*Министерство общего и профессионального образования*

*Сургутский Государственный Университет
кафедра финансов, денежного обращения и кредита*

***Курсовая работа***

***по дисциплине «Деньги. Кредит. Банки.»***

***«Современные платежные системы»***

*Выполнил: Ляшенко А.В.*

*Экономический факультет, группа 371*

*Принял: Микитюк А.М.*

*Сургут 2000*

***Реферат***

**Исполнитель:** *Ляшенко Андрей Владимирович.*

**Количество:**

* страниц 43
* иллюстраций и таблиц 1
* использованных источников 10

**Название курсовой работы:***«Современные платежные системы».*

В предлагаемой работе дан краткий обзор существующих на сегодняшний день типов современных банковских платежных систем, рассмотрены некоторые из существующих на сегодня реализаций, как российских, так и зарубежных. Особое внимание уделено проблемам безопасности, сопутствующих их внедрению и промышленной эксплуатации.

***Оглавление***

1. Введение 4

2. Системы удаленного управления банковским счетом 6

2.1. История появления и современные реализации 6

2.2. Безопасность 11

3. Платежные системы на пластиковых картах 12

3.1. Виды платежных систем, этапы их развития. 12

3.2. Проблемы внедрения и функционирования системы пластиковых карт 17

4. Цифровые наличные деньги 26

4.1. Общие сведения 26

4.2. Западные реализации 27

4.3. Отечественные реализации. 31

4.4. Безопасность. 35

5. Правовой статус платежных систем 37

Источники 43

# 1. Введение

В последнее время банки все больше и больше используют в своей деятельности современные технологии. И, как всякие сложные системы, они наряду с полезными возможностями предоставляют массу путей для манипулирования ими в корыстных целях. Уже сейчас кражи с помощью электронных средств в США наносят годовой ущерб, измеряемый десятками миллиардов долларов. Причем, действительные цифры ущерба тщательно скрываются всеми причастными, поскольку это может повредить репутации банка.

Развитие экономики любого государства сегодня невозможно без высокоэффективной системы денежного обращения и использования современных платежных механизмов. Платежный механизм – структура экономики, которая опосредует "обмен веществ" в хозяйственной системе. Методы платежа делятся на наличные и безналичные. Безналичные расчеты постепенно вытесняют налично-денежные платежи в денежных системах различных стран. Основная доля проведения безналичных расчетов приходится на коммерческие банки. Именно им принадлежит важнейшая расчетно-платежная функция в платежной системе государства.

Современные платежные системы позволяют банку расширять сферу услуг, охватывая бездоходные для него наличные операции и переводя их в доходные для себя безналичные.

В предлагаемой работе дан краткий обзор только маленькой части айсберга – современных банковских платежных систем и сопутствующих их внедрению и промышленной эксплуатации проблем, связанных с безопасностью.

Платежные системы, создаваемые коммерческими банками, можно подразделить на:

* Системы удаленного управления своим банковским счетом;
* Системы, построенные на использовании пластиковых карт;
* Совсем новые системы, построенные на цифровых наличных деньгах, платежи по которым проходят через Интернет.

Российская банковская система смело перешагнула через многие этапы развития банковских систем западных стран, и в настоящее время уровень автоматизации отдельных российских банков значительно превосходит западный[[1]](#footnote-1). Для организации систем передачи информации о платежах и расчета по ним в России были применены наиболее прогрессивные (из возможных) технологий. Особенно явно это проявилось в создании платежных систем построенных на использовании пластиковых карт, которые более подробно будут рассмотрены в последующих главах.

# 2. Системы удаленного управления банковским счетом

## 2.1. История появления и современные реализации

Рассмотрим коротко первую группу – системы удаленного управления банковским счетом. Они могут быть реализованы без применения средств вычислительной техники. Клиент звонит в банк оператору, представляется и говорит, что хотел бы перевести такую-то сумму со своего счета на счет магазина, в котором заказал себе костюм. Вместо оператора на другом конце провода может быть голосовая система, которая управляется клавишами на телефоне.

Впервые подобная услуга начала применяться в 1983 г. Систему HomeLink, созданную совместно с Банком Шотландии и телефонной компанией British Telecom, внедрило строительное сообщество Notingham Building Society. Популярность этих услуг выросла в 1994 г. До 35% всех банковских транзакций по частным вкладам в США приходилось на автоматизированные системы ответа на телефонные запросы.

Как вариант, подобная система может быть реализована с помощью персонального компьютера и модема. Клиент получает возможность осуществлять банковские операции круглосуточно без выходных и праздничных дней. Среди операций можно выделить следущие:

* Получение баланса счета на текущий момент;
* Ознакомление с деталями инструкций и правил;
* Возможность заказа чековой книжки и отчета о движении средств на счете за определенный промежуток времени;
* Выполнение операций с ценными бумагами. [1]

Развитию рынка электронных банковских приложений способствуют распространение недорогих ПК и сетевых устройств, а также дальнейший рост числа пользователей Интернет. По данным IDC, перед рынком электронных банковских приложений — неплохие перспективы развития. В 1998 г. онлайновые банковские операции проводили 6.6 млн. клиентов, а в 2003 г. таких пользователей должно быть уже более 32 млн.

Электронные банковские приложения привлекательны для банков, рассчитывающих увеличить свои прибыли за счет новых клиентов (в первую очередь удаленных). По данным IDC, объем продаж электронных банковских приложений в США в 1998 г. составил $93 млн. Все большее количество банков предлагают своим клиентам услуги Интернет банкинга. По оценке IDC, число таких банков должно увеличиться с 1150 в 1998 г. до 15845 в 2003 г. Более 1200 банков и кредитных объединений США в 1998г. подписали соглашения с производителями и провайдерами услуг Интернет банкинга об открытии сайтов с выполнением всех видов транзакций. В 1999 г. число таких желающих превысило 7200. По оценке IDC, в 2000 г. приложения Интернет банкинга займут почти треть всего рынка банковских приложений в США. По данным компании Gomez Advisors (специализирующейся на исследовании деятельности банков, финансовых организаций и брокерских фирм) 39 из 100 ведущих банков США уже предоставляют онлайновые услуги по оплате счетов (в 1998 г. таких банков было 17). 62% опрошенных банков предоставляют по Интернет информацию о совершении транзакций в реальном времени. Следует отметить, что банки используют любые возможности для получения прибыли с помощью современных технологий. Например, Deutshe Bank уже начал торговать акциями через Интернет.

Развитие приложений Интернет банкинга должно пройти три основных этапа. На первом этапе предусматривается доступ клиентов к банковским счетам и проведение транзакций по телефону или через Web-браузер. На втором этапе используются такие интерактивные технологии, как сервисы онлайновой оплаты счетов и персонализированного напоминания о состоянии счета клиента. На третьем этапе предлагаются такие функции управления личными финансами, как возможность кредитования, совершения безопасных торговых сделок и оформления страховок.

По мере дальнейшего развития рынка электронных банковских услуг клиенты смогут вообще не приходить в банк. Они смогут открывать счет, переводить деньги, оплачивать товары и услуги прямо из дома, офиса или магазина, используя для этого ПК или терминал для приема кредитных карт. Наличные они могут снимать в банкомате. Примером процветающего Интернет-банка может служить американский Security First Network Bank. У него даже нет офиса для обслуживания клиентов, и при этом их число ежегодно увеличивается. За счет экономии на арендной плате и прочих издержках он предлагает своим клиентам весьма конкурентоспособные условия обслуживания и, тем самым, привлекает их. В настоящее время в Западной Европе (Германии, Испании, Франции, Нидерландах) электронных банков в 2 раза больше, чем в США.

Наивысшим рейтингом у потребителей за качество предоставляемых онлайновых услуг пользуются следующие банки: Security First Network Bank; Wells Fargo Bank; Citibank; Salem Five Cents Saving Bank; Bank of America[[2]](#footnote-2).

Функции, выполняемые системами, можно разделить на группы:

* Платежные (передача в банк платежных поручений по списанию средств со счетов клиентов);
* Справочно-информационные (получение выписок по счетам, получение электронных документов, информация о курсах валют, получение текущего баланса);
* Почтовые и специализированные (прием/передача почтовых сообщений, требующих ручной обработки со стороны банка, заказ на покупку/продажу валюты на бирже).

В России подобные системы не очень распространены по разным причинам. Из примеров конкретных реализаций можно назвать системы «Телебанк» и «Интернетбанк».

Система «Телебанк» создавалась в 1997г. как система дистанционного обслуживания клиентов ГУТА БАНКА. Основной целью являлось создание для клиентов удобных механизмов оплаты телекоммуникационных и иных счетов. Система ориентирована на использование частными лицами. Доступ возможен по телефону через оператора, через круглосуточную интерактивную службу и через Интернет. Счета до востребования открываются в рублях, долларах США, немецких марках, фунтах стерлингов, евро.

В системе «Телебанк» в настоящее время обслуживаются только частные лица. Клиент осуществляет предварительное оформление по телефону или интернет. Для завершения оформления и заключения договора Клиент посещает офис ГУТА БАНКА.

Клиенты могут не посещая банк:

* Делать все коммунальные платежи (электроэнергия, газ, телефон, кварт­плата, теплоснабжение и др.);
* Оплачивать счета за связь – межгород (ММТ), МТС, БИ ЛАЙН, МСС, СОНЕТ, Мобил Телеком, МТУ Интел, ПТТ Телепорт, Элвис–Телеком и др.;
* Производить оплату услуг – спутниковое телевидение (НТВ+, Космос ТВ), охрану, стоянку, домофон, обучение и др.;
* Переводить средства в оплату счетов за товары, в том числе, купленные через Интернет-магазины;
* Производить денежные переводы, в том числе, в иностранной валюте;
* Покупать и продавать иностранную валюту;
* Размещать средства в срочные вклады со счета в системе «Телебанк»;
* Пополнять свои пластиковые карточки со счета в системе «Телебанк»;
* Переводить средства с пластиковых карточек на счет в системе «Телебанк»;
* Подписываться на газеты и журналы;
* Получать по факсу и через Интернет выписки по счетам и пластиковым карточкам;
* Получать на счет в Системе «Телебанк» денежные переводы, в том числе,
перечисление заработной платы.

Интернетбанк – традиционная система для предоставления он-лайн управления счетом с базовыми возможностями.

Система Интернетбанк, разработана банком «Северная казна» ОАО, пробная эксплуатация – лето 1999, альфа-тестирование – сентябрь, октябрь 1999, 20 ноября 1999 – сдача системы в бета-тестирование, работают 3 клиента. 20 января 2000 начата промышленная эксплуатация системы. На настоящее время заключено около 100 договоров на пользование системой. С помощью системы Интернетбанк можно управлять одним или несколькими расчетными счетами через Интернет.

Используя Интернетбанк возможно:

* Получать выписки о состоянии счета за определенный период;
* Получать информацию (номер платежа, сумма, от кого он поступил, с каким назначением, все реквизиты плательщика) о поступивших платежах в режиме реального времени;
* Получать информацию об отправленных платежах (оплачены ли они). В случае отказа в оплате можно узнать причину отказа;
* Отказаться от неоплаченного платежа;
* Проводить платежи партнерам, формировать платежные документы в любое время дня и ночи;
* Платить по заранее заведенным платежам (коммунальные, оплата за услуги в Интернет-магазинах);
* Переводить деньги на карт-счет;

Расчеты в таких системах осуществляются путем передачи клиентом в банк электронных платежных документов, заверенных цифровой подписью, которая обеспечивает идентификацию отправителей документов и защищает от несанкционированного изменения. Электронные документы, применяемые в системе, идентичны финансовым платежным документам, используемым в соответствии с нормативными актами Центрального Банка и являются основанием для осуществления бухгалтерской деятельности. Для обеспечения безопасности и конфиденциальности расчетов используется шифрование электронных документов по стандарту DES либо ГОСТ 28147-89.

## 2.2. Безопасность

Взглянув на эти системы с другой стороны можно обнаружить, что единственное препятствие для несанкционированного доступа – механизм идентификации пользователя. Обычно он происходит с помощью паролей. Если пароль передается голосом или с помощью тонального набора на телефоне, то он элементарно подслушивается с помощью «жучка» или с помощью улавливания побочного излучения от кабелей. На девочку-оператора можно оказать давление вне ее рабочего места. Наконец, можно позвонить клиенту домой и от имени администрации банка попросить его продиктовать свой пароль якобы для проверки системы. Много ли людей что-то заподозрит?

Наиболее защищенным в этом плане можно считать доступ с помощью специализированного терминала или персонального компьютера, когда можно прозрачно для пользователя менять пароли и ключи шифрования хоть каждый сеанс. Однако, злоумышленник может проанализировать достаточно большой объем переданных и принятых данных, реконструировать протоколы обмена и получить незаконный доступ. Протоколы обмена в системах, реализованных на базе спецтерминалов, обычно нестандартны и разработаны по заказу банка. Фирмы-разработчики, стремясь «привязать» банк к своей системе, делают их несовместимыми друг с другом. Поскольку эти фирмы обычно не располагают достаточными ресурсами для проведения всестороннего тестирования своей продукции, она несовершенна в плане защиты от несанкционированного доступа.

При реализации систем на базе обычных персональных компьютеров становится возможным использовать стойкую криптографию и электронную цифровую подпись без существенного удорожания системы но появляются другие возможности для проведения операций со счетом без ведома владельца. Например, клиенту могут прислать по электронной почте вирусную программу, которая по той же электронной почте перешлет злоумышленнику все пароли, номера счетов и подобную секретную информацию. Изображение на мониторе может быть получено с помощью улавливания побочного излучения от соединительных кабелей и самих устройств. К компьютеру может получить доступ посторонний. Все это затрудняет распространение подобных систем.

# 3. Платежные системы на пластиковых картах

## 3.1. Виды платежных систем, этапы их развития.

Пластиковые карточки, точнее их прообраз появились в США, традиционной стране потребительского кредита. Еще в 1914 г. крупные универмаги стали здесь выдавать кредитные карточки своим клиентам. В 1928 г. был изобретен прообраз пластиковых карточек – металлический ярлык, на котором было выдавлено имя и адрес клиента. В 1936 г. появилось первое объединение предприятий, согласившихся кредитовать общих клиентов. Особый успех выпал на долю ресторанной кредитной карточки “Diners Club”. Постоянные посетители ресторанов, имеющие хорошую репутацию, могли получить карточку “DC” и предъявлять ее во многих ресторанах Нью-Йорка вместо наличных денег. Рестораны передавали копии счетов в “DC”, который ежемесячно выставлял клиенту общий счет. Клиент расплачивался с “DC”, а тот – с ресторанами.

Ряд крупных американских банков, оценив успех первооткрывателей, выпустили свои кредитные карточки. Так, начали образовываться платежные системы: банк выпускал карточку и открывал счет клиенту; на территории страны и за рубежом создавалась целая сеть магазинов, баров, ресторанов, отелей и т.д., где принимали к оплате карточки, выпущенные банком-эмитентом, оборудовался центр, который занимался обслуживанием пластиковых карточек. Первопроходцами в освоении рынка пластиковых денег были известные ныне всему миру Bank of America; Master Card; American Express; Visa International.

Успех использования небумажных платежных средств объясним тем, что:

1. Они более защищены от подделки, что позволяет их использовать в более широкой сфере расчетов и с большим количеством участников;
2. Клиенты видят в них более удобную форму расчетов и позволяют широко использовать кредит в повседневной практике;
3. Заинтересованность появляется у торговых точек, которые с согласием принимать, как платежное средство, карточки расширяют круг своих клиентов;
4. С позиций государства использование платежных систем снижает стоимость обслуживания наличной массы, ускоряет оборачиваемость денег.

Основной сферой применения систем, построенных на пластиковых картах, является розничный товарооборот.

В ходе развития платежных систем возникли разные виды карт, различающихся назначением, функциональными и техническими характеристиками.

Различают *кредитные* и *дебетовые* карточки. Первые связаны с открытием кредитной линии в банке, что дает возможность владельцу пользоваться кредитом при покупках товаров. Вторые предназначены для получения наличных денег в банковских автоматах или покупки товаров с расчетом через электронные терминалы. Деньги при этом списываются со счета владельца карточки в банке в пределах остатка.

*Карточки туризма развлечений и отдыха* выпускаются компаниями, специализирующимися на обслуживании указанной сферы (American Express, Dinners Club). Карточки принимаются сотнями тысяч в торговых и сервисных предприятий во всем мире для оплаты товаров или услуг, а также предоставляют владельцам карт различные льготы при по бронированию авиабилетов, номеров в гостиницах, получению скидках с цены товара, страхованию жизни и т.д.

*Карточки для банковских автоматов* (ATM cards). Это разновидность дебетовых карточек, которые дают возможность владельцу счета в банке получать наличные деньги в пределах остатка средств на счете через автоматические устройства, установленные в банках, торговых залах и т.д.

*Карточка для покупки через терминалы в торговых точках*. Карты этого вида также относятся к разряду дебетовых. Они “привязаны” к чековому или сберегательному счету владельца карточки и не предусматривают автоматического предоставления кредита. Карта выполняет функции банковского чека, однако, ее применение более надежно, так как идентификация владельца производится в момент совершения сделки и деньги перечисляются на банковский счет торгового предприятия немедленно.

Еще одна классификация кредитных карточек связана с их технологическими особенностями. Наиболее распространены карточки двух видов – с магнитной полосой и со встроенной микросхемой, т.н. смарт-карты.

Карточки с магнитной полосой имеют на обороте магнитную полосу, где записаны данные, необходимые для идентификации личности владельца карточки при ее использовании в банковских автоматах и электронных терминалах торговых учреждений. Когда карточка вставлена в терминал, индивидуальные данные владельца передаются по коммуникационным сетям для получения разрешения на осуществление сделки.

Карты с микросхемой была изобретена во Франции в 1974 г. и получили большое распространение в этой стране и за рубежом. Встроенная в нее микросхема является хранителем информации, которая записывается заранее, а затем может обновляться в момент совершения сделки. Она же может производить некие внутренние вычисления. Это расширяет функциональные возможности карточки и повышает ее надежность.

На основании записанных в чипе сведений сделка по карточке может осуществляться в автономном режиме (off-line), т.е. без непосредственной связи с центральным процессором банковской компьютерной системы в момент совершения операции. Поскольку карточка сама хранит в памяти сумму средств, имеющихся на банковском счете, то авторизации здесь не требуется: если лимит превышен, сделка просто не состоится. Если же сумма операции меньше суммы лимита, то в момент ее совершения сумма свободного лимита будет уменьшена и записывается новый остаток, который может быть использован при следующей покупке. При внесении денег на счет лимит восстанавливается, о чем делается новая запись в микросхеме.

Информационные возможности смарт-карт гораздо шире чем, у карточек с магнитной полосой. Кроме того, достоинством ее является возможность оперативного обновления данных в памяти микропроцессора. Наконец, важным достоинством карточки является ее более высокая надежность. К недостаткам стоит отнести относительно высокую стоимость (в 5-7 раз выше по сравнению с магнитной карточкой).

В настоящее время платежные системы переживают модернизацию технологий расчетов, которая заключается в переходе с пластиковых карт на магнитном носителе, на смарт-карты. Причина модернизации состоит в технологических преимуществах этих карт и возможности расширения сферы использования платежных систем.

На российский, точнее советский рынок пластиковые деньги пришли в конце 60-х годов. Первые пластиковые карты были от Diners Club International. Представители этой системы подписали с Госкомимуществом в лице ВАО "Интурист" агентское соглашение на обслуживание в СССР этой платежной системы. В 1974 году аналогичное соглашение было подписано с Visa International, в 1975 году с Evrocard, Master Card. Обслуживались по пластиковым карточкам исключительно иностранцы.

Перемены, начавшиеся в нашей стране в середине восьмидесятых годов и ознаменовавшие собой начало приобщения банковской системы к западным стандартам, создали почву для появления современных пластиковых карточек. В начале девяностых годов за освоение рынка пластиковых карт взялись российские коммерческие банки. В сентябре 1991 года “Кредобанк”, принятый в члены Visa International, начал эмиссию карточек VISA в России. Затем программы по выпуску карточек VISA в России начали осуществлять “Мост-банк”, “Инкомбанк” и “Мосбизнесбанк”. А обслуживал платежи процессинговый центр "Интуркредиткард" (39% акций которого принадлежали “Кредобанку”).

 Через некоторое время “Кредобанк”, “Мост-банк” и “Диалог-банк” учредили другой процессинговый центр – “Кардцентр”. Однако вскоре “Кредобанк” отделился от “Кардцентра” и учредил АО United Card Service с русским вариантом названия “КОКК - Компания объединенных кредитных карточек”.

В апреле 1992 года на российском рынке появилось АО "СТБ КАРД", учрежденное банком "Столичный", которое в январе 1993 года выпустило первую отечественную пластиковую карточку STB CARD.

Одной из коммерческих структур, активно занимающихся развитием услуг, связанных с внедрением электронных платежей, является “Мост-банк”. В июне 1992 года им были выпущены первые карточки "Еврокард-Мастеркард". В январе 1993 года была эмитирована карточка VISA. Затем появилась дебетовая карточка самого "Моста". Чуть позже "Мост-банк" стал акционером “КОКК” (49% акций). А в феврале 1995 года группа “Мост” ввела в строй процессинговый центр "Мультикарта", который сертифицирован сразу двумя системами - "Визой" и "Еврокард-Мастеркард", и занимается как выпуском пластиковых карт, так и их обслуживанием.

Третьим расчетным центром, обслуживающим в основном карточки American Express, стала компания “American Express (Russia) LTD”. Среди российских карточек, следует отметить, прежде всего, Union Card (эмитенты "Автобанк", "Инкомбанк") и СТБ-кард (банк "Столичный").

Опыт и сильные стороны карточной технологии на магнитном носителе, успешно используемых западными банками и компаниями, активно используется российскими коммерческими банками, для развития карточного дела, отдача от которого в полной мере будет позднее.

Россия, находившаяся в изоляции от мировых платежных систем вплоть до 90-х годов, получила уникальный шанс миновать технически не совершенный вариант организации платежных систем построенных на пластиковых картах, использующих в качестве носителя информации магнитную полосу. Речь идет о проектах внедрения на внутри российском рынке смарт-карт. Первые российские публикации, посвященные смарт-картам как платежному средству стали появляться в 1992 году.

В последние время все чаще в банковских кругах возникает вопрос о создании национальной платежной системы, построенной на смарт-картах. VISA проявляет в этом вопросе завидную бойкость. VISA в сентябре 1996 года объявила о создании в России масштабного проекта COPAC по введению в обращении универсальной платежной микропроцессорной VISA карточки. Первоначально VISA планировала создание пилотного проекта на базе Инкомбанка. Но на фоне этого VISA вела переговоры с Сбербанком, который на сегодняшний день уже имеет платежную систему по поводу ее сертификации. Желание VISA проникнуть в данный сектор рынка говорит о его перспективности. Оценка стратегии VISA неоднозначна: с одной стороны создание такой системы, лидером в карточном бизнесе, обеспечит совместимость национальной системы с международной; с другой стороны, остро встает вопрос распределения доходов и размещения страховых депозитов.

## 3.2. Проблемы внедрения и функционирования системы пластиковых карт

Верьте брахману больше, чем змее,
а змее – больше, чем шлюхе, а шлюхе – больше, чем афганцу.

Р.Киплинг. «Ким».

Переход на новые, более надежные системы в западных странах замедляется и откладывается из-за огромных капиталовложений, которые банки в свое время сделали в традиционную, существующую сегодня технологию магнитных карт, инфраструктуру из сотен тысяч банкоматов, миллионов торговых терминалов и специализированных высококачественных сетей передачи данных. Эти системы отлажены, работают, а потери, связанные с мошенничеством, статистически вычисляются и учитываются как неизбежные эксплуатационные издержки.

Ситуация на Российском рынке абсолютно иная. С одной стороны, очень низкая кредитоспособность массового клиента, отсутствие высококачественных разветвленных и надежных средств коммуникаций (особенно на периферии) и высокий уровень криминальности делает практически невозможным применение стандартных западных систем в национальном масштабе. С другой стороны, находясь на начальном этапе своего развития, российские системы имеют уникальную возможность использовать все последние технологические достижения. Вот почему количество поставщиков платежных систем на Российском рынке столь велико. Многие из этих фирм, реально оценивая ситуацию, предлагают только микропроцессорные карты в качестве базового элемента систем.

 Кроме того, и крупнейшие международные системы (VISA, EUROPAY и др.) перестраивают свою маркетинговую политику по мере осознания того факта, что борьба за будущий стандарт платежных систем уже развернулась и полигоном для этой борьбы становится российский рынок.

Оценка рисков – важный критерий при выборе платежной системы. Как и любая деятельность банка, создание и функционирование системы безналичных расчетов несет на себе определенные риски.

Общие риски функционирования платежной системы возникают из-за возможных технических отказов и возможностью хищения денежных средств банка или клиента. Другими словами природа данного риска лежит в области технических особенностей работы системы. Величина данного риска довольно значительна на сегодняшний день. Основная доля убытков от данного риска приходится на хищения. Крупные платежные системы закладывают в свои бюджеты расходные статьи с учетом возможных убытков от хищений, рассчитанные статистически на основе прошлых периодов. По данным зарубежных источников, потери от преступлений в сфере оборота банковских пластиковых карт составляют в среднем 10 % от прибыли. Причем, в последнее время отмечается рост таких потерь.

По данным опроса, проведенного Computer Security Institute (CSI) и FBI Computer Intrusion Squad (обработаны ответы 643 компьютерных специалистов из 273 американских корпораций, финансовых институтов, правительственных агентств и университетов), 90% респондентов отметили, что претерпели то или иное нарушение системы безопасности в 1997 году, ставшее результатом хакерских атак. 74% респондентов заявили, что понесли убытки в результате хакерских атак, но только 42% были в состоянии подсчитать все убытки.

По данным комитета Europay Int. по рискам и мошенничествам, потери европейских банков (в том числе и российских) от мошенничеств с пластиковыми картами за последний год выросли в десятки раз. По приблизительным подсчетам, в 1998 году они составили около $15 млрд.

Europay Int. пока не сообщает конкретных цифр о потерях банков. Но их легко подсчитать: согласно опубликованным в предыдущие годы данным, общие потери банков от деятельности карточных мошенников во всем мире составляли $600 млн. в год. Теперь же эта цифра выросла примерно в 25 раз. Причем, владельцы платежных систем не расположены обнародовать свои потери от обслуживания системы, боясь подорвать доверие к ней.

В России потери от действий мошенников по всем кредитным карточкам в 1996 г. оценивались в $2,3 млн., в т.ч. $90 тыс. – потери по карточкам Eurocard/MasterCard. Особая опасность таких преступлений состоит в высокой степени их латентности. Выявляется только одно из десяти криминальных проявлений

Самым распространенным мошенничеством (87%) в настоящее время является подделка карт. До 30 видов незаконных операций с картами осуществляется через Интернет. Например, оплата покупок несуществующими картами, создание фальшивых виртуальных магазинов и пр.

Хищения происходят как сторонними лицами, так и персоналом платежной системы. Персонал вообще является самым ненадежным, а часто просто опасным звеном любой автоматизированной системы. Нелояльные сотрудники, имеющие доступ к компьютерам, играют главную роль в большинстве финансовых преступлений. Статистика приводит очень печальные данные, утверждая, что лишь четверть сотрудников банка вполне лояльна. Четверть настроена безусловно враждебно к фирме и не имеет моральных ограничителей, лояльность же оставшейся половины зависит исключительно от обстоятельств. Процедуры безопасности могут обеспечить проверку паролей и строгий контроль доступа к ценным общим данным, но взломщика, хорошо знающего внутреннее устройство системы, практически невозможно остановить. Уволенные служащие иногда пытаются разрушить систему и оборудование. Известен случай, когда уволенный служащий воткнул сетевой коаксиальный кабель в электрическую розетку, чем вывел из строя полсотни компьютеров. В другом происшествии из окна в реку был выброшен файловый сервер. Даже законопослушные пользователи часто нарушают правила работы в сетях. Это проявляется в неправомочном использовании чужого компьютера, просмотре, копировании или модификации чужих файлов, а также преднамеренном саботаже чужих программ и вызове крушения или перезагрузки системы. Наиболее серьезный вид нелояльности можно ожидать от программистов, чьи модули, установленные в защищенной системе имеют неописанные в документации возможности.

Сторонние лица также проявляют хороший уровень знаний и изобретательности. Преступники действуют с размахом. Ими создаются фирмы прикрытия, “хакерские братства”, подпольные корпорации для совершения мошенничеств с помощью пластиковых карт. На “вооружении” таких преступных формирований находится самая современная техника, необходимые документы прикрытия, в них входят наиболее квалифицированные специалисты. Для осуществления преступной деятельности создаются фиктивные предприятия, банки, для затруднения работы налоговых и иных контрольных органов используются зарубежные оффшорные счета.

Примером может служить разоблачение фирмы, которая занималась оказанием посреднических услуг в оформлении карт зарубежных платёжных систем. Мошенники открывали корпоративный счёт (которым могут пользоваться несколько человек), выдавая его клиенту за индивидуальный. В нужный момент, когда ничего не подозревающий владелец, убедившись в том, что карта нормально функционирует в нашей стране и за рубежом, переводил на свой счёт крупную сумму денег, преступники, обладающие равными правами, распоряжались её по своему усмотрению.

Совместными усилиями сотрудников МВД, ФСБ и службы безопасности Сбербанка удалось пресечь преступную деятельность группы мошенников, пытавшихся похитить 1,5 млрд. рублей через банкоматы отделений Сбербанка в Перми, Москве и Санкт-Петербурге.

Работниками органов внутренних дел и службой безопасности банка “Российский кредит” выявлена группа лиц, пытавшихся выпустить пластиковые карты с реквизитами вышеназванного банка и использовать их в Южной Америке и Азии.

В сентябре 1997 года в Санкт-Петербурге были задержаны лица, пытавшиеся получить мошенническим путем в “Международном банке реконструкции и развития” 75 тысяч долларов США.

На сегодняшний день из известных видов мошенничеств “лидирует” полная подделка карты. Обычно, на ней указываются подлинные реквизиты, довольно точно воспроизводятся степени защиты, но фамилия владельца фиктивна. Этот вид мошенничества распространяется по миру со скоростью эпидемии. Первыми подделывать карты начали в Нигерии, но там поднять этот вид мошенничества "на должную высоту" не смогли, не хватило технологий. Миниатюрные устройства для копирования магнитной полосы, которые могут помещаться в ладони, были изготовлены уже в Восточной Европе. Скажем, владелец карты при посещении ресторана может даже не заметить, в какой момент с карты, находящейся в руке официанта, была считана магнитная полоса. Часто применяется установка в банкоматы специальных устройств, которые сохраняют в своей памяти и передают злоумышленникам данные с карты вкупе с введенными пользователями пин-кодами. Многие карты с магнитной полосой (включая, например, карты для проезда в Московском метрополитене) копируются вообще «на коленке» с помощью утюга, куска магнитной ленты от видеокассеты и мелких железных опилок.

Затем следуют преступления, которые можно объединить в группу “незаконное использование подлинной карточки”. Сюда можно отнести банальную кражу карты с последующими операциями по ней, так называемую “двойную прокатку” (когда продавец откатывает слип несколько раз, оставляя себе незаполненные экземпляры. Известны случаи, когда мошенники (в основном работники банков и фабрик по производству карт) пользуются задержкой между изготовлением и вручением её владельцу.

Совершают мошенничества и сами владельцы карт. Наиболее часто карта заявляется ими как украденная, после чего незамедлительно следуют операции (пока номер карты не попал в “стоп-лист”). Затем недобросовестный клиент предъявляет претензии банку. Также для избежания снятия денег со счёта карты частично подделывают, изменяя реквизиты путём физического воздействия.

Работниками торговли и других сфер обслуживания используется так называемый “белый пластик” (суррогат карты) с последующим “замыванием” (маскировкой) фальшивых слипов среди подлинных.

С развитием глобальной компьютерной сети Интернет и появлением “виртуальных магазинов”, где можно сделать заказ с персонального компьютера, получив товар по почте, расширилось поле деятельности для мошенников. Для оплаты в таких магазинах достаточно указать реквизиты карты. Следовательно, любая утечка такой информации (а это может произойти при любой операции) чревата для владельца большими потерями. А способов “выманить” у владельца реквизиты карты существует множество. Сейчас уже известно около 30 приёмов мошеннических действий с помощью Интернет, который в настоящее время находится, фактически, вне правового поля. Даже если магазин не преследует цели присвоить себе ваши деньги, номер карточки (и еще сотни тысяч других, накопленных в его базе данных) у него вполне могут украсть. Недавно в Интернет прошло сообщение о том, что у одного из крупных онлайновых магазинов были украдены 485 тыс. номеров карточек. Они были спрятана на веб-сайте одного из ведомств правительства США. Это тайное хранилище похищенных данных было обнаружено в ходе аудиторской проверки еще в январе 1999 года, но за прошедшее с тех пор время оповещенные финансовые институты не только не закрыли счета скомпрометированных кредитных карт, но даже не известили владельцев карт о происшедшем.

Российский хакер под кличкой Maxus внедрился в базу данных компании CD Universe, содержащей порядка 350.000 записей о клиентах и номерах их кредитных карточек. Он потребовал у компании $100.000 за неопубликование информации, и после того, как CD Universe отказалась, информация была опубликована на веб-сайтах. Через некоторое время ФБР обнаружило и закрыло сайты с этой информацией. Вскоре была установлена его личность. ФБР имеет достаточно данных и доказательств для ареста, однако вопрос об этом пока не решен до договоренности с российскими властями[[3]](#footnote-3).

Компания Expedia, ведущее интернет-агентство путешествий, заявила о том, что на третий финансовый квартал она запланировала увеличить средства, зарезервированные на убытки из-за поддельных кредитных карт. Если раньше этот резерв составлял около $500 000, то теперь он составит от $4 млн до $6 млн. Увеличение резерва связано с ростом числа мошеннических онлайновых операций с использованием поддельных кредитных карт. В минувшем квартале компания понесла из-за этого убытки, объем которых составляет около трети доходов, полученных от продажи билетов[[4]](#footnote-4).

По крайней мере 9 сайтов были взломаны хакерами с января этого года с целью воровства номеров кредитных карточек. Счёт ворованных номеров ведётся на сотни тысяч, причём большинство из них были размещены на хакерских сайтах. Как сообщает администрация сайтов-жертв, взлом стал возможен из-за "дыры" в ПО Microsoft Internet Information Server, которое предоставляет доступ к записям о клиентах и сделках.

Смарт-карты являются на сегодняшний день самым надежным вариантом пластиковой карты. Установленный на ней процессор может обладать весьма развитой логикой, чтобы, например, регулярно менять пин-коды по определенным правилам, что, правда, создает некоторые неудобства владельцам. Внутренние данные в карте могут быть зашифрованы или доступны только на чтение или только на запись с целью затруднить дублирование. Однако, эти все меры не являются препятствием для увлеченного человека. Пару лет назад в одной из телеконференций проходило сообщение, что в неком российском НИИ приспособили сканирующий электронный микроскоп, который позволяет фотографировать отдельные молекулы вещества, для изучения внутренней структуры микросхемы в смарт-карте. Вполне возможно собрать эмулятор некоторых карт на микроконтроллере за пять долларов и двух микросхемах обвязки. Этот эмулятор имеет размер пачки сигарет и ведет себя в точности как оригинальная карта. Одно время в Москве на рынках вовсю продавались и были очень популярными эмуляторы для телефонных карт, позволяющими бесплатно звонить с городских таксофонов хоть в Африку.

В 1998 г. в Омске, по сообщению ПРАЙМ-ТАСС, злоумышленник взломал защиту карт системы "Золотая Корона". Он открыл картсчета в Сибирском филиале Инкомбанка /Новосибирск/, Новосибирской дирекции Мосбизнесбанка, Омскпромстройбанке и Омск-банке. После этого, используя специальное оборудование, снял имеющуюся на них информацию и внес в нее изменения при помощи разработанного программного обеспечения. Внесенные изменения позволили получать в банкоматах сумму, находящуюся на картсчете неоднократно.

Затем, как сообщили, он изготовил поддельные пластиковые карточки системы "Золотая Корона", и внес на них данные о заводском серийном номере, идентификаторе банка-эмитента, номере счета, коде валюты, базовом остатке, платежных лимитах, а также другие данные, полностью соответствующие оригиналам, получив таким образом возможность совершать поддельные транзакции и получать деньги в банкоматах в неограниченном количестве[[5]](#footnote-5).

Использование современных устойчивых криптографических алгоритмов, позволяют значительно снизить вероятность несанкционированных платежных транзакций. Но прогресс не стоит на месте, и уже сегодня ведутся разработки в области повышения надежности смарт-карт.

 Примером таких работ может служить научно-исследовательский проект, спонсируемый Европейской Комиссией – программа Esprit (EP8670) под названием Cascade. Перевод данной аббревиатуры на русском выглядит как «способы идентификации портативных “разумных” устройств». Способ повышения надежности специалисты данной организации видят в увеличении объема памяти (для работ с большим количеством данных), и в наращивании разрядности процессора. Данная организация ведет разработки технологии биометрической идентификации: по голосу, по отпечаткам пальцев.

При той открытости стандартов, к которой стремятся и которая требуется для совместимости оборудования и программного обеспечения, особые требование по безопасности возлагаются на операционные системы, чья декларируемая надежность давно уже под большими сомнениями.

Проблемы безопасности платежных систем носят не только частный характер, а представляют собой национальные интересы. С этой позиции государству необходимо разрабатывать процедуры сертификации систем платежей с точки зрения безопасности. Основная контрольная функция должна принадлежать Центральному Банку.

В России уделяется недостаточное внимание разработке национальной концепции безопасности платежных систем. К основным проблемам национального характера можно причислить:

1. Отсутствие национального законодательства и других норм, регулирующих взаимоотношения между участниками платежных систем;
2. Отсутствие в Уголовном кодексе статей, предусматривающих наказание за незаконное использование пластиковых карт (ст. 187 УК регламентирует только один вид мошенничества – подделку);
3. Недостаток специалистов и специальных подразделений правоохранительных органов по борьбе с “карточным” мошенничеством;
4. Слабое взаимодействие между банками и правоохранительными органами;
5. Отсутствие единой национальной организации по противодействию мошенничеству с использованием пластиковых карт.

Риски, зависящие от вида оказываемых услуг, носят экономический характер. Оказывая услуги своим клиентам по краткосрочному кредитованию с помощью пластиковых карт, банк берет на себя все риски, присущие операциям кредитования. Основной вес приходится на кредитный риск – риск невозврата кредита в срок и не уплаты процентов. В операциях кредитования с использование пластиковых карт, кредитный риск носит более выраженный характер, учитывая небольшой размер кредита, неопределенность возникновения кредитных отношений. Процентный риск также более выражен, по причине несовпадения сроков заключения договоров на обслуживание пластиковых карт и моментом выдачи кредита.

Для уменьшения кредитного риска при выдаче кредитной пластиковой карты, банк должен разрабатывать рейтинговые методы оценки кредитоспособности клиента. Принимая во внимание, что выдача кредитной карты, носит поточный характер, рейтинг клиента не сможет в должной мере застраховать банк от данного риска. Наиболее надежным способом оценки кредитоспособности в данном случае является история взаимоотношений заемщика с банком. Сюда входит и кредитная история клиента и наличие вкладов у клиента. Банк более информирован о финансовом положении клиента, с которым он работает определенный промежуток времени, при привлечении клиента со стороны банк берет на себя повышенный риск. В условиях России использование рейтинговых методов оценки затруднено, из-за отсутствия надежных источников информации о клиенте.

Защищенность инвестиций коммерческого банка при создании платежной системы состоит из обоснованности затрат на создание платежной системы сегодня и неподверженность моральному износу завтра. С этих позиций коммерческий банк должен сделать выбор между современными технологиями, как правило, более капиталоемкими, и менее современными, но более дешевыми.

# 4. Цифровые наличные деньги

## 4.1. Общие сведения

Цифровые наличные, по своей сути, относятся тоже к дебетовым системам. Существует два типа цифровых наличных – хранящиеся на смарт-картах (Mondex) и хранящиеся на жестком диске компьютера. Со временем эти типы сольются в один.

Эти системы по существу аналогичны наличным деньгам. Грубо говоря, эти и есть наличные деньги. Цикл жизни электронных денег содержит следующие этапы: сначала клиент создает на своем компьютере электронные купюры, определяя их номинал и серийный номер. Они заверяются собственной цифровой подписью клиента. Затем он посылает их в банк, который, при поступлении реальных денег на счет, подписывает эти купюры, зная только их номинал и отправляет их обратно клиенту. Теперь мы имеем цифры, которые являются на самом деле деньгами. Их можно записать на бумажку и отдать кому-нибудь, это будет эквивалентно передаче наличности. Их можно записать на дискету и потерять, при этом вы потеряете все деньги. Их можно пересылать по каналам связи.

При покупке клиент посылает купюры продавцу, который предъявляет их банку. Банк проверяет подлинность и производит зачисления на счет продавца. Причем продавец не получает никаких сведений о покупателе, но покупатель всегда может доказать, что покупку совершил он, так как только он знает серийные номера своих купюр. Таким образом реализуется система “слепой подписи”, которая позволяет проводить операции анонимно, но с перспективой доказательства их действительности. Электронные деньги способны циркулировать вне банковских сетей, между самими клиентами или продавцами. Однако, для проведения расчетов необходимо открытие счета в каком-либо конкретном банке.

Цифровые наличные – это очень гибкий инструмент. С их помощью также легко оплатить покупку в интернете или устроить там свой собственный бизнес. Только цифровые наличные могут обеспечить микроплатежи – так необходимые для информационного бизнеса и продажи публикаций. Такие электронные деньги могут быть помечены для специального использования (только для кино, например), что весьма удобно для контроля денег в семье.

Стоимость транзакции с использованием цифровых наличных и их обработка и учет значительно дешевле стоимости обработки традиционных денег, кредитных карт и чеков и других средств платежа. Обработка цифровых наличных проще, и их использование может серьезно изменить структуру банков и сократить персонал.

Цифровые наличные, в отличие от чеков и кредитных систем, позволяют поддерживать анонимность транзакций (в той или иной степени), так как не требуют при их использовании удостоверения личности плательщика и его кредитоспособности.

В отличие от традиционных наличных денег оплата с помощью цифровых наличных не требует присутствия плательщика и получателя, так как передача может производиться дистанционно по Интернет или по телефону. В последнем случае, правда, у обеих сторон должен быть специальный телефон с приемным устройством для карты (они уже выпускаются).

## 4.2. Западные реализации

Поподробней рассмотрим одну из реализаций, созданных пионером в области подобных систем. **DigiCash** – голландская компания, разработавшая целый ряд систем с использованием цифровых наличных, например, систему оплаты проезда по платным дорогам Европы. Основной продукт компании – цифровые наличные –- полностью анонимная система. По лицензии этой компании из Голландии уже действуют два банка – Mark Twain Bank в США и Merita Bank в Финляндии, с помощью которых можно проводить любые операции с цифровыми деньгами, включая их конвертацию в уже реальные, соответственно, доллары США и финские марки.

Операции в цифровыми наличными деньгами DigiCash выглядят следующим образом:

1. Клиент, найдя интересующий его товар, если у него еще нет программного обеспечения DigiCash, скачивает его прямо из виртуального магазина;
2. С его помощью клиент устанавливает связь с одним из DigiCash-банков и открывает там счет;
3. Любым доступным способом (чеком, кредитной картой, банковским переводом), клиент переводит деньги на этот счет. Затем, в любое время клиент, с помощью полученного программного обеспечения, связывается со своим банком и снимает необходимую сумму "на расходы", кладя ее в свой электронный кошелек или, наоборот, переводит ее в банк на хранение;
4. С деньгами в кошельке, клиент готов к покупкам в Интернет по магазинам, принимающим цифровые деньги. Оплата производится мгновенно, переводом денег из кошелька клиента в кошелек продавца.
5. Продавец, с помощью банка, проверяет полученные наличные и сразу посылает клиенту товар или оказывает услугу.

Опишем чуть подробнее четвертую стадию – процесс "снятия" своих денег в банке, который заключается в том, что клиент сам, с помощью полученного программного обеспечения и ключа, который знает только он, генерирует длинные случайные числа, служащие потом основой для "монет" и "банкнот"; Эти числа затем посылаются в банк, в некотором "цифровом конверте", подписанным клиентом.

Цифровой конверт – это технология, основанная на слепой цифровой подписи (blind signature), позволяющая идентифицировать полученную информацию, то есть быть уверенным, что она пришла от конкретного клиента в неизмененном виде, и удостоверить или подписать ее не зная о ее содержании.

Числа подписываются банком (но сам банк не может их узнать!) и возвращаются клиенту. Соответствующая сумма списывается с банковского счета клиента.

Клиент "вскрывает конверт" (то есть удаляет идентифицирующую его информацию) и записывает на диске своего компьютера (в электронном кошельке) полученные таким образом числа (файлы), которые содержат подпись банка и свой номинал, и являются наличными.

Все это происходит в течении нескольких секунд. Так как банк подписал “банкноты” их самих не видя, но зная, кому он их подписывает, банк не может знать, кто и на что истратил эти “банкноты”, которые к нему в конце концов поступают, совершив круг в виртуальной экономике.

Лицензию на использование описанной технологии выдает компания DigiCash, продавец платит $5-25 в месяц и 2-3% от объема обмена накопленных цифровых денег на реальные, покупатель не платит ничего, с банками претендующими на роль эмитентов цифровых наличных проводятся особые переговоры. Таким образом, в системе DigiCash даже такие маленькие транзакции как 20, 10, 5 и даже 1 цент, становятся возможными, что очень важно, так как по прогнозам именно такие микроплатежи будут основой миллиардного информационного бизнеса в Интернете.

Однако к 1997 году стало ясно, что данные проекты продолжают оставаться в стадии опытной эксплуатации, вместо того, чтобы привлекать реальные денежные потоки. Компания была существенно реорганизована с привлечением венчурного капитала. В компанию были привлечены "профессиональные менеджеры с опытом работы в сфере платежных систем".

К сожалению, принятые меры по "маркетизации" компании не дали нужного эффекта. После того как Mark Twain Bank был поглощен Mercantile Bancorp. of St. Louis, представители последнего прекратили участие в проекте, заявив, что "5000 пользователей данной системы не создали сколько-нибудь заметного потока капиталов". После этого DigiCash закрыла отделение в Амстердаме и резко сократила штат. Наконец, 4 ноября компания фактически объявила о своем банкротстве.

Показательным является не столько сам крах, а то, что он проходил по предсказанному заранее механизму. Аналитики давно указывали на ошибки DigiCash в продвижении электронных наличных. Указывалось, во-первых, что политика компании "одна страна – один уполномоченный банк" сужала число банков-участников системы. Второй существенной ошибкой был акцент на анонимность как на самоцель, в то время как ее более продуктивно рассматривать в качестве средство создания дешевой и гибкой платежной системы. При этом DigiCash являлась держателем патентов на базовые методы платежей электронными наличными и развитие компании, по сути, было экспериментом в чистых условиях.

**Mondex** – это самая многообещающая электронная платежная система. Пока она развивается отдельно от Интернета, но в недалеком будущем, по мере распространения считывающих устройств для компьютера, она обещает стать самой популярной и в интернете. Собственно Mondex – это смарт-карта.

Mondex – это разновидность цифровых наличных, то есть дебетовая система, при этом она гораздо более безопасна чем другие системы, хотя бы уже потому, что деньги, то есть соответствующие числа, хранятся не на диске, а в карте, откуда их скопировать сложнее. А раз так, то и не требуется авторизация со стороны различных процессинговых центров, что в свою очередь имеет два важных следствия: операции проводятся непосредственно между двумя участниками, и стоимость транзакции стремится к нулю, а во-вторых, система абсолютно анонимна.

Все что сдерживает сейчас Mondex, купленной недавно компанией MasterCard, и другие похожие проекты цифровых наличных, базирующихся на смарт-картах – это отсутствие должной инфраструктуры, то есть устройств работающих со такими картами. Эта проблема будет постепенно решаться и все устройства по приему обычных кредитных карт будут заменены на устройства принимающие и те и другие.

Следует обратить на другие явные преимущества Mondex перед другими платежными системами, которые быстро позволят ей стать самым популярным платежным средством для расчетов примерно до $50 (хотя ничего не мешает проводить расчеты и держать в карте гораздо большие суммы).

Низкая стоимость – Mondex не требует никакой оплаты за транзакции (да и при всем желании Mondex не может проследить за ними), поэтому Mondex выгоднее использовать, чем существующие кредитный карты, за пользованием которыми банки удерживают от 2-3% от транзакции плюс 20 центов; кроме этого последние практически невозможно использовать для микроплатежей .

Глобальный характер – как и кредитные карточки. В отличии от чеков, Mondex это система в основе своей интернациональная, и расплатиться с ее помощью можно практически в любой валюте.

Высокая степень защищенности от подделок и несанкционированного использования – Mondex использует все последние разработки из области криптографии с открытым и закрытым ключами, система защищена цифровыми подписями с двух сторон (клиент-банк или клиент-клиент) личным паролем клиента и прочими хитростями. По надежности Mondex превосходит кредитные карты.

**VISA Cash** – это основной конкурент Mondex. Основные принципы заложенные в VISA Cash и Mondex одни и те же. Поэтому нет смысла подробно их описывать снова. VISA Cash - это тоже смарт-карта со всеми ее свойствами и атрибутами. Однако изначально VISA Cash гораздо меньше ориентированна на Интернет, возможно потому что для транзакций по Интернету по мнению “визы” вполне достаточно обычных кредитных карточек используемых совместно с новым стандартом SET. Так или иначе “виза” вполне может предложить для независимых производителей спецификации VISA Cash для создания специальных считывающих устройств для компьютера, после чего карточки VISA Cash легко могут быть использованы и в Интернете. На сегодняшний день VISA Cash уже используется для покупок недорогих вещей и услуг (книги, кафе, кино, бензоколонки и т.д.) в пилотных проектах в пяти странах: Аргентина, Австралия, Канада, Колумбия и США.

## 4.3. Отечественные реализации.

Российский рынок платежей в Интернет может предложить любое решение. Уже действуют системы цифровых денег **PayCash**, **WebMoney**, системы, обслуживающие платежи по кредитным картам **АССИСТ**, **Russian Shoppig** **Club**, **Киберплат**, **InterRussia**, **Элит**, **Instant**! и др. Все они отличаются между собой удобством и ценой обслуживания, и каждый владелец Интернет-магазина может подобрать для себя наиболее подходящую и безопасную. Краткие характеристики некоторых предлагаемых сегодня систем приведены в таблице 1.

Табл.1. Сравнительные характеристики Российских платежных систем.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *Система* | *Тип системы* | *Конфиденциальность* | *Мульти­-валютность* | *Уровень безопасности* | *Целевой рынок (размеры транзакций)* | *Целевой рынок товаров* |
| До $1 | $1-$100 | Свыше $100 | Информационные | Физические |
| **CyberPlat** | Дебетовая (платеж осуществляется цифровым чеком, подписанным ЭЦП) | Неанонимная (для банка) система для покупателя и продавца) | На сегодня обслуживаются только рубли | Система применяет асимметричный алгоритм криптографического преобразования RSA (512 бит. Ключ) | Да | Да | Возможно | Да | Да |
| **PayCash** | Дебетовая (платеж осуществляется цифровыми наличными, носитель - ПК, предварительно переведенными со своего счета на платежную книжку) | Абсолютно анонимная система для покупателя (ни банк, ни продавец не может определить покупателя). Продавец банком не опреде­ля­ется. | Присутствует изначально | Система применяет шифрование с открытым (RSA с ключом 1024 бит) и закрытым ключами (160 бит) ключ. | Да | Да | Возможно | Да | Да |
| **ЭлИТ** | Оплата по пластиковым картам VISA, Euro / Master Card, Union Card. Работа по слиповой и безслиповой технологии.  | Конфиденциальная система со стороны пользователя. Гарантом совершения операции в системе являются торговые организации и Банк. | Присутствует | Secure Socket Layer (SSL). Соответствует всем требованиям банковского эквайренга. Не требует установки клиентского ПО. Банк предоставляет документы, необходимые для ведения бухгалтерского учета. Могут использоваться сертифицированные средства защиты информации.  | Да | Да | Да | Нет | Нет |
| **Web-Money** | Система Интернет расчетов, аналогичная "цифровым наличным",  | Абсолютно анонимная система для покупателя и продавца.  | Только доллары США, хранятся в IMTB | Вся информация, передаваемая по каналам Интернет, кодирована со стойкостью не менее чем RSA с длиной ключа 1040 бит.  | Да | Да | Да | Да | Да |

Рассмотрим особенности системы **PayCash** [8].

Участниками платежной системы являются Банк (компания-оператор системы) и клиенты. В качестве клиентов могут выступать физические и юридические лица, а также роботы, т. е. автономно функционирующие компьютерные программы, играющие роль магазинов, казино, дилинговых центров, букмекерских контор и т.д. Все клиенты равноправны с точки зрения Банка. В частности, чтобы иметь возможность принимать платежи клиенту не требуется никакого особого статуса "магазина". Все свои операции в рамках системы PayCash клиент проводит при помощи специального программного обеспечения Кошелек. Участники системы взаимодействуют между собой посредством пересылки сообщений по Интернет.

Схема работы системы выглядит следующим образом. Будущий клиент при помощи Кошелька открывает счет в Банке (открытие счета производится по сети Интернет "из дома"), и каким-либо способом переводит на этот счет деньги (внесением наличных в кассу Банка, банковским или почтовым переводом, при помощи кредитной карты, и, наконец, другой клиент может заплатить ему в рамках системы PayCash). После этого он становится клиентом. Чтобы иметь возможность расплачиваться в рамках системы PayCash, клиент создает у себя в компьютере при помощи Кошелька одну или несколько платежных книжек. Затем опять же при помощи Кошелька переводит некоторую сумму денег со своего счета на одну из книжек, т. е. в свой компьютер. При этом Банк не может определить, на какую книжку переводятся деньги. Кроме того, Банк не знает, кому принадлежат конкретные платежные книжки. Теперь клиент готов расплачиваться в Интернет, причем анонимно, теми деньгами, которые лежат на его платежных книжках. Каждый платеж авторизуется Банком. Цепочка сообщений во время платежа имеет следующий вид:

**Продавец ⇒ Покупатель ⇒ Продавец ⇒ Банк ⇒ Продавец ⇒ Покупатель.**

На первом шаге продавец просит деньги у покупателя, причем в запрос включен подписанный контракт сделки. На втором шаге покупатель отсылает продавцу данные платежа. Далее продавец отсылает данные платежа в Банк для авторизации. Банк проводит необходимые проверки и отправляет продавцу квитанцию, а также квитанцию для покупателя. Продавец сообщает покупателю свое решение и пересылает ему данные, зашифрованные Банком на имя покупателя.

В системе PayCash клиент получает в свое распоряжение "электронные наличные", которые, как и обычные бумажные деньги, можно потерять. Например, если компьютер клиента "сгорит" или его украдут, то клиент лишится всех денег, которые он перевел в свой компьютер и не успел потратить. Однако если у благоразумного клиента сохранились резервные копии параметров Кошелька для последнего перевода денег со счета в компьютер, то он может восстановить свои деньги. Таким образом, система PayCash – это система анонимных цифровых денег, а не просто система клиент-банк. Это выражается еще и в том, что Банк не может (например, по требованию суда) воспрепятствовать клиенту тратить деньги, которые тот успел перевести в свой компьютер, иначе, как прекратив все платежи в системе.

**Анонимность платежей.**

Анонимность платежей в системе PayCash обеспечивается на двух уровнях. Во-первых, при открытии счета в Банке клиент может не предоставлять никакой достоверной информации о себе. Во-вторых, для любого платежа Банк не имеет даже теоретической возможности установить, с какого счета были сняты деньги, которыми производилась расплата, так как при переводе ЭД со счетов на платежные книжки клиенты используют технологию слепой подписи.

**Безопасность.**

При пересылке по сети все данные шифруются методами, имеющими устоявшуюся в криптографических кругах репутацию. При этом используются открытые ключи не короче чем 1024 бита и симметричные ключи не короче чем 128 битов, поэтому перехват зашифрованных сообщений в обозримом будущем невозможен. При реализации системы предусмотрены также меры предосторожности, ограждающие клиента от попыток похитить информацию непосредственно с его компьютера: а) целостность программного обеспечения и баз данных контролируется Кошельком, б) базы данных хранятся на жестком диске компьютера в зашифрованном виде, в) имеется возможность сохранять на дискету в зашифрованном виде копии данных, достаточных для восстановления статуса клиента после краха его компьютера, г) запуск Кошелька закрыт паролем и т. д. Клиент, выполняющий элементарные правила предосторожности, может быть уверен в безопасности своих денег.

**Защищенность.**

Все участники системы защищены друг от друга и от внешних злоумышленников в том смысле, что они имеют в своем распоряжении технические средства для доказательства своей правоты и изобличения нечестного партнера.

## 4.4. Безопасность цифровых денег.

С точки зрения надежности единственным уязвимым местом подобной системы является механизм электронной подписи. Стандартным решением обеспечения безопасности платежей в Интернет является использование технологии SSL, базирующейся на криптографическом алгоритме RSA (назван по фамилиям авторов – Ривест, Шамур, Адлеман). Его стойкость к взлому строго математически не доказана, но на практике пока не опровергнута.

Этот криптоалгоритм построен на операциях с большими простыми числами, так что, пока не найдено алгоритмов факторизации (разложения этих чисел на их простые делители), реальной опасности с "математической" стороны нет. Алгоритм RSA является мировым стандартом для шифрования с открытым ключом.

Реально используются алгоритмы RSA с длиной ключа до 1024 бит, при этом, Рон Ривест, один из разработчиков RSA, подсчитал, что для того, чтобы “пробить” криптотекст, зашифрованный с помощью ключа длиной 512 бит нужно потратить $8.2 миллиона.

Ничто не говорит о том что такие алгоритмы вообще могут быть найдены. Скорее потенциальная угроза безопасности цифровых систем может исходить от "человеческого фактора". Излишне, видимо, говорить о том, что компьютерные центры, занимающиеся ключевыми операциями: эмиссией цифровых наличных, учетом и взаиморасчетами (клирингом) между участниками расчетов, должны охраняться примерно также как хранилища золотовалютных запасов и госбанки. А то, что даже в госбанке не все оказываются, мягко говоря, чисты на руку, известно у нас всем. Так что, в принципе конечно, нельзя исключить подкуп и шантаж персонала, в результате которого, преступники могли бы завладеть ключами, паролями, цифровыми подписями и получить контроль над компьютером. Это, правда, маловероятно так как в системах с хорошим уровнем безопасности части наиболее важной информации распределены среди довольно большого количества работников и компьютеров, так что никто всего не знает, и нужна кооперация всех этих сотрудников для получения полного контроля над системой. Это резко снижает риск. И вообще, все-таки эта проблема не самой сети Интернет, сам процесс передачи информации и самих денег сегодня вполне защищен.

# 5. Правовой статус платежных систем

Поскольку при несбалансированной экономике движение больших наличных денежных масс может вызывать кризисные ситуации, переход денежных средств из безналичной формы в наличную довольно жестко контролируется государством, и искусственно создаются и законодательно закрепляются условия для преимущественного хранения денежных средств в безналичной форме на счетах в кредитных организациях. Безналичные денежные средства весьма подвижны: для уплаты (передачи) денег достаточно списать сумму задолженности со счета плательщика и зачислить ее на счет получателя, чтобы таким способом передать денежный эквивалент стоимости поставок, работ, услуг.

Объектом расчетных правоотношений являются деньги, подлежащие уплате за выполненные работы, поставленную продукцию, оказанные услуги. Но, учитывая, что характерной чертой безналичных расчетов является отсутствие передачи денег плательщика непосредственно получателю, возникают такие вопросы, как "что следует понимать под термином "безналичные деньги"?" и "являются ли они самостоятельным объектом расчетных правоотношений?".

Сам по себе способ безналичных расчетов как бы не создает новых средств платежа - "безналичных денег", которые следовало бы включить в понятие объекта расчетных правоотношений. Их объектами остаются деньги в виде денежных знаков, причем не только в идеальном представлении, когда они используются для расчетов или как мера стоимости, но и реально, в виде банковских и казначейских билетов, когда в предусмотренных законом случаях банк выдает их владельцу счета на основании чеков.

Сущность денег при переходе их в безналичную форму не нарушается. Более того, все функции денег, сформулированные современными экономистами, в полном объеме выполняются и безналичными деньгами.

Развитие техники привело к появлению новых терминов – "электронные деньги" и "электронные расчеты". С этим связан следующий эволюционный шаг денежного обращения, и объектом этих подобных расчетов по-прежнему являются те же безналичные деньги. "Электронные деньги" являются подвидом безналичных денег и имеют все характеристики, присущие безналичным деньгам. Знаки стоимости, отраженные на электронных носителях информации, находятся в прямой зависимости не только от специального субъекта – банка, но и от целой системы обеспечения их оборота, включающей технические средства приема, обработки и хранения информации (компьютеры, базы данных, специальное программное обеспечение поддержки платежных операций, каналы связи и такие средства проведения платежных и расчетных операций, как банкоматы, платежные терминалы и пластиковые карточки). Появление электронных носителей стоимости породило новые правовые проблемы, при неизменной экономической природе новоявленных денег. Эти проблемы лежат в области “отмывания” денежных средств теневой экономики и прав человека. Существует специальная межправительственная комиссия по финансовым операциям (Financial Action Task Force, FATF) из представителей 26 стран изучает возможность использования систем электронных денег для отмывания незаконных доходов. Она хочет убедиться, что создаваемые системы электронных денег позволят банкам выявлять подозрительные сделки и сообщать о них. В опубликованном докладе юридической группы по вопросам информационных технологий при Лондонском университете содержится предостережение, что развитие систем электронных денег чревато опаснейшими последствиями. В частности, в этом докладе говорится, что способы регистрации операций в действующих системах электронных денег существенно облегчают отмывание денег и уклонение от уплаты налогов. В этом докладе предлагается организовать систему агентств для контроля частных телефонных сообщений с целью выявления операций с электронными деньгами.

Если бы даже такой контроль был возможен, то получаемые данные, включая номера телефонов отправителя и получателя, необходимо было бы переправлять в полицейские компьютеры. А это затрагиваются права человека на неприкосновенность частной жизни и защиту данных, так что эти вопросы еще необходимо рассматривать с правовой точки зрения.

Платежные системы создаваемые банками для проведения расчетно-кредитных операций, регулируются Гражданским кодексом. Он устанавливает наиболее общие правила для кредитных и расчетных обязательств, которые не могут быть изменены другими законами и иными правовыми актами. Важным является предоставление сторонам при заключении соглашений в области кредитных и расчетных обязательств права строить свои взаимоотношения, основываясь не только на законе и банковских правилах, но также с учетом обычаев делового оборота, применяемых в банковской практике [4].

Законодательство не устанавливает определенных норм для создания, эксплуатации, управления, определения ответственности в платежных системах. Все отношения в платежных системах носят договорной характер. Определенно тот правой пробел, сложившийся в данной области, будет решен. И учитывая заинтересованность государства в контроле за платежными системами, можно предположить, что дальнейшее развитие нормотворчества в этой области будет идти по пути повышения контроля и ответственности.

Процесс проведения электронных платежей в системе Центробанка пока далек от совершенства. Само понятие “электронный документ”, принятое во всем мире, в том числе в подавляющем большинстве развивающихся стран, у нас существует теоретически, но не закреплено в законодательстве.

В Гражданский кодекс РФ уже заложены необходимые положения, описывающие документооборот в электронном виде, и на этой основе уже успешно введен в действие ряд документов и инструкций таких организаций, как Банк России. Например, временное положение ЦБР от 12 марта 1998 г. N 20-П "О правилах обмена электронными документами между Банком России, кредитными организациями (филиалами) и другими клиентами Банка России при осуществлении расчетов через расчетную сеть Банка России" (с изменениями от 28 апреля 1999 г.)

По мнению многих экспертов, это положение открывает новый пакет документов, принятие которого полностью уравняет в правах документы бумажные и электронные. В ожидании закона об электронных документах такое временное положение должно было появиться именно у Банка России, как у организации наиболее заинтересованной в безбумажном документообороте.

До момента принятия Положения, при внедрении систем обмена электронными документами, организации руководствовались в основном положениями Гражданского Кодекса, закрепляющими понятие "электронная подпись". Формулировки кодекса носят самый общий характер и требуют конкретизации в дополнительных документах.

Функцию подобной конкретизации по замыслу авторов Положения, оно и должно выполнять. В соответствии с этим Положение формально определяет участников системы электронного документооборота, электронно-цифровую подпись, электронные документы, понятие подлинности электронного документа. На рамочном уровне определен порядок работы с электронными документами: особенности оформления, хранения, подтверждения подлинности и исполнения.

Вместе с тем Положение не лишено ряда недостатков, которые могут проявиться в ближайшее время, как по объективным, так и по субъективным причинам.

Вызвано это тем, что Положение носит рамочный характер. Уместна аналогия с Конституцией, которая гарантирует права граждан, но не содержит механизмы для их реализации. Такая "рамочность" ни в коей мере не умаляет достоинств принятого документа. Более того, на первом этапе она неизбежна, поскольку принятое Положение – временное, и, несомненно, либо будет дорабатываться до постоянного, либо просуществует до принятия аналогичного Федерального закона.

Положений ГК является достаточно для легализации систем электронных платежей, работающих на основании управления личным счетом клиента, таких как CyberPlat. Методом платежа в таких системах является перевод денег со счета покупателя на счет продавца, а электронные деньги играют роль платежного поручения. Законодательство не накладывает принципиальных ограничений на форму поручения.

В схеме функционирования цифровых денег практически нет электронной специфики. Человек, знакомый с банковскими операциями, легко увидит в ней аналог обращения банковских обязательств, например векселей на предъявителя. Собственно, первыми попытками легализации электронных наличных и были попытки заявить их как традиционные инструменты в бездокументарной форме. К сожалению, эти попытки оказались неудачными.

Дело в том, что банковское законодательство является одной из наиболее формализованных отраслей права. При этом большинство деталей банковских обязательств детально оговорены. В целом они легко переносятся на бездокументарную основу, но какая-нибудь мелочь неизбежно встает неодолимым препятствием. Как, например, взимать с электронных наличных-векселей гербовые сборы? Правомерность применения электронных векселей не удалось отстоять даже Новосибирской области, имевшей развитую систему поддержки обращения этого инструмента.

При этом существует множество лазеек, которые позволяют эти ограничения обойти, но вполне определенной ценой. Возможность существования в России платежной системы в условиях практического отсутствия сколько-нибудь полного и последовательно описывающего ее законодательства блестяще подтвердила история распространения кредитных карт. Оборот электронных платежных систем оказалось возможным легализовать для государственных органов, интерпретируя его в существующих терминах (например, как агентской деятельности), ценой потерь в функциональности. При этом в зависимости используемой юридической схемы, страдать могут или гарантии покупателя, или гарантии Банка, или полнота функций системы. Иными словами, такие меры хороши для решения локальных задач, например запуска платежной системы какого-либо провайдера или Интернет-магазина. С другой стороны, ни один из крупных игроков на рынке электронных платежей не ставит своей целью решение таких локальных задач, рассчитывая на масштабное введение системы.

Поэтому сейчас юридическая деятельность сконцентрирована именно на создании полностью легальной прозрачной концепции обращения электронных наличных. Деятельность ведется в двух направлениях. Во-первых, концепция клубной системы. Это означает, что вместо документа на государственном уровне разрабатывается пакет договоров, принимаемый всеми участниками системы. Законодательство не накладывает существенных ограничений на такие договоры, что позволяет использовать, например, корпоративные аналоги векселей. Основной трудностью здесь является стыковка с налоговой системой. Признав определенный договор корпоративным, мы автоматически выводим его из сферы генерального банковского законодательства и, тем самым, попадаем под все налоги с обычных операций, включая НДС. Это обстоятельство не является фатальным, но чрезвычайно затрудняет бухгалтерское сопровождение системы.

Таким образом, можно с большой долей вероятности предсказать следующие направления развития соответствующих юридических документов. Во-первых, компании, действующие на этом рынке, будут создавать свои концепции платежей, используя текущее законодательство. Во-вторых, в результате синтеза таких попыток и независимой деятельности аналитиков будет создана некая общая юридическая концепция электронных платежей на государственном уровне и будет принят соответствующий закон или законы. Наконец, на основе этого законодательства будут разработаны соответствующие нормативные документы, описывающие как общие аспекты такой деятельности, так и ее существующей финансовой и налоговой системе. Есть основания оптимистично оценивать перспективы и сроки этого процесса. В России практически отсутствует торможение новых систем устоявшимися платежными схемами. Можно верить, что окончательное становление законодательства по электронным платежам ненамного отстанет от окончательного становления законодательства по таким "традиционным" инструментам как платежные карточки или дорожные чеки.

# Источники

*Печатные издания:*

1. О.С.Рудакова. *Банковские электронные услуги*. – М.: Банки и биржи, ЮНИТИ, 1997. – 261 с.
2. В.Жельников. *Криптография от папируса до компьютера. –* М.: ABF, 1996, ил., 336 с.
3. *Компьютеризация банковской деятельности.* Под. Ред. Г.А.Титоренко. – М.: Финстатинформ, 1997 – 304 с.
4. *Гражданский кодекс РФ.*

*Электронные издания:*

1. Агентство «*РосБизнесКонсалтинг*». http://www.rbc.ru.
2. «*Платежные системы Интернет*». http://www.emoney.ru
3. «*Финансовые Интернет услуги*». http://www.internetfinance.ru
4. «*Платежная система PayCash*». http://www.paycash.ru
5. «*Платежная система CyberPlat*». http://www.cyberplat.ru
1. В качестве примера можно привести сургутский «Аккобанк», обладающий самой развитой автоматизированной системой в России. [↑](#footnote-ref-1)
2. *Компьютер-информ* № 2 '2000
 [↑](#footnote-ref-2)
3. Сообщение «*РосБизнесКонсалтинг*», 11.01.2000, 13.01.2000, [↑](#footnote-ref-3)
4. Сообщение «*РосБизнесКонсалтинг*», 02.03.2000, Москва [↑](#footnote-ref-4)
5. BIT №41 19/10/98 [↑](#footnote-ref-5)