# Электронный чек(ECheck): безопасная схема

*Мартынов И. В., МФТИ, апрель 2005*

**Предпосылки возникновения**

Прежде чем рассказывать про систему Echeck, я считаю надо напомнить о том, что такое обычный чек и каким образом он используется. Банковский чек – это письменное безусловное поручение банку, в котором у человека имеется счёт, снять определённую сумму денег с этого счёта. Согласно существующим нормам, чек должен выписываться на специальном листе бумаги (взятом из чековой книжки) с обязательным указанием следующих реквизитов :

1) Название банка
2) Номер счёта, зарезервированного под чековые расходы
3) Снимаемая сумма с указанием валюты
4) Дата
5) Подпись

Также чек может содержать различную дополнительную информацию, например, указание, что обналичить его может только определённый человек (именной чек). Банковский чек является довольно удобным средством оплаты, особенно при крупных сделках. Для расчёта чеком достаточно попросить свой банк выдать чековую книжку (если сумма на счёте превышает некоторое минимальное значение).

Рассмотрим, как проходит расчет с помощью чека. Допустим, две стороны – плательщик и получатель, заключили сделку, и получатель передал товар/оказал услугу и теперь ожидает её оплаты. Для этого он высылает (как правило по почте) счёт-фактуру - это документ, содержащий перечень поставленных товаров/услуг с кратким описанием и счёт на них. Плательщик, получив счёт-фактуру, выписывает чек на указанную сумму и высылает его по почте. Далее получатель подтверждает (индоссирует) чек, указывает на нем номер своего счёта, подписывает чек, и отправляет его в свой банк на оплату. Банк проверяет все подписи и реквизиты чека и кредитует счёт плательщика – депонирует чек. Теперь банк получателя должен вернуть свои деньги, то есть банк плательщика обязан снять со счёта, указанного в чеке, требуемую сумму, и выплатить её банку получателя в обмен на чек.

Так как в каждом банке обналичивается много разных чеков, выписанных клиентами разных банков, то неизбежно возникают взаимные денежные требования между банками. Например, клиент банка А заплатил чеком в 100 долл. клиенту банка Б, а другой клиент банка Б заплатил чеком на 90 долларов клиенту А соответственно. Возникают взаимные требования: получается, что один банк должен другому 100 долларов, а тот ему 90. Логично было бы не проводить встречные выплаты, а зачесть сумму в 90 долл. и ограничиться уплатой остатка (сальдо) в 10 долл. На практике этот зачет представляет собой технически трудную задачу, так как требования друг к другу могу иметь десяток и более банков. Для решения этой задачи существуют специальные организации. Они называются клиринговые, или расчетные палаты (clearing house), которые выполняют взаимные зачеты требований банков друг к другу. Эти организации осуществляют приём от банков инкассируемых чеков и их анализ. По окончании дневного зачета расчетная палата составляет специальный меморандум, согласно которому проходят расчётные операции между банками. Взаимный зачет дает огромную экономию средств и времени, по сравнению с тем, что если бы каждый банк рассчитывался со всеми другими банками отдельно.

Отметим, что число операций, проводимых с чеками, велико, поэтому велики будут издержки. На проверку, транспортировку, клиринг бумажных чеков расходуется значительное количество ресурсов банка. Кроме того, проверять подлинность чека

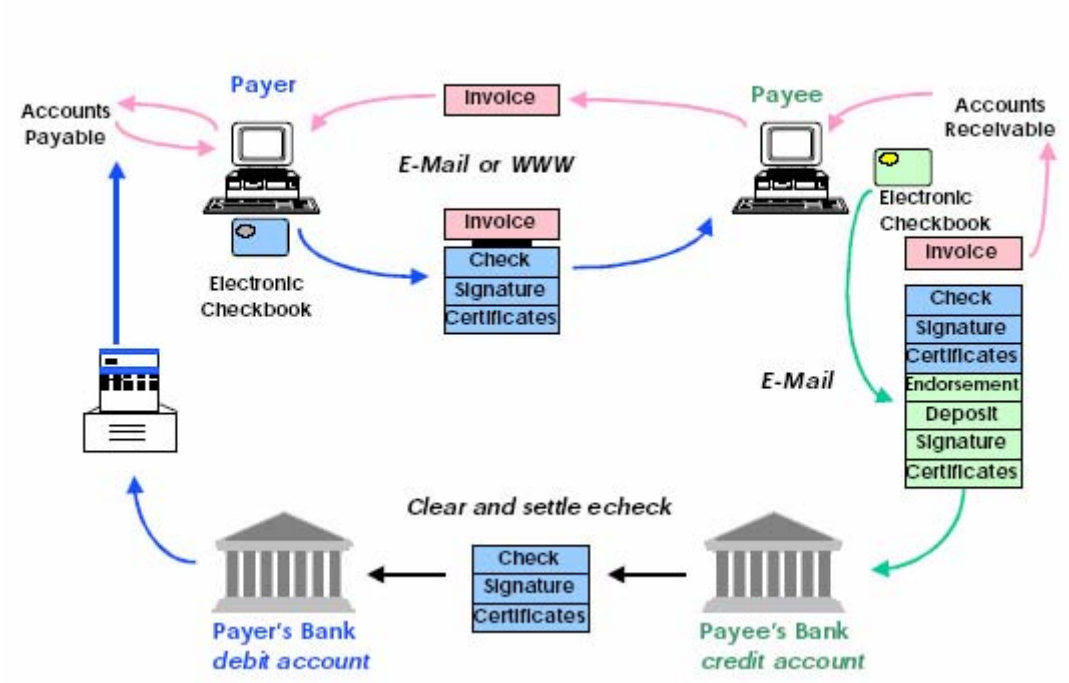
приходится вручную, а это чревато ошибками. Поэтому, в качестве стимула для экономики, была предложена система, которая оперирует электронными документами, сохраняющими все права обычных.

## Проект ECheck

Система **ECheck** была разработана Технологическим Консорциумом Финансовых Служб (FSTC), крупной финансовой организацией, включающей в себя порядка 100 ведущих банков, исследовательских институтов и лабораторий. Работа над проектом началась в 1995 г. и длилась около 4х лет. Система ECheck была испытана Министерством Финансов США и является единственной электронной платёжной системой, признаваемой этой организацией.

Электронный чек - это объект, предназначенный для выполнения оплаты и прочих функций бумажного чека. По сути, он представляет собой файл в памяти компьютера, но этот файл будет обладать теми же правами, что и соответствующий реальный чек. Система ECheck была спроектирована таким образом, чтобы как можно лучше вписаться в существующую систему обращения чеков. Она не нацелена на полное вытеснение бумажных аналогов, эти два вида чеков будут мирно сосуществовать. Но преимущества ECheck весьма ощутимы : это более высокая скорость обработки, проверки подписи, возможность безопасной пересылки по электронной почте и сети Интернет. На Рис. 1 показан типичный жизненный цикл электронного чека. Как видим, он очень похож на путь обычного чека.

**Рисунок 1 – обращение е-чека**




## Электронные подписи

Гарантией подлинности обычного чека служит подпись, подделать которую довольно сложно, даже имея образец. Для удостоверения электронных чеков используется цифровая подпись, выполненная по методу открытого ключа. Подписывается не сам документ, а хэш от отдельных его блоков, каждая сторона подписывает только свои блоки(об этом речь пойдёт ниже). При этом используется один из алгоритмов шифрования с открытым ключом(RSA или DSA). Стойкость этих алгоритмов достаточно велика для того чтобы подписывать чеки на огромные суммы денег. Разумеется, пару

отрытый/секретный ключ надо где-то получать, для этого нужен центр сертификации, о них будет сказано тоже ниже.

## Язык FSML

Язык написания электронных чеков - FSML(Financial Services Markup Language) – является производным от SGML(Standard Generalized Markup Language). Этот язык предназначен для составления финансовых документов; с помощью тэгов он жёстко задаёт блочную структуру документа и содержание каждого блока. Для документа ECheck определён следующий перечень блоков:

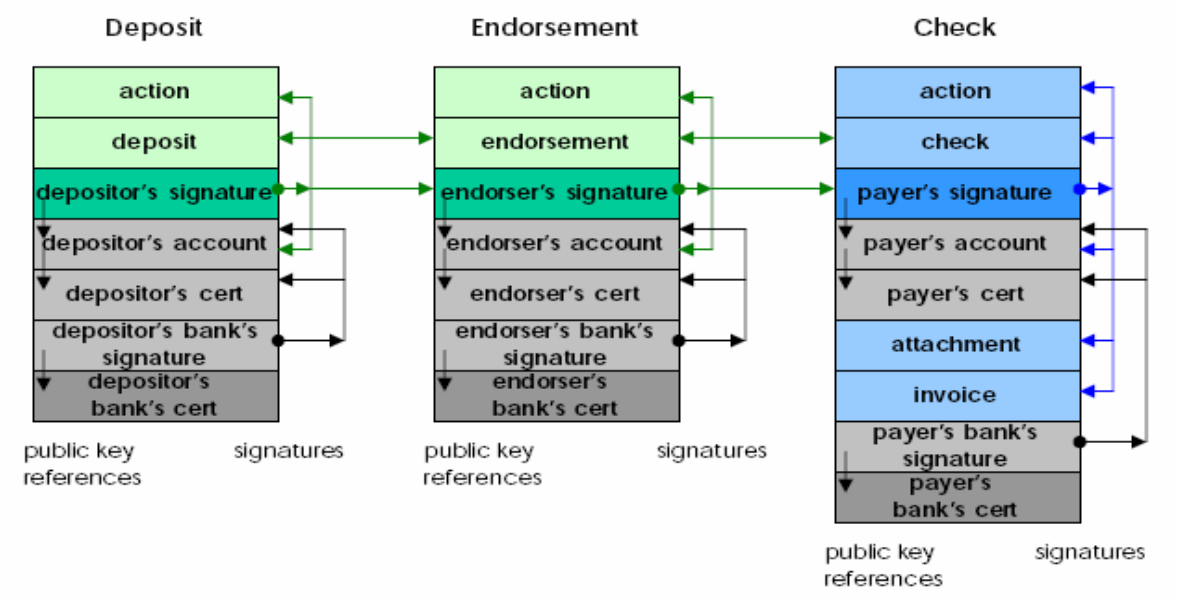
**Таблица 1 – блоки е-чека**

| **Название блока** | **Содержание** |
|---|---|
| <account> | Данные по банковскому счету плательщика. Заполняется банком плательщика. |
| <action> | Действия, которые должен выполнить получатель |
| <attachment> | Дополнительная информация, передаваемая плательщиком |
| <bankstamp> | Состояние обработки |
| <bundle> | Заполняется, если пересылается сразу несколько чеков |
| <cashletter> | Кассовые письма |
| <cert> | Информация о сертификате X.509 плательщика. |
| <certification> | Данные для создания сертифицированного е-чека |
| <check> | Данные непосредственно е-чека(сумма, дата, когда он подлежит оплате ). |
| <deposit> | Данные, добавленные при депонировании чека |
| <endorsement> | Данные, добавленные при подтверждении чека |
| <invoice> | Оплачиваемый этим чеком счёт |
| <signature> | Список названий подписанных блоков, список их хэшей, ссылка на сертификат открытого ключа, необходимая для проверки подписи. |

Заметим, что <signature> - это блок, содержащий подпись нескольких других блоков. Таких блоков <signature> в чеке несколько, каждый из них представляет собой цифровую подпись одной из сторон(плательщика, получателя, банка). Схема подписания чека приведена на Рис 2. Сначала плательщик, создав чек, подписывает блоки <action>, <check>, < payer’s account>, <attachment>, <invoice>. Открытый ключ для проверки этой подписи находится в блоке < payer’s cert>. Этот блок вместе с <account> подписывается банком плательщика, подпись хранится в блоке <payer’s bank signature>. Блок подписи банка содержит ссылку на сертификат банка, в котором находится ключ для проверки его подписи. Индоссант подписывает свои блоки, плюс ещё блок <check> и подпись плательщика, банк индоссанта подписывает его счёт и сертификат. Похожим образом действует депозитор.

Отдельно надо сказать об устройстве блока подписей(упрощённо показан на таблице 2). Пары строк <blockref> и <hash alg="TYPE"> повторяются столько раз, сколько блоков мы подписываем. Случайная строка <nonce> присоединяется к началу каждого блока перед хэшированием, и делает результат непредсказуемым. Теперь злоумышленник не сможет подобрать два документа с одинаковым хэшем, чтобы, подписав одно, потом выдавать за подписанное другое. Заметим, что здесь мы фактически подписываем хэш от хэшей блоков.

**Рисунок 2 – процесс подписания**




Блочная структура чека удобна тем, что позволяет легко добавлять/удалять информацию, когда этого требует процесс обработки. Например, счёт-фактура прикрепляемая к чеку плательщиком, отделяется от него получателем при подаче на оплату. Отделив счёт-фактуру, мы оставляем его хэш в блоке подписей, и цифровая подпись плательщика всё равно может быть проверена.

**Таблица 2 – блок подписи**

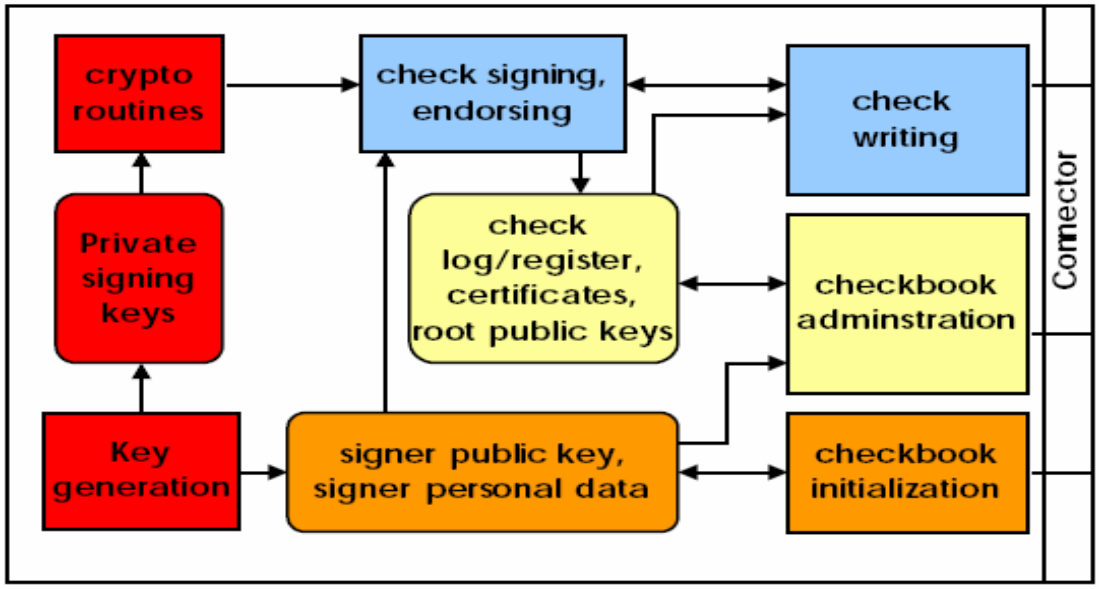
| Тэг | Тип данных | Описание |
|---|---|---|
| <**sigdata**> | | Маркер начала данных, которые будут хэшированы и подписаны |
| <blockref> | Строка | Имя блока, чей хэш находится в следующей строке |
| <hash alg="TYPE"> | HEX-строка | Хэш этого блока. "TYPE" определяет хэширующий алгоритм |
| <nonce> | Строка | Случайная строка, генерируемая перед хэшированием и добавляемая к блокам |
| <sigref> | Строка | (Необязательный)Ссылка на <account> или на блок сертификата |
| <certissuer> | Строка | (Необязательный)Имя издателя сертификата |
| <certserial> | | (Необязательный)Уникальный номер сертификата |
| <algorithm> | Строка | Алгоритм, используемый для хэширования и подписания. Может быть "md5/rsa", "sha/dsa", или "sha/rsa" |
| <username> | Строка | (Необязательный)Имя подписавшегося |
| **</sigdata>** | | Маркер конца данных, которые будут хэшированы и подписаны |
| <sig> | HEX-строка | Подпись того, что содержится между маркерами <sigdata>. Подписывается закрытым ключом! |

## Электронная чековая книжка

Вся индустрия электронного чека основывается на доверии банков и получателей денег к цифровой подписи плательщика. Если секретный ключ будет украден, то ничто не

мешает злоумышленнику создавать поддельные чеки, неотличимые от настоящих. Поэтому так важно обеспечить сохранность закрытого ключа. Для этого предназначены устройства, называемые электронными чековыми книжками. Они выдаются банком при создании счёта для выплаты чеков, и имеют в своём составе смарт-катру, на которой хранится секретный ключ, информация о владельце, его данные о банковском счёте, и сертификат, подписанные банком.

**Рисунок 3 - смарт-карта**




Именно эта смарт-карта ставит цифровую подпись на чеках. Весь процесс простановки проходит внутри неё, таким образом, секретный ключ не покидает карты и не подвергается риску быть похищенным. Более того, невозможно извлечение секретного ключа из книжки без повреждения последней. Помимо проставления цифровой подписи, чековая книжка выполняет следующее:

- Добавляет данные о плательщике и его банковском счёте.
- Ведёт историю всех выписанных чеков, что может понадобиться при обнаружении фальшивок.
- Генерирует случайную строку и добавляет её в начало блока перед хэшированием.
- Добавляет в е-чек свой уникальный заводской номер, проводит их последовательную нумерацию, что гарантирует уникальность номера.

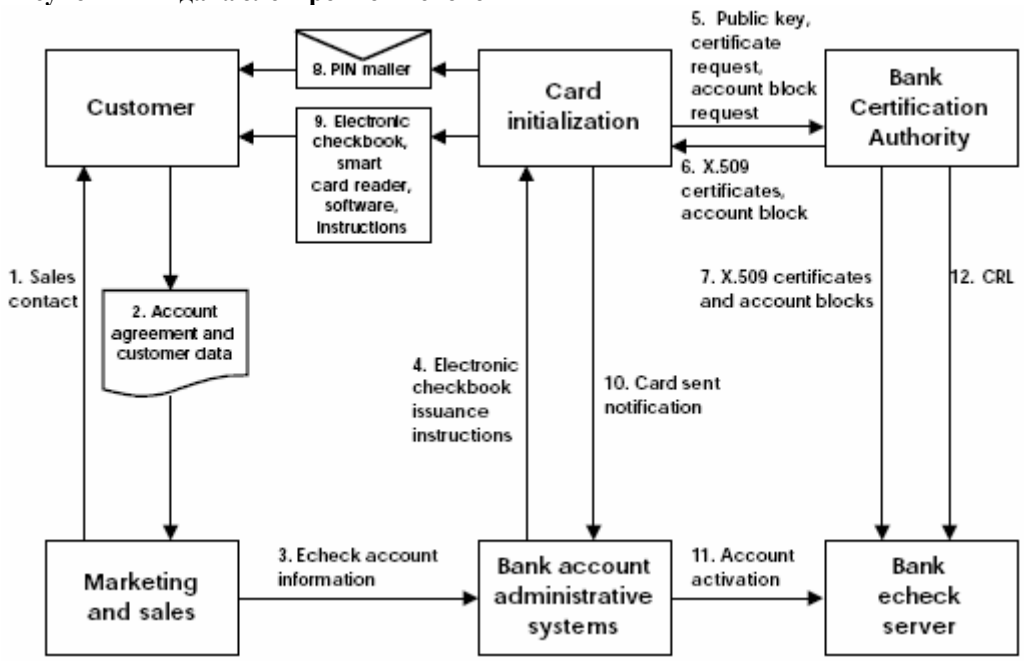
При инициализации банком карты внутри неё происходит генерация пары ключей, затем открытый ключ извлекается и включается в состав сертификата, который подписывает банк. Секретный ключ остаётся неизвестен даже банку.

Карта защищается ПИН-кодом, без которого невозможно подписание/подтверждение чека. Для каждой карты существует 3 ПИН-кода, открывающих один из режимов пользования :

1) Создание и подписание/подтверждение чека(показан голубым на Рис 3).
2) Администрирование. Открывается возможность изменять лог, сертификат, считывать данные о держателе и его открытый ключ(жёлтый цвет). Также из этого режима можно разблокировать карту, блокированную неправильными действиями пользователя
3) Инициализация. Доступно всё прочее + генерация пары ключей и запись личных данных держателя(оранжевый цвет).

На Рис 4 показан механизм выдачи электронной чековой книжки. Клиент направляет свои данные и согласие на изготовление чековой книжки в отдел маркетинга. Банковская система администрирования создаёт, в случае необходимости, счёт для е-чека, и посылает инструкции для создания чековой книжки в службу инициализации карт(она может быть отдельной фирмой) Далее, генерируется пара ключей,

**Рисунок 4 - выдача электронной чековой книжки**

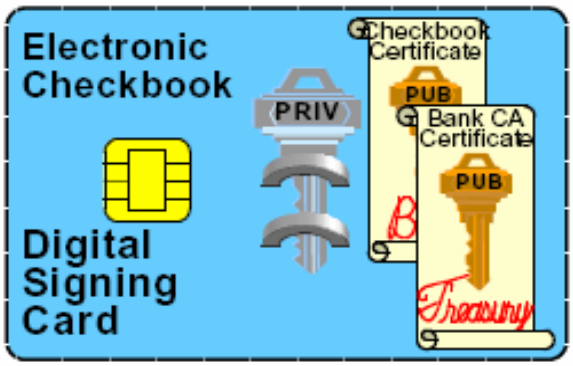



открытый ключ извлекается и направляется в банковский центр сертификации, где создаётся и подписывается сертификат и блок счёта. Служба инициализации карт прошивает их в смарт-карты, и отсылает готовую карту вместе с ПИН-ом, устройством чтения и программой для работы клиенту. Как только клиент пришлёт подтверждение о получении карты, банковская система администрирования активирует его чековый счёт. Банк имеет сервер е-чека, на котором ведётся база данных всех выписанных сертификатов, где хранятся данные о состоянии соответствующего счёта.

**Инфраструктура открытого ключа**

Как система, работающая с открытым ключом, ECheck содержит средство проверки открытого ключа – *сертификат ключа*. Это электронный документ, связывающий открытый ключ с субъектом, правомерно владеющим соответствующим банковским счётом. Без такой верификации злоумышленник может выдать себя за любого плательщика, подменив открытый ключ. Для заверения сертификата своего клиента банк ставит на нем цифровую подпись, для проверки которой, в свою очередь, нужен сертификат банка. А он уже выдаётся неким Главным Сертификационным Центром,

**Рисунок 5 - сертификаты**




которому доверяют все. В США, например, таким центром служит Министерство Финансов. Сертификат Министерства Финансов, содержащий его открытый ключ, предполагается общеизвестным. Кстати, издаёт его само Министерство Финансов, т. е. сертифицирует само себя.

Все изданные сертификаты банки хранят у себя, и могут выдавать их в случае необходимости другим банкам или организациям. При нарушениях со стороны клиента

банк может отозвать свой сертификат, для этого он ведёт CRL(Список Отозванных Сертификатов). Если при поверке выясняется, что сертификат числится в этом списке, то подпись на чеке считается недействительной.

Сертификаты в системе ECheck имеют формат X.509, что является международным стандартом в этой области.

## Заключение

Электронный чек обеспечивает высокую безопасность обращения денежных средств. Лежащие в основе алгоритмы цифровой подписи(RSA/DSA) и хэширования (MD5/SHA) достаточно надёжны и испытаны. Обойти их, используя дыры в протоколе, на сегодняшний день не представляется возможным. Пара ключей генерируется в смарт-карте сертифицированной  схемой, что обеспечивает хороший их выбор. При этом секретный ключ остаётся неизвестен ни банку, ни хозяину карты, что исключает его компрометацию. Даже если злоумышленник завладеет картой, он не сможет извлечь закрытый ключ без повреждения последней. В случае же повреждения или утери карты банк отзывает сертификат, все остальные банки узнают об этом посредством передачи CRL, и чек, подписанный этим ключом, становится недействительным. ECheck также предусматривает защиту от повторной оплаты одного и того же чека, каждый е-чек имеет свой уникальный номер. Для пересылки электронных чеков используется либо защищённая электронная почта(MIME), либо безопасная web-транзакция SSL. Однако, полностью подтвердить безопасность е-чека могут только испытания на рынке.

Первый этап испытания системы ECheck успешно закончился в 2000 г., за это время Министерство Обороны США рассчиталось со своими поставщиками посредством электронных чеков на сумму 10 млн. долларов. Сейчас проходит вторая фаза испытания, в которую вовлечено большее число банков и организаций. В случае успеха начнётся массовое внедрение электронного чека в банковскую систему, что обещает значительное (порядка 30%) сокращение издержек на чековые расчёты.

Создание такой системы особенно актуально для США, где примерно 75% крупных безналичных расчетов приходится на чеки. В других странах, эта цифра меньше, например, в Великобритании и Франции около 40%, поэтому ECheck в этих странах будет введён позже. Внедрение электронных чеков и создание соответствующей инфраструктуры требует значительных инвестиций, которые не всегда смогут себя окупить.

Что касается России, то в силу разных причин чековый оборот здесь ещё меньше, вместо чеков чаще всего используют платёжные поручения и векселя. Кроме того, сказывается отсутствие специального закона о чеках, который бы легализовал их электронные варианты. Так что внедрение ECheck в России вряд ли состоится в обозримом будущем. Но, тем не менее, некий аналог системы ECheck в России существует – это проект CyberCheck, являющийся по сути системой оплаты с помощью чека. Подробнее об этом смотрите на сайте http://www.cyberplat.ru/cybercheck/

**Используемая литература**

1) *The Electronic Check Architecture* by Milton M. Anderson,
Version 1.0.2 -- September 29, 1998.
Источник: [ http://www.echeck.org/library/wp/architecture.html ]

2) *eCheck. An overview and explanation of security measures* by Chuck Wade,
BBN Technologies, a part of GTE, 22-September-1999, C 27-42
Источник: [ http://www.echeck.org/demos/meeting92299/echeck-overview-security.pdf ]

3) Реферат "*Коммерческий банк и система денежных расчетов*" Скороходов В.В.
Московский Государственный Авиационный Институт, 1995 г.
Источник: [ http://www.5ka.ru/8/18027/1.html ]

4) *Современное чековое обращение: проблемы и перспективы развития в России*.
Беляева О.А., директор юридического департамента ЗАО «Генинжконсалт»
Источник: [ http://www.optim.ru/bh/2002/2/rbelyaeva/rbelyaeva.asp ]

5) Материал сайта http://*www.echeck.org*