, но и для расчетов через Интернет с помощью специального устройства – считывателя карт, подключаемого к компьютеру. По принципу работы эти смарт-карты, по-видимому, аналогичны картам Mondex. Хранение денег осуществляется путем записи в память карты соответствующих записей. Передача денег с одного кошелька в другой осуществляется через специальное устройство – кассу. Перевод денег с карты на банковский счет или получение их наличными в кассе или банкомате выполняется при помощи другого специального устройства – банкомата. Для оплаты товаров и услуг в Интернет при помощи смарт-карт Сбербанка необходимо иметь две смарт-карты (у стороны, принимающей платеж и у отправляющей его стороны) и специальное устройство, поэтому применение смарт-карт Сбербанка весьма ограничено. Еще одним фактором, сдерживающим распространение

системы, является достаточно высокая стоимость (около 100\$) устройства для связи смарт-карты с компьютером.

Платежные системы

Общие сведения о платежных системах

За основу в платежных системах взяты долговые обязательства. Сертификат на обязательство представляет собой файл, в котором содержатся обязательства выплатить предъявителю определенную сумму денег, подписанную цифровой подписью банка. Далее клиент может обменять у банка определенную сумму денег на такое обязательство и совершать им оплату в Интернет. После получения такого обязательства, получатель может предъявлять его к оплате или использовать дальше аналогичным образом. Такие проблемы как размена и защиты от копирования успешно решаются криптографами.

Сами электронные сертификаты размещены не в банке, а на компьютере их владельца. Их истинность может быть проверена без обращения к банку. Применение сертификатов сильно упрощает клиринг между банками, при этом защищенность системы может быть выше, чем в случае счетов. В рамках данных систем возможно обеспечение полной анонимности и приватность пользователей. Сертификаты связываются со счетами, в результате чего появляются достаточно гибкие и эффективные системы.

Электронные монеты DigiCash

Рассмотрим систему Ecash, являющуюся системой электронных платежей через Интернет фирмы DigiCash. В основе системы лежит представления денежных знаков различного достоинства в цифровой форме. Данная система разработана на основе патентов Дэвида Чаума (David Chaum). Электронная монета, как последовательность цифр, может сохраняться на жестком диске компьютера, а затем быть передана различными способами: послана по Интернету, по факсу или в письме, продиктована по телефону и т.д., при этом основным применением цифровых денег являются платежи в Интернете. Продавец, при получении цифровой монеты, предъявляет её в банк для авторизации, после чего данная цифровая монета помещается в список использованных, а соответствующая сумма зачисляется на расчётный счёт продавца.

Основные недостатки системы Ecash:

- необходимость доверять банку в вопросах предотвращения повторного использования электронных монет, т.к. в системе нет механизмов, с помощью которых была бы возможность независимо от банка проверить, использовалась ли ранее данная монета или нет, что, в свою очередь, допускает техническую возможность обмана клиентов путем присваивания банками цифровых денег клиентов;
- невозможность доказать факт совершения покупки (этот недостаток свойственен всем вышеперечисленным платежным системам);

Платежная система PayCash

В системе PayCash исключен случайный или преднамеренный обман участников платежной системы банком или другим участником из-за того, что любая совершаемая операция обязательно сопровождается электронными цифровыми подписями всех ее участников. Специальное программное обеспечение “Кошелек” PayCash хранит как сами электронные деньги, так и договора купли-продажи, подписанные электронными цифровыми подписями участников операции.

Деньги пользователя могут находиться на счете в банке системы PayCash или непосредственно в “Кошельке” на компьютере пользователя. Управление счетом в системе PayCash осуществляется только через Интернет при помощи того “Кошелька”, с помощью которого он был открыт, при этом сам банк не может управлять этим счетом. Владелец

“Кошелек” несет полную ответственность за сохранность кошелька, как средства управления счетом и совершения сделок при помощи электронных денег.

Банк не может отказаться признать “электронные деньги”, выплаченные посредством “Кошелька”, т.к. при переводе денег с банковского счета в системе PayCash в “Кошелек” пользователя используется процедура слепой подписи. Технология слепой подписи подобна процедуре передачи пин-кода владельцу банковской карты: сгенерированный системой пин-код распечатывается на принтере без печатающей ленты на бланке, помещенном в запечатанный конверт. Оттиск пин-кода формируется в запечатанном конверте, и не известен никому, даже служащему, выдающему карты.

“Кошелек” может быть использован для платежей на любую сумму в пределах имеющихся средств, не задумываясь о необходимости их размена, вплоть до сотых долей, что, к примеру, позволяет строить систему оплаты телекоммуникационных услуг в зависимости от объема передаваемых данных (0,002 коп за 1Кб).

Литература

1. Виктор Достов, "Компьютерра", №40, 2000, "Банк или кошелек".
2. Александр Иванов, "Век Электронной Коммерции", №2, 2002, "Как сегодня можно честно приобрести программу через Интернет?".
3. Алексей Гришин, "Корпоративные системы", №2, 2003, "Электронные платежи и Internet"
4. Сергей Волков, Виктор Достов, "Мир Интернет", № 5, 2000, "Платежные механизмы современного Интернета"
5. Кирилл Сурский, "Вестник НАУФОР", №5, 2002, "Бум платежных решений"