# Введение.

Бурное развитие Интернета в 90-х годах прошлого века заставило переосмыслить саму сущность денег, их форму и назначение. «Покупка не отходя от компьютера" требовал простого и удобного способа платить за товары и услуги на расстоянии.

В 1994 году Дэвид Чаум, которого впоследствии назвали отцом электронной наличности, начал выпуск в рамках системы DigiCash первых электронных денег.

Десять лет спустя системы, основанные на цифровой наличности, стали для Интернета таким же привычным явлением, как, например, безналичные деньги для реального мира. И это притом, что электронные платежные системы, как правило, экстерриториальны, как и весь рынок интернет-торговли. То есть, скажем, француз может запросто совершить покупку в английском электронном магазине, оплатив товар деньгами английской же электронной платежной системы.

# Электронные платежные системы России.

Электронные деньги - это несколько усовершенствованный вариант кредитной карточки, но вместо банкомата используется компьютер, а вместо самой кредитной карточки - файлы сертификатов (или хотя бы имя пользователя и пароль, в зависимости от платежной системы). Для формализации понятия "электронные деньги", приведем определение, которое дает им Артем Генкин, докторант Финансовой академии при Правительстве РФ, автор книги "Частные деньги: история и современность". Под "электронными деньгами" он предлагает понимать некоторую информацию, передаваемую любыми способами электронной коммуникации и исполняющую роль купюр и монет при произведении платежей как в Интернете, так и в оффлайне. Существует несколько синонимов: "цифровые деньги", "цифровая наличность", "электронная наличность".

Любая Электронная Платежная Система обеспечивает ряд преимуществ своих электронных денег по сравнению с деньгами традиционными, ведь переводы и платежи внутри ЭПС обладают следующими свойствами:

* Моментальностью (занимают считанные секунды);
* Анонимностью (не во всех платежных системах);
* Относительно небольшими комиссиями (сопоставимыми с комиссиями банков);
* Экстерриториальностью;
* Защищенностью (электронные деньги нельзя или крайне сложно подделать, в отличие от наличных);
* Делимостью (любая сумма ЭД больше принятого в данной ЭПС минимума может быть без труда разделена на много более мелких частей).

Принципы использования электронных денег остались теми же, что и для средств на кредитках:

- Для самостоятельного пополнения своего счета нужно идти в банк, независимо от того, чем пользоваться, - кредиткой или электронным кошельком. Однако электронные кошельки можно пополнять и предоплаченными картами, почтовым переводом или в офисе компании, создавшей платежную систему.

- Используя электронный кошелек, как и при применении кредитки, можно получать деньги от других участников системы, для этого кто-либо должен отправить деньги с карточки и/или электронного кошелька на карточку или кошелек. Возможны двусторонние обмены карточка-кошелек, кошелек-кошелек.

- Вывод денег (получение наличных) с кошелька так же прост, как и с карточки. Можно отправить деньги на карточку и снять их в ближайшем банкомате.

- В гарантиях безопасности оба средства на одинаковом уровне. Пользователь кредитки - потенциальная жертва для преступников, промышляющих возле банкоматов. Если пользоваться электронным кошельком, есть риск стать жертвой виртуального преступника.

- Для управления счетом и электронного кошелька, и кредитки используется терминал. В случае с кредитной картой - банкомат, в случае с кошельком - компьютер с соответствующим программным обеспечением. Пользоваться банкоматом просто, а компьютером - удобно. Для тех, кто совсем не умеет работать на компьютере, электронный кошелек – непозволительная роскошь, в то время как ни для среднеквалифицированного пользователя, ни для высоко квалифицированного нет никаких сложностей в этом деле - нужно разобраться всего с одной программой.

## 1.1 «Яндекс Деньги »

Яндекс.Деньги -внебанковская система мгновенных наличных расчетов в сети Интернет, использующая цифровые наличные. «Яндекс.Деньги» оперирует только рублями,.

Система позволяет

- внести деньги на свой кошелек,

-перевести деньги другому абоненту системы

- вывести деньги (получить наличные),

- произвести покупку в интернет-магазине, который работает с "Яндекс.Деньги",

- заплатить за коммунальные услуги и т.д..

Система работает только с российскими рублями. Тем не менее, давнее родство системы с PayCash позволяет совершать покупки в любых интернет-магазинах, подключенных к иностранными представительствам PayCash, что дает очень широкие возможности.

Схема работы системы «Яндекс.Деньги»:

1. Вы регистрируетесь в платежной системе Яндекс.Деньги и кладете деньги на свой счет в Процессинговом Центре системы . Таким образом у вас в Кошельке оказывается электронная наличность

2. Выбираете товар или услугу в электронном магазине и отсылаете заказ — нажимаете кнопку «купить». Кошелек продавца (магазина) выставляет вашему Кошельку требование об оплате, содержащее текст контракта (договора купли-продажи). Контракт подписан электронной цифровой подписью продавца.

3. 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.

4. Кошелек продавца предъявляет полученные от вас электронные деньги в Процессинговый Центр для подтверждения их достоверности.

5. 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.

6. Получив ответ из банка, Кошелек продавца передает сообщение об успешном зачислении денег на его счет, и посылает «квитанцию» вашему Кошельку.

## 1.2 ****«CyberPlat»****

[CyberPlat](http://www.cyberplat.ru) - Интегрированная универсальная мультибанковская система Интернет-платежей CyberPlat® ("КиберПлат"), исторически первая российская платежная система, создана в 1997 году.. Расчеты в платежной системе [CyberPlat](http://www.cyberplat.ru/) ведутся между тремя основными участниками: Покупателем, электронным Интернет-Магазином и Банком.

Клиентами системы [CyberPlat](http://www.cyberplat.ru/) могут стать:

Физические лица - в качестве Покупателей товаров, услуг и информации в Интернет - Магазинах.

Юридические лица:

в качестве Покупателей товаров, услуг и информации в Интернет - Магазинах;

в качестве электронных Магазинов;

в качестве корпоративных клиентов, регистрирующих своих работников как Покупателей.

В настоящее время в системе [CyberPlat](http://www.cyberplat.ru/) предусмотрена оплата товара или услуги:

со счета, открытого Покупателю в Банке-Участнике системы;

по банковской кредитной карточке любого банка-эмитента.

Свой счет в Банке-участнике Покупатель пополняет:

либо взносом наличными через кассу дополнительного офиса;

либо безналичным переводом через любой российский банк.

Основные компоненты системы CyberPlat:

**CyberCheck** - подсистема обслуживания транзакций Покупателей, зарегистрированных в системе. CyberCheck обеспечивает конфиденциальность, надёжность и юридическую чистоту взаимодействия сторон, а также полное отсутствие отказов от заявленных платежей. Это реализуется механизмами поддержки электронного документооборота с применением имеющей юридическую силу электронной цифровой подписи (ЭЦП) с длиной ключа 512 бит. Благодаря перечисленным свойствам, подсистема используется в схемах класса business-to-business.

**CyberPOS** - подсистема обслуживания платежей по пластиковым картам международных и российских платежных систем, не требующая регистрации клиента-покупателя в системе CyberPlat.

**Internet-Banking** - управление счетом в банке-участнике системы через Интернет, независимо от того, является получатель платежа клиентом системы CyberPlat или нет.

## 1.3 ****«WebMoney»****

[Web Money Transfer](http://www.webmoney.ru) –внебанковская система мгновенных наличных расчетов в сети Интернет, использующая цифровые наличные. Средством расчетов в системе служат титульные знаки - WebMoney (WM). Поддержкой системы занимаются:

в России - автономная некоммерческая организация “ВМ-Центр”

в США – компания IMTB Inc.

Банком-эмитентом WM является [International Media Bank AD (Podgorica)](http://www.imtb.com), юрисдикция - Республика Черногория (Югославия).
Все WM, имеющиеся в системе, хранятся на электронных счетах (кошельках) ее участников (WM типа R – эквивалент RUR – на R-кошельках, WM типа Z – эквивалент USD – на Z-кошельках). При этом финансовые расчеты между участниками осуществляются только с использованием однотипных кошельков. Приобрести WM можно:

путем безналичного перевода денежных средств с любого банковского счета в IMB (доллары США) или на счет АНО "ВМ-Центр" (российские рубли) 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 же в обмен на наличные деньги.

Участникам системы гарантируется полная и безоговорочная анонимность расчетов. Все сообщения в системе передаются в закодированном виде, с использованием алгоритма защиты информации подобного RSA с длиной ключа более 1024 бит. Для каждого сеанса используются уникальные сеансовые ключи. Система безопасности включает также 12-значный идентификатор пользователя, его личный пароль, уникальные номер кошелька и код сделки.
Необходима установка клиентского программного обеспечения WebMoney Keeper. WebMoney Keeper позволяет выполнять следующие операции:

создавать и удалять WM-кошельки (количество создаваемых кошельков не ограничено);

переводить доллары США, российские рубли, иную валюту в WM;

осуществлять мгновенные расчеты в WM с другими участниками системы (частными лицами или компаниями, принимающими WebMoney в качестве средства платежа за товары и услуги);

получать WM, отправленные другим участником;

переводить WM на банковские счета;

обсуждать с предполагаемыми партнерами условия торговой сделки по встроенной в WM Keeper защищенной системе обмена сообщениями.

В системе реализовано два типа платежей:

Обычный платеж. Покупатель производит оплату. При этом с его кошелька списывается, а в кошелек магазина зачисляется сумма в размере стоимости товара. После чего магазин осуществляет доставку товара.

Двухфазный платеж (с протекцией торговой сделки). Покупатель оплачивает счет, задавая при этом секретный пароль — код протекции. Деньги переводятся в кошелек продавца, но остаются при этом заблокированными – продавец не может воспользоваться ими до тех пор, пока полностью не выполнит своих обязательств, и покупатель не сообщит ему код протекции.

# *Устройство электронных платежных систем.*

При всем многообразии электронных платежных систем, присутствующих на рынке, им присуще некоторые общие черты. В каждой системе присутствует как минимум плательщик (payer) и получатель (payee). Перемещение денег от плательщика к получателю обеспечивается определенной последовательностью действий - протоколом электронного платежа. Теоретически обе стороны могут связываться и напрямую (современный криптографический аппарат позволяет это), но практически такая схема оказывается ненадежной и приходится вводить так называемые "финансовые институты", которые соотносят электронный перевод с реальным перемещением денежных средств. В роли "финансового института" могут выступить и банк, и любая другая уважаемая контора, которой доверяют участники обмена. Кстати, банки очень настороженно относятся к рискованным экспериментам с виртуальной наличностью. В основном финансовыми институтами становятся сами разработчики платежных систем, которые в принципе не способны обеспечить все электронные единицы живыми деньгами. Налицо превышение эмиссионного права. Чтобы хоть как-то сгладить углы и удержать систему от падения, привлекаются дополнительные игроки...

Финансовый институт, принимающий денежные средства от плательщика, называется эмитентом (issuer). Институт, передающий их получателю, - эквайр (acquirer). Эмитент и acquirer могут осуществлять перевод любым платежным протоколом, и даже быть единым, обслуживающим и плательщиков, и получателей.

Если все собрано в одно, платежная система называется централизованной, что, во-первых, означает постоянный "перегруз" центрального сервера, во-вторых - подрыв доверия к системе (возможность оппортунистического поведения). Вот почему центральный финансовый институт обычно делегирует часть своих прав сторонним конторам, контролируя их деятельность или не контролируя. В контроле есть как положительные так и отрицательные стороны. "Полоожтельные "в том что центр в ответе за все: если эмитент скрылся с чужими деньгами, их оплачивает "материнская" организация. С другой стороны, в такой системе задавлена инициатива и отсутствует конкуренция, значит, спектр предоставляемых услуг невелик...

Если контроль отсутствует, работать с электронными деньгами может любой желающий. Добиваться одобрения "центра" необязательно, и потому можно вводить любые услуги, лишь бы существовал спрос. Ценой за это становится отсутствие каких бы то ни было гарантий. Если вас кто либо обманул, можно обращаться только в прокуратуру, но добиваться возврата наличности от других участников рынка бессмысленно (хотя в условиях свободного рынка обязательно появятся лица, которые предложат услуги подобного рода, так что ситуация не совсем безнадежна).

В банковском мире действует первая схема. Центробанк следит за всеми коммерческими банками и в случае малейших подозрений немедленно устраивает разбирательства. А если банк, в который положены деньги, вдруг пропал, все долги перебрасываются на Центробанк. Но и спектр предоставляемых услуг остается на недоразвитом уровне, так как он контролируется Центробанком. Электронные платежные системы могут использовать либо первую, либо вторую схему, либо их комбинацию. Тогда на рынке будут присутствовать и "доверенные" конторы, и "серые" участники, которым люди доверяют только на свой страх и риск.

# 3. Безопасность и анонимность

Удаленное обслуживание в банке позволяет повысить эффективность частного бизнеса при минимальных усилиях со стороны его владельцев. При этом обеспечиваются: экономия времени (не нужно приходить в банк лично, платеж можно выполнить в любое время); удобство работы (все операции производятся с персонального компьютера в привычной деловой обстановке); высокая скорость обработки платежей (банковский оператор не перепечатывает данные с бумажного оригинала, что дает возможность исключить ошибки ввода и сократить время обработки платежного документа); мониторинг состояния документа в процессе его обработки; получение сведений о движении средств по счетам.

Однако, несмотря на очевидные преимущества, электронные платежи в России пока не очень популярны, поскольку клиенты банков не уверены в их защищенности. Это прежде всего связано с распространенным мнением, что компьютерные сети легко может "взломать" какой-нибудь хакер. Этот миф прочно укоренился в сознании человека, а регулярно публикуемые в СМИ новости об атаках на очередной веб-сайт еще сильнее укрепляют это мнение. Но времена меняются, и электронные средства связи рано или поздно заменят личное присутствие плательщика, желающего сделать безналичный банковский перевод с одного счета на другой.

Безопасность электронных банковских операций сегодня можно обеспечить. Гарантией этому служат современные методы криптографии, которые используются для защиты электронных платежных документов. В первую очередь это ЭЦП, соответствующая ГОСТ 34.10-94. С 1995 г. она успешно применяется в Банке России. Вначале он ввел систему межрегиональных электронных расчетов всего в нескольких регионах. Сейчас она охватывает все регионы Российской Федерации и представить без нее функционирование Банка России практически невозможно. Так стоит ли сомневаться в надежности ЭЦП, если ее использование проверено временем и уже так или иначе касается каждого гражданина нашей страны?

Электронно-цифровая подпись - гарантия безопасности. Согласно типовому договору между банком и клиентом наличие под электронным документом достаточного количества зарегистрированных ЭЦП уполномоченных лиц служит основанием для совершения банковских операций по счетам клиента. В Федеральном законе от 10.01.02 г. N 1-ФЗ "Об электронной цифровой подписи" определено, что ЭЦП должна формироваться и проверяться сертифицированным ФАПСИ программным обеспечением. Сертификация ЭЦП является гарантией того, что данная программа выполняет криптографические функции согласно нормативам ГОСТ и не совершает деструктивных действий на компьютере пользователя.

Чтобы проставить на электронный документ ЭЦП, необходимо иметь ее ключ, который может храниться на каком-нибудь ключевом носителе информации. Современные ключевые носители ("e-Token", "USB-drive", "Touch-Memory") по форме напоминают брелоки, и их можно носить в связке обычных ключей. В качестве носителя ключевой информации можно также использовать дискеты.

Если клиент желает использовать в расчетах с банком электронные платежи, нужно заключить договор, получить от банка документацию и необходимое программное обеспечение. Потом надо настроить на своем компьютере программное обеспечение (согласно документации) и сформировать ключи ЭЦП. Подписать документ электронной цифровой подписью можно автоматически, вставив ключевой носитель в компьютер. Затем носитель следует извлечь и убрать в надежное место - без ключа личную электронную подпись никто не сможет подделать. Для защиты платежных документов от просмотра информация в них шифруется при передаче в банк и обратно.

Каждый ключ ЭЦП служит аналогом собственноручной подписи уполномоченного лица. Если в организации бумажные "платежки" обычно подписывают директор и главный бухгалтер, то в электронной системе лучше всего сохранить тот же порядок и предусмотреть для уполномоченных лиц разные ключи ЭЦП. Впрочем, можно использовать и одну ЭЦП - данный факт необходимо отразить в договоре между банком и клиентом.

Ключ ЭЦП состоит из двух частей - закрытой и открытой. Открытая часть (открытый ключ) после генерации владельцем представляется в Удостоверяющий центр, роль которого обычно играет банк. Открытый ключ, сведения о его владельце, назначение ключа и другая информация подписываются ЭЦП Удостоверяющего центра. Таким образом формируется сертификат ЭЦП, который нужно зарегистрировать в системе электронных расчетов банка.

Закрытая часть ключа ЭЦП (секретный ключ) ни при каких условиях не должна передаваться владельцем ключа другому лицу. Если секретный ключ был передан даже на короткое время другому лицу или оставлен где-нибудь без присмотра, считается, что ключ "скомпрометирован" (т.е. подразумевается вероятность копирования или нелегального использования ключа). Иначе говоря, в этом случае лицо, не являющееся владельцем ключа, получает возможность подписать несанкционированный руководством организации электронный документ, который банк примет к исполнению и будет прав, так как проверка ЭЦП покажет ее подлинность. Вся ответственность в данном случае ложится исключительно на владельца ключа. Действия владельца ЭЦП в этой ситуации должны быть аналогичны тем, которые предпринимаются при утере обычной пластиковой карты: этот человек должен сообщить в банк о "компрометации" (утере) ключа ЭЦП. Тогда банк заблокирует сертификат данной ЭЦП в своей платежной системе и злоумышленник не сможет воспользоваться своим незаконным приобретением.

Предотвратить нелегальное применение секретного ключа можно и с помощью пароля, который накладывается как на ключ, так и на некоторые виды ключевых носителей. Это способствует минимизации ущерба при утере, поскольку без пароля ключ становится недействительным и у владельца будет достаточно времени, чтобы сообщить банку о "компрометации" своей ЭЦП.

# Заключение.