Классификация ЭПС

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

I. Классификация ЭПС в зависимости от вида электронных расчетов

Электронные расчеты, в свою очередь, можно классифицировать по нескольким критериям. Приведем два наиболее важных для понимания сущности ЭПС:

1) по составу участников платежа

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 C2B	Конечные потребители товаров и услуг и юридические лица - продавцы	Наличные и безналичные платежи покупателей продавцам	Webmoney Paycash Cyberplat Assist E-port Кредит-пилот Eaccess Phonepay Rapida
Платежи C2C	Физические лица	Прямые расчеты наличными между физическими лицами, почтовый, телеграфный перевод	Webmoney Paycash Anelik Contact Rapida

2) по виду производимых операций

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.	Телебанк (Гута-банк)
Операции по переводу денег без открытия банковского счета	Системы перевода денег по компьютерным сетям, аналогичные почтовым и телеграфным переводам	Anelik Western Union Money Gram Contact Rapida
Операции с карточными банковскими счетами	Дебетовые и кредитные пластиковые карточки	Cyberplat (Cyberpos)
Операции с электронными	Закрытые системы межкорпоративных	Cyberplat

чеками и другими неденежными платежными обязательствами	платежей	(Cybercheck)
Операции с электронной (квази) наличностью	Расчеты с физ. лицами, электронные аналоги жетонов и предоплаченных карт, используемых в качестве денежных суррогатов для оплаты товара	Paycash Webmoney

II. Классификация ЭПС в зависимости от используемой технологии

Одним из важнейших качеств ЭПС является устойчивость ко взлому. 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.

Таблица 3

Технология	На чем основана устойчивость системы	Пример ЭПС
Системы с центральным сервером клиент-банк, первод средств	Сектретность ключей доступа	Телебанк (Гута-банк), "Интернет Сервис Банк" (Автобанк) Anelik
Смарт-карты	Аппаратная устойчивость смарт-карты ко взлому	Mondex, АККОРД-кард
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	Paycash Webmoney
Оплачиваемый телефонный звонок	секретность центральной базы данных с pin-кодами и аппаратная устойчивость интеллектуальной телефонной сети	Eaccess, Phonepay

Пример платежной системы в Интернет.

В рамках всемирной сети Интернет еще не устоялись методы проведения платежей, которые могли бы полностью удовлетворить все запросы нарастающей волны электронной коммерции. Тем не менее, в настоящее время большинство платежей в Интернете осуществляется при помощи кредитных карточек. Платежи при помощи карточек обладают рядом недостатков, к которым можно, например, отнести низкий уровень безопасности и защищенности, полное отсутствие анонимности участников платежа, узкий диапазон сумм возможных платежей, жесткое разделение клиентов на покупателей и продавцов, относительная медленность расчетов. Кроме того, в некоторых странах, например в России, кредитные карточки мало распространены. В ближайшие годы эти недостатки вряд ли будут преодолены из-за инерции, порождаемой существующей инфраструктурой и огромной массой консервативных потребителей (кроме того, модернизация существующей карточной инфраструктуры требует значительных инвестиций и приводит к потере инвестиций, вложенных ранее). Все это указывает на то, что у пользователей Интернета существует потребность в альтернативных платежных системах.

Банк “Таврический” совместно с компанией “Алкорсофт” разработали свою систему платежей в Интернете, которую назвали PayCash.

Перспективная платежная система, которая могла бы заполнить нишу в сфере Интернет-платежей, не занятую карточными системами, и которая при определенных обстоятельствах могла бы конкурировать с карточными системами, должна обеспечивать:

- высокий уровень безопасности и защищенности, включая защиту от банка,
- высокий уровень анонимности участников,
- проведение платежей в широком диапазоне сумм, включая платежи в несколько центов,
- низкую стоимость трансакций,
- легкую интегрируемость в различные торговые системы,
- равноправие продавцов и покупателей, стимулирующее появление новых продавцов и облегчающее возврат денег,
- стимулирующее спонтанных покупателей быстродействие (любая операция должна занимать меньше 10 секунд),
- масштабируемость.

Понятие безопасности платежной системы включает в себя наличие в системе процедур разрешения конфликтов. При этом беспристрастная третья сторона должна быть в состоянии справедливо разрешить спор вовлеченных в конфликт сторон на основании несекретных данных, предоставляемых каждой стороной. Нами сразу же были отброшены такие модели платежных систем, в которых защита интересов банка (эмитента) существенно зависит от "честности" клиентского программно-аппаратного обеспечения. Очевидно, что в такой системе клиентское программное обеспечение должно функционировать на специализированном оборудовании, защищенном от внешнего вмешательства (физического и программного), например на специальном компьютере, размещенном на чиповой карточке. Защита секретов банка при помощи устройств, доступных для злонамеренного исследования вне банка, представляется нам малонадежной, особенно в сравнении с надежностью современных криптографических методов. В частности, современные чиповые карточки не в состоянии надежно защитить секреты банка, как это показывает удручающая история академических взломов таких

карточек, осуществленных в последние годы. Криминальный взлом одного такого устройства может привести к катастрофическим последствиям для всей системы. Ярко выраженным примером платежной системы, полагающейся на "честность" клиентского программно-аппаратного обеспечения, является карточная система Mondex.

Платежные системы, не полагающиеся на "честность" клиентского программно-аппаратного обеспечения, можно разбить на две группы. В первую группу входят аппаратные системы, в которых клиентское программное обеспечение функционирует на специализированном компьютере, предназначенном для вычислений только в рамках платежной системы. В настоящее время большинство аппаратных систем имеют примитивное клиентское программное обеспечение со скудной функциональностью, так как оно ориентировано на маломощные компьютеры чиповых карточек. Во вторую группу входят программные платежные системы, в которых клиентское программное обеспечение является всего лишь одним из приложений, запущенных пользователем на компьютере общего назначения. Программное обеспечение клиента в этом случае может быть достаточно сложным и многофункциональным, так как разработчики не слишком стеснены аппаратными ограничениями. Очевидно, что принципиальной разницы между этими группами платежных систем нет, хотя в практических приложениях системы из этих групп могут иметь некоторые преимущества друг перед другом. Например, в аппаратной системе отсутствуют риски, связанные с действиями компьютерных вирусов и "троянских коней".

Мы решили разрабатывать программную платежную систему, так как такую систему легче модифицировать, добавляя к ней новые услуги или иным образом приспосабливая ее к складывающимся условиям. Кроме того, любой Интернет-путешественник всегда имеет под рукой "приличный" компьютер, на котором он может запустить соответствующее клиентское программное обеспечение (возможно, это не совсем верно для пользователей WebTV). Высокие темпы миниатюризации компьютеров, а также темпы роста их мощности, позволяют надеяться, что в ближайшем будущем различие между аппаратными и программными системами нивелируется, так как сколь угодно прихотливое клиентское программное обеспечение можно будет установить в специализированный компьютер размером в спичечный коробок. Отметим также, что возможны гибридные варианты, когда часть работы выполняется специализированным компьютером, а часть - компьютером общего назначения. Далее мы рассматриваем только программные системы.

Один из способов обеспечения анонимности клиента состоит в открытии банком анонимного счета, ассоциированного с некоторым публичным ключом. Банку, вообще говоря, не надо знать о своем клиенте ничего, кроме его публичного ключа, при помощи которого банк проверяет цифровую подпись под распоряжениями этого клиента. Хотя анонимному клиенту нельзя предоставлять некоторые услуги, например выдавать необеспеченный кредит, анонимный клиент все же очень удобен для банка, так как в этом случае банк не расходует свои ресурсы на выяснение предыстории (благонадежности) клиента. Поэтому накладные расходы по обслуживанию анонимного клиента гораздо меньше, чем расходы по обслуживанию неанонимного клиента, по крайней мере до тех пор, пока в широкую практику не войдут цифровые удостоверения личности. Чтобы быть дешевой, массовая платежная система должна, как мы считаем, допускать наличие анонимных клиентов. В системе PayCash анонимные счета допускаются.

Другой способ обеспечения анонимности плательщика состоит в том, что плательщик производит платеж путем передачи получателю платежа цифровых денежных сертификатов на предъявителя. Сертификаты плательщик предварительно получает в

банке с использованием технологии слепой подписи. Технология подписания банком денежного сертификата вслепую позволяет разорвать связь между выпускаемым сертификатом и счетом, с которого снимаются деньги: по данному сертификату банк не в состоянии установить, в каком сеансе выпуска сертификатов он его подписал. Тем самым обеспечивается свойство непрослеживаемости платежей. Однако при таком способе проведения платежей возникает специфическая проблема многократного использования денежных сертификатов, так как цифровые сертификаты легко копируются. По способу решения этой проблемы платежные системы делятся на онлайновые и оффлайновые.

Платежная система называется онлайновой, если моментом получения денег получателем платежа является момент успешной авторизации платежа банком, то есть момент признания банком предъявленных сертификатов. Таким образом, в онлайновой платежной системе получатель платежа должен обращаться в банк для подтверждения каждого платежа.

Платежная система называется оффлайновой, если моментом получения денег получателем платежа является момент успешной проверки получателем платежа сертификатов, предоставленных плательщиком в качестве оплаты. Это означает, что получатель платежа, например продавец, в момент платежа может не обращаться в банк - ему достаточно предъявить все полученные сертификаты банку, например в конце рабочего дня. В этом случае уменьшается зависимость продавца от доступности банка в сети, а банк немного экономит на времени установления многочисленных повторных контактов с продавцом. Банк обязан зачислить на счет продавца сумму, соответствующую корректным цифровым сертификатам. Выявлять многократно использованные сертификаты и разбираться с мошенниками банк должен без участия клиентов. Имеется ряд остроумных методов слепого получения сертификатов на предъявителя и последующей их передачи в качестве платежного средства, которые позволяют раскрыть анонимного плательщика, если плательщик использует цифровой денежный сертификат дважды.

В системах обоих типов банк должен составлять список использованных сертификатов, по которому он должен проверять на повторное использование сертификаты, предъявляемые получателями (продавцами) для зачисления денег на их счета. По сравнению с онлайновыми системами оффлайновые системы заметно сложнее, требуют больше ресурсов и их протоколы более интерактивны. Вполне возможно, что, когда оффлайновые программные системы созреют, наконец, для практического применения, на рынке платежных систем в Интернете не останется свободного места. Это значит, что время массовых оффлайновых систем может никогда не наступить. Однако основной причиной нашего выбора в пользу онлайновой системы является то, что в оффлайновой системе в момент получения сертификатов в банке клиент не может быть анонимом.

При построении системы PayCash в качестве отправной точки была использована онлайновая платежная система, предложенная Чаумом. Денежным сертификатом (монетой номинала i) в этой системе являются следующие данные:

Coin(i, X) = {i, X, gi-1(f(X))},

где X - выбираемый клиентом случайный серийный номер монеты, который является элементом большого множества M' M M = (Z/mZ)*; m - составное число, чье разложение на множители известно только банку; f : M' -> M - легко вычисляемое отображение, публично известное и трудно обратимое для всех участников платежной системы, кроме, быть может, банка (другой вариант - образ f имеет "очень специальный" вид); gi(x) = xEi :

M -> M - публично известные отображения с подходящими показателями степени. Отображение gi-1 является RSA-подписью банка, соответствующей номиналу монеты i. Если в системе используется несколько валют, то каждой валюте должен соответствовать свой набор функций gi (индекс валюты мы опускаем). Множество M (число m) и отображение f также могут зависеть от номинала и валюты. Описанные монеты банк может изготавливать для клиента вслепую. Покупатель осуществляет платеж, передавая продавцу набор монет, сумма номиналов которых равна величине платежа. Продавец отправляет полученные монеты в банк для авторизации. Банк удостоверяется в том, что предоставленные монеты отсутствуют в списке использованных монет, после чего заносит их в этот список, увеличивает сумму на счету продавца на величину платежа и сообщает продавцу об успехе. Платежи в данной системе абсолютно не связаны друг с другом.

Некоторые недостатки системы Чаума

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

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

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

прогресс компьютерной техники постепенно снижает серьезность проблемы большого списка использованных монет. Кроме того, Чаум предложил остроумный способ слепого возврата банком сдачи, что позволяет использовать для платежа всего лишь одну монету.

Модифицированная монетная система Чаума

Введем следующее изменение в монетную систему Чаума. Для каждой планируемой монеты клиент генерирует случайную пару {S, P} из закрытого и открытого ключей в рамках некоторой системы подписи, например RSA. Обозначим соответствующие подписывающие и верифицирующие функции через SignP(·) и VerifyP(·, ·), так что VerifyP(X, Y) = True тогда и только тогда, когда Y = SignP(X). Монета, которую клиент получает в кооперации с банком, состоит из следующих данных:

Coin(i, P) = {i, P, gi-1(f(P))},

то есть в качестве случайного серийного номера монеты в данной модификации используется случайный открытый ключ. Теперь, однако, в качестве платежа клиент отсылает расширенную монету

{Order, Y, Coin(i, P)}, (1)

где Y = SignP(Order), а Order - уникальное описание платежа, которое может, в частности, содержать номер счета, на который следует зачислить деньги. Формат описания не существен для общего рассмотрения. Банк авторизует платеж только в том случае, если монета с данным P отсутствует списке использованных монет и выполнено равенство

VerifyP(Order, Y) = True. (2)

Если авторизация прошла успешно, то банк заносит монету (1) в список использованных монет, зачисляет на счет продавца надлежащую сумму и отправляет продавцу и плательщику подписанные квитанции, упоминающие Order.

При помощи описанной модификации мы избавились от необходимости для банка и плательщика доверять друг другу. Действительно, банк не может присвоить монету, так как он не в состоянии изготовить расширяющие монету данные, которые удовлетворяли бы соотношению (2). В свою очередь, банк защищается от обвинений в присвоении монеты, предъявляя расширяющие монету данные, которые удовлетворяют соотношению (2).

Эта модификация позволяет также легко связывать платежную систему практически с любой торговой системой: достаточно в Order включить хэш контракта, описывающего условия сделки. В этом случае квитанция с подписью банка будет связывать платеж и контракт, а содержание контракта останется для банка неизвестным.

Заметим также, что с теоретической точки зрения использование открытого ключа в качестве серийного номера монеты усиливает защищенность монеты. Например, если фальшивомонетчик научится обращать функцию f, то, чтобы воспользоваться монетой, ему потребуется еще найти секретный ключ, соответствующий открытому ключу монеты.

Во время платежа плательщик должен подписать Order столько раз, сколько монет включено в платеж. Так как платеж может включать десятки монет, а наложение подписи является довольно длительной операцией, то описанная схема может оказаться

неприемлемо медленной, если иметь в виду существующий парк персональных компьютеров. Ситуацию можно заметно улучшить, если воспользоваться методом слепого возврата сдачи Чаума. В этом случае в каждом платеже может участвовать небольшое число монет, например одна.

Платежная система PayCash

В системе PayCash клиент расплачивается при помощи данных, которые называются платежной книжкой и имеют следующую структуру:

PayBook(N, P) = {N, P, g-N(f(P))},

где P, f и g имеют тот же смысл, что и выше, и g-N(X) = g-1(g-1(...g-1(X)...)). Неотрицательное целое число N (диспозиция книжки) определяет платежеспособность книжки. Необходимым условием для того, чтобы тройка {n, P, A} была платежной книжкой, является равенство

f(P) = gn(A), (3)

которое может проверить любой участник системы, и в частности сам владелец книжки. Таким образом, платежная книжка отличается от монеты Чаума тем, что вместо случайного серийного номера используется случайный открытый ключ, а сумма закодирована не с помощью "номинала", а с помощью степени подписывающего отображения.

Любой клиент, очевидно, может изготовить пустую платежную книжку, то есть книжку с нулевой диспозицией PayBook(0, P) = {0, P, f(P)}. Кроме того, имея в своем распоряжении платежную книжку PayBook(N, P), клиент может построить все книжки с тем же P, но с меньшей диспозицией

PayBook(0, P), PayBook(1, P),..., PayBook(N - 1, P).

С другой стороны, понижение диспозиции известной клиенту книжки является единственным для него способом изготовления платежных книжек с ненулевой диспозицией без помощи банка. Изготовление платежных книжек с ненулевой диспозицией "с нуля" без помощи банка не менее трудно, чем изготовление монет в исходной системе Чаума. Действительно, если клиенту удалось изготовить платежную книжку PayBook(N, P) = {N, P, A} с диспозицией N>0, то в соответствующей системе Чаума ему также удалось изготовить монету Coin(i, P) = {i, P, gN-1(A)}, где i - номинал, соответствующий подписи g-1. Задача самостоятельного увеличения диспозиции непустой платежной книжки {N, P, A}, которая не получена клиентом из известной ему книжки путем понижения ее диспозиции, эквивалентна получению банковской подписи g-1(A) для данных A = g-N(f(P)), которые являются фиксированными и имеют случайный характер.

В кооперации с банком клиент может пополнять платежную книжку, то есть увеличивать ее диспозицию, причем он может увеличить как диспозицию вновь созданной платежной книжки с нулевой диспозицией, так и диспозицию ранее пополнявшейся платежной книжки. Для пополнения платежной книжки PayBook(N1, P) на сумму N2 клиент передает в банк ослепленные данные B. Один вариант ослепления, являющийся простейшей модификацией метода Чаума, имеет следующий вид:

B = gN3(r) g-N1(f(P)),

где r - случайный элемент множества M, а N3iN2. В обмен на сумму N2 банк возвращает клиенту подпись C = g-N2(B), из которой клиент извлекает требуемую часть книжки PayBook(N1+ N2, P)

C/gN3-N2(r) = g-N1-N2(f(P)).

В описанной схеме можно использовать и другие варианты слепого получения подписи RSA, например метод Чаума. Отметим, что банк не получает никакой информации о диспозиции той книжки, которую пополняет клиент.

В неослепленном виде платежные книжки предъявляются в банк во время проведения платежей. Банк ведет список всех открытых ключей P, соответствующих когда-либо предъявлявшимся действительным платежным книжкам, то есть книжкам, удовлетворяющим соотношению (3). Вместе с каждым ключом P банк также хранит некоторые другие данные, которые мы будем называть виртуальным счетом. В частности, на виртуальном счету хранится экспозиция виртуального счета, которая равна наибольшей раскрытой в платежах диспозиции платежной книжки с данным P. Кроме того, на виртуальном счету хранится сумма всех расходов, произведенных при помощи соответствующей книжки. Список виртуальных счетов является аналогом списка использованных монет в монетной системе Чаума.

Рассмотрим теперь операцию платежа. Предположим, что плательщик имеет в своем распоряжении платежную книжку PayBook (N, P). В общем случае в качестве платежа плательщик отсылает продавцу следующие данные:

{Order, Y, PayBook(n, P)},

где n J N, а Y и Order описаны выше. Продавец пересылает эти данные в банк, который, в свою очередь, проводит авторизацию платежа следующим образом:

1. Банк проверяет необходимое условие (3) корректности предъявленной платежной книжки. Если необходимое условие не выполнено или если n = 0, то банк отказывает в авторизации платежа.

2. Банк разыскивает виртуальный счет, соответствующий P. Если счет не найден, то есть если платежная книжка с ключом P никогда ранее не предъявлялась, то банк создает его и устанавливает экспозицию виртуального счета равной n, а сумму расходов приравнивает нулю.

3. Если экспозиция виртуального счета меньше n, то банк устанавливает экспозицию виртуального счета равной n.

4. Банк проверяет корректность платежа. Если равенство (2) не выполнено, то банк отказывает в авторизации платежа.

5. Если расходы виртуального счета вместе с величиной данного платежа не превосходят n, то банк увеличивает расходы виртуального счета на величину платежа и авторизует платеж; в противном случае - отказывает в авторизации платежа.

Если авторизация прошла успешно, то банк зачисляет на счет продавца нужную сумму и отправляет плательщику и продавцу подписанные квитанции, включающие Order.

Если плательщик уверен, что экспозиция виртуального счета, соответствующего платежной книжке PayBook(N, P), достаточна для проведения планируемого платежа, например, если в предыдущей квитанции банк сообщил экспозицию виртуального счета, то плательщик может отправить в качестве платежа сокращенные данные

{Order, Y, P}.

Авторизация в этом случае происходит с очевидными модификациями.

Заметим, что величина платежа может принимать фактически произвольные значения и не обязана быть кратной минимальной единице съема денег на книжку, которая равна g-1(f(P)). Например, снимать на книжку можно только целое число центов, но при этом иметь возможность заплатить 2.718 цента.

Описанную схему можно очень грубо охарактеризовать как систему анонимных счетов с возможностью непрослеживаемого перевода денег (обязательств) с одного счета на другой. Так как виртуальный счет, как правило, обслуживает много платежей, то список виртуальных счетов растет значительно медленнее, чем соответствующий список использованных монет в системе Чаума.

Очевидно, что все платежи, проведенные с помощью одной платежной книжки, легко могут быть связаны банком друг с другом через общий виртуальный счет. Это представляет некоторую угрозу для анонимности клиента, так как если один из платежей клиента будет атрибутирован внешними по отношению к системе средствами, то тогда и вся платежная история клиента, связанная с данной платежной книжкой, может быть раскрыта. Для уменьшения этой угрозы клиент может прерывать свою платежную историю, открывая новые платежные книжки и прекращая использовать старые. Кроме того, по истечении срока действия книжки ее платежная история заканчивается. Как часто следует клиенту прерывать свою платежную историю и сколько платежных историй иметь одновременно, зависит от его мнительности и от расценок, установленных банком для различных операций. Высокая стоимость открытия виртуального счета и/или высокая стоимость съема денег на книжку стимулирует среднего пользователя использовать одну и ту же платежную книжку для большего числа платежей, не закрывая полностью, однако, возможность для мнительного пользователя ограничивать количество платежей, проведенных с одной книжки. Кроме того, взимание банком платы за открытие виртуального счета защищает его список виртуальных счетов от переполнения, так как каждое место в этом списке оплачивается, а также предоставляет банку дополнительный источник дохода.

Обсудим теперь вопрос связываемости платежной книжки (виртуального счета) со счетом, с которого деньги были переведены на эту книжку. Технология слепой подписи, используемая при пополнении платежной книжки, гарантирует лишь несвязываемость счета с книжкой в сеансе пополнения. Однако книжка может быть косвенно связана банком со счетом иными средствами, например по Интернет-адресу их владельца. Банк может также пытаться связать книжку со счетом путем анализа общей суммы денег, переведенных на платежную книжку. Однако этот косвенный способ связывания в значительной степени затруднен тем, что одна и та же платежная книжка может пополняться с разных счетов, и тем, что при платеже владелец платежной книжки не раскрывает банку сразу всю сумму N платежной книжки PayBook(N, P). Кроме того, в

платежную систему PayCash легко может быть встроен слегка модифицированный механизм слепого возврата сдачи Чаума, который может быть использован для реструктуризации сумм на платежных книжках, и в частности для перевода на свежую платежную книжку остатка денег с книжки, предназначенной для удаления, что еще больше уменьшает возможность связывания книжки со счетом.

Таким образом, подход, избранный для построения платежной системы PayCash, обеспечивает разумный уровень непрослеживаемости платежей.