Лекция 2
Платежные системы Интернет

1 Этапы развития платежных систем в Интернете

2 Классификация и характеристика существующих платежных систем

3 Российские платежные системы с использованием кредитных карт

1 Этапы развития платежных систем в Интернете

Не успел появиться Интернет, как тут же наиболее предприимчивыми его пользователями была осознана возможность развернуть в Сети торговлю.

В 1992 г. появился термин World Wide Web

в 1994 г. первый коммерческий сайт предложил посетителям вводить реквизиты кредитных карт для оплаты своих услуг.

На первенство в вопросе использования платежных систем в интернет-бизнесе претендуют несколько ныне действующих сайтов (в частности, **Hotwired.com**). Определить, кто же на самом деле был в авангарде, похоже, уже не представляется возможным, так как для американцев этот шаг был вполне естественным: к тому времени они уже привыкли расплачиваться кредитными картами буквально за все. Однако между сайтом и банкоматом существовала определенная разница, в чем скоро убедились владельцы кредитных карт, недосчитавшись кругленьких сумм на своих счетах. Впрочем, хозяева интернет-магазинов тоже быстро осознали, что прогонять карту через PKS-терминал – это одно, а принимать никем не подтвержденные реквизиты карты через сайт неизвестно от кого – это совсем другое.

Так началась не лишенная драматизма история борьбы за безопасность платежей в Интернете.

Для минимизации возникших рисков были созданы специализированные процессинговые центры и надежный протокол электронных транзакций (SET), виртуальные одноразовые кредитные карты и "электронные деньги".

Многое успело измениться за прошедшие годы, но ***кредитные карты*** до сих пор остаются основным платежным инструментом электронной коммерции – разумеется, в тех странах, где они широко распространены – и деньги с них по-прежнему время от времени пропадают неизвестно куда. Это обстоятельство является одной из *причин появления платежных интернет-систем* (ИПС) на базе электронных денег (ЭД): людям хочется большей безопасности.

Другая причина развития альтернативных технологий расчетов – существенный *выигрыш в стоимости транзакции*. Процессинг кредитных карт обходится на порядок дороже, чем операции с электронными деньгами.

Для наглядной иллюстрации хода событий приведем краткую хронологическую таблицу, содержащую основные вехи истории ИПС в мире и в России. История интернет-платежей насчитывает уже более двадцати пяти лет. Возраст отечественных ИПС чуть меньше (на два года).

Год	Вехи истории ИПС
1991	«Кредо-банк» выпускает первую в России общедоступную международную кредитную карту VISA Classic
1994	Появляется возможность осуществлять покупки через сеть Интернет. В качестве средства расчета предлагается использовать карты с магнитной полосой
	Голландская компания DigiCash заявляет о разработке технологии расчетов с использованием электронных денег Ecash
1995	Английская компания Mondex заявляет о разработке первого электронного многовалютного кошелька. Первые испытания проходят в Суиндоне (Англия)
	Американский Mark Twain Bank первым в мире приступает к эмиссии электронных денег по технологии DigiCash
1996	Банк международных расчетов (г. Базель) публикует первые официальные систематизированные исследования по электронным деньгам. В этих исследованиях впервые официально выдвигается идея эмитирования электронных денег ЦБ. Крупнейшие "карточные" ассоциации VISA, MasterCard и Europay заявляют о выработке единых требований к изготов лению микропроцессорных карт (EMV-спецификация). Начинает работу американская платежная система E-Gold

Год	**Вехи истории ИПС**
1997	Крупнейшие "карточные" ассоциации VISA, MasterCard и технологические компании разрабатывают протокол для осуществления безопасных транзакций в Интернете SET (Secure Electronic Transaction)
	Американский банк Cardin al Bank Shares учреждает Security First Network Bank – первый виртуальный банк, предоставляющий все виды банковских услуг через Интернет
1998	Компания MasterCard совершает первую международную транзакцию с электронными деньгами Mondex
	Российский банк "Таврический" впервые заявляет о разработке российского аналога электронных денег компании DigiCash
	Начинает работу американская платежная система PayPal. В России начинают работать платежные системы PayCash, WebMoney Transfer, Assist. Первые 1000 клиентов WebMoney получают на счет по 30 WMZ в порядке рекламной акции
1999	Начинают работу системы CyberPlat, Instant! и КредитПилот
2000	Начинают работу системы E-Port , Eaccess, Cashew
2001	На рынок выходит система "Рапида"
2002	Компания "Яндекс" заключает партнерское соглашение с PayCash. Результат – появление системы Яндекс. Деньги

Можно выделить ***четыре этапа развития*** платежных систем в Интернете:
1) протоколы сеанса связи, обеспечивающие безопасную передачу данных;
2) системы на основе пластиковых карт;
3) платежные системы на основе смарт-карты;
4) платежные системы на основе электронных денег.

1. Протоколы сеанса связи, обеспечивающие безопасную передачу данных

Первым и самым простым способом оплаты товаров через Интернет является обмен открытым текстом. По сути его даже нельзя назвать платежной системой. При этом способе оплаты покупатель передает информацию, например, о своей кредитной карте, как и при заказе по телефону, без каких-либо особых мер безопасности. Недостатки такой передачи очевидны: информация легко может быть перехвачена с помощью специальных фильтров и использована во вред владельцу карты; у продавца возникают проблемы, связанные с отказами от оплаты. Этот способ, широко применявшийся несколько лет назад, сегодня уже практически не использу ется. Его сменили системы, использующие шифрование обмена – оплата производится посредством передачи по Интернету информации о кредитной карте с использованием безопасных и защищенных протоколов сеанса связи, обеспечивающих шифрование передаваемых данных. На начальном этапе самым распространенным протоколом сеанса связи являлся ***Secure Socket Layer Protocol*** , ***SSL*** – протокол, разработанный компанией Netscape.

По своей сути SSL не является платежной системой и призван обеспечивать безопасную передачу по Интернету не только данных для проведения платежей, но и любой другой информации. Это свойство протокола обусловлено тем, что он позволяет удостовериться в том, что никто не изменил данные, передаваемые от отправителя к получателю. В настоящее время на смену ему пришел более безопасный протокол SET.

2. Системы на основе пластиковых карт

Лидирующее положение среди существующих платежных систем занимают системы с использованием кредитных карточек. Успех применения пластиковых карт для расчетов в Интернете связан с привычностью такого вида оплаты, во многом схожего с оплатой в реальном мире, и большинство транзакций в Internet сегодня совершаются с применением именно этого вида платежа. Упомянутый выше протокол SSL также в большинстве случаев используется для передачи информации о пластиковых картах.

Однако этот способ обладает некоторыми недостатками.

Хотя перехватить информацию во время транзакции практически невозможно, важная информация в случае недобросовестного ее хранения на сервере продавца может находиться под угрозой доступа к ней злоумышленников.

К тому же существует возможность подделки или подмены подлинности торговца или *личности пользователя* (identity) как продавцом, так и покупателем. Фирма может предоставить о себе недостоверную информацию, а покупатель может произвести покупку, а затем отказаться от оплаты – доказать, что именно он пользовался своей картой, практически невозможно из-за отсутствия подписи.

Новой технологией, призванной устранить вышеназванные недостатки, является протокол ***SET***, ***Secure Electronic Transaction specification***. Спецификация ***SET*** является одним из кардинальных решений по безопасной оплате товаров с использованием кредитных карт.

SET разработана компаниями MasterCard и Visa при поддержке Netscape, IBM, Verisign и др. В основе спецификации SET лежит крип тография с использованием публичных ключей и цифровых сертификатов. В соответствии с технологией номер карточки, передаваемый по сети, шифруется с использованием электронной подписи клиента. Дешифровку смогут осуществлять только уполномоченные банки и компании, осуществляющие обработку транзакций по карточкам.

Протокол SET должен обеспечить защиту клиентов от недобросовестных продавцов и защиту продавцов от мошенничества при помощи поддельных или краденых карточек. Это обеспечивается тем, что процесс проверки безопасности включает сопоставление цифровых сертификатов, выданных покупателю, продавцу, банку и процессинговым компаниям.

SET состоит из *четырех основных элементов*.

Первый элемент – *Бумажник владельца карты* (Cardholder Wallet), ко торый работает в режиме он-лайн, позволяя проводить защищенные платежи.

Второй элемент – *Серверная часть продавца* (Merchant Server), позволяющая осуществлять авторизацию и обработку платежных карт.

Третий элемент – *Шлюз прохождения платежей* (Payment Gateway) – осуществляет авторизацию продавца и платежных инструкций (включая инструкции от покупателя) и взаимодействует с финансовыми сетями.

Четвертый элемент SET – *Центр выпуска сертификатов* (Certificate Authority), который выпускает и сверяет цифровые сертификаты.

Недостатки SET:

- все участники SET должны установить у себя соответствующее *программное обеспечение*, что требует значительных инвестиций;

- результаты проведенного фирмами тестирования показали *недостаточно высокую скорость проведения транзакций*, доходящую до 30 с из-за операций шифрования.

Несмотря на это, протокол SET рассматривается как будущее электронной коммерции Интернет и считается призванным поднять ее на новый, более высокий уровень.

Одним из ограничений использования пластиковых карт является *ограничение на нижний предел производимых покупок*, составляющий около 5 долл. США.

Так как за проведение каждой транзакции эмитент карточки берет порядка 1,5 - 3% от суммы транзакции, но не менее 20 центов, то про изводить оплату товаров в нижнем ценовом диапазоне становится невыгодно. Все-таки некоторые фирмы предпринимают попытки распространить кредитную схему на сектор мелких платежей и для снижения расходов на проведение клиринга и процессинга разрабатывают механизмы сбора мелких транзакций, чтобы обработка выполнялась лишь после того, как их сумма достигнет определенной величины.

Примерами российских платежных систем на базе пластиковых карт могут служить Assist, "Элит", "Рапида", Russian Story, WebPlus, Instant и др.

3. Смарт-карты

Современная смарт-карта представляет собой миниатюрный компьютер с процессором, памятью, программным обеспечением и системой ввода/вывода информации.

Одна из важнейших характеристик любой системы на базе пластиковых карточек – ее *безопасность*.

Еще одно достоинство смарт-карт – их *многофункциональность*, т. е. возможность использования одной и той же карточки в различных финансовых приложениях и в различных коммуникационных инфраструктурах.

Наличные электронные деньги на базе смарт-карт могут не только обеспечить необходимый уровень конфиденциальности и анонимности, но и не требуют связи с центром для подтверждения оплаты. В связи с этим стоимость транзакции стремится к нулю.

Перечисленные свойства смарт-карт позволяют прогнозировать постепенное распространение этого вида платежных систем. Однако для их применения в качестве инструмента оплаты по Интернету требуется широкое распространение читающих периферийных устройств для персональных компьютеров.

4. Электронные деньги

Новым видом расчетов в Интернете являются электронные деньги. Термин "электронные деньги" определяет категорию электронных платежных систем, которые пытаются перенести преимущества наличных денег из реального мира в мир Интернета.

По определению Банка России,
электронные деньги – это денежные обязательства кредитной организации, составленные в электронной форме и заменяющие в процессе их обращения требования юридических и физических лиц по оплате товаров или услуг.

Электронные деньги представляют собой очень большие числа или файлы, которые выполняют функции денежных знаков. В отличие от других платежных систем, эти файлы и есть сами деньги, а не записи о них.

Надежную работу систем с использованием электронных денег обеспечивают современные методы криптографии: алгоритмы криптографии с открытым ключом, электронной подписи и электронной "слепой" подписи. Затраты на функционирование таких систем минимальны. К тому же отсутствие в схемах расчетов кредитной карты, а значит и значительных затрат на оплату транзакций процессинговым ком паниям, позволяет применять их для микроплатежей, т.е. расчетов в самом нижнем ценовом диапазоне – меньше одного доллара. По общему мнению, именно микроплатежи могут обеспечить основной оборот продаж информации в Internet.

Кроме того, электронные деньги могут обеспечить полную *анонимность*, так как не несут никакой информации о потратившем их клиенте.

Среди компаний, развивающих системы электронных денег, можно назвать Net Cash, Citibank, DigiCash, Mondex, в России – PayCash, WebMoney.

Правовые вопросы функционирования платежных систем на основе электронных денег в России пока не разработаны, и наши соответствующие компетентные органы руководствуются положениями и рекомендациями по этим вопросам директивных органов Европейского союза. Суть их сводится к следующему.

В государствах Евросоюза запрещено проведение эмиссии электронных денег лицам или предприятиям, которые не являются кредитными учреждениями. Введение такого запрета свидетельствует о стремлении европейских законодателей ввести в сфере электронных денег достаточно жесткое регулирование – аналогичное тому, которое осуществляется в банковской деятельности.

В связи с этим пришлось значительно расширить понятие "кредитное учреждение", включив в него и "учреждения в сфере электронных денег". В свою очередь "учреждение в сфере электронных денег" трактуется как "предприятие или любое другое юридическое лицо, которое выпускает средства платежа в форме электронных денег".

Для учреждений-эмитентов электронных денег установлен достаточно жесткий режим деятельности как по кругу выполняемых ими операций, так и по финансовым показателям.

Определен механизм признания электронных денег в качестве средства платежа третьими лицами, т.е. неэмитентом. Такое признание осуществляется не в силу закона, а в силу договора с эмитентом, который может быть заключен различными способами. Таким образом, электронные деньги представляют собой еще и признанное требование к эмитенту. Оно состоит в том, что предъявитель (держатель) электронных денег в течение срока их действия может требовать от эмитента их погашения по номинальной стоимости (монетами и банкнотами или путем перевода на счет), причем плата за погашение не должна превышать необходимых для выполнения такой операции расходов, т.е. взимание комиссии с держателя электронных денег не разрешается.

Вместе с тем не запрещено взимать комиссионные при эмиссии электронных денег. Допускается и выплата процентов по полученным в обмен на электронные деньги средствам, что позволяет назвать эти средства квазивкладом.

В России в настоящее время происходит оценка влияния электронных денег на операции клиентов кредитных учреждений и на эффективность денежной политики в целом. В результате можно ожидать определенных шагов в целях регулирования этой сферы деятельности.

2 Классификация и характеристика существующих платежных систем

Классификация существующих платежных систем. Системы, обеспечивающие возможность платить и принимать платежи в Интернете, делятся на *два основных класса*, в зависимости от характера информации, передающейся в момент платежа.

1. Одни базируются на системе счетов, содержащих записи в электронном виде об остатках средств клиентов, причем счета могут быть как банковскими, так и виртуальными (к этому классу относятся и платежи с использованием предоплаченных карт).

2. Другие используют так называемые электронные деньги – некие "условные единицы", которые обладают свойствами обычных денег. И если системы, работающие с кредитными картами, уже стали достаточно привычными для россиян, то все "цифровое" и "виртуальное" (применительно к деньгам) остается пока экзотикой.

Сам термин "электронные деньги" вызывает определенные нарекания, в особенности у экономистов. Основное возражение против него звучит примерно так: "это не особый вид денег, а лишь форма существования денег обычных". Однако это вопрос скорее академический, факты же говорят сами за себя: во многих странах электронные деньги – ***e-money*** – уже получили юридический статус.

Наиболее известным документом является директива Евросоюза № 2000-46-ЕС, которая содержит одно из самых популярных *определений электронных денег*:
"*Электронные деньги – денежная стоимость, представляющая собой требование к эмитенту, которая хранится на электронном устройстве; эмитируется после получения средств в размере не меньшем, чем выпускаемая денежная стоимость; принимается в качестве средства платежа иными предприятиями, нежели эмитент*".

Европарламент несколько раз обращался к этой теме, и каждый раз определение менялось в соответствии с развитием технологий электронных платежных систем и в зависимости от ведомства, которое разрабатывало очередной документ.

Еще одно определение, которое встречается довольно часто: "*электронными деньгами называют стоимость, помещенную в электронном виде на устройство типа чиповой карты или жесткий диск персонального компьютера*".

Consumer Advisory Board Федерального резервного банка США описывает электронные деньги как "*деньги, которые передаются в электронной форме*".

Системы электронных денег получают у клиентов деньги вполне реальные. Взамен они предоставляют клиенту право оперировать с некими "платежными эквивалентами". Эти "эквиваленты" можно пересылать по почте (а электронные деньги – даже переносить с одного носителя на другой), а затем конвертировать в "живые" деньги.

Ценность "эквивалентов" определяется способностью компании-эмитента в любой момент конвертировать их обратно в "реальные" деньги, поэтому такие платежные средства, по крайней мере, в России, гораздо менее универсальны, чем платежи обычными безналичными деньгами, и имеют хождение лишь в достаточно узком кругу клиентов их эмитента. Однако эмитенты стараются всеми силами расширить сферу своей деятельности, и уже сейчас электронными деньгами можно расплатиться практически за любую услугу, предлагаемую через Интернет.

В России активно действует лишь одна система электронных денег – ЯндексДеньги (бывшая PayCash).

Относительно WebMoney существует несколько мнений. До публикации алгоритма, однако, назвать WM электронными деньгами нельзя.

Системы, работающие со счетами, можно разделить на:

– *банковские*, позволяющие клиентам с помощью электронных сообщений дистанционно управлять своим расчетным счетом в банке, и

– *комбинированные*, у которых счета могут быть и виртуальные, а все расчеты с клиентами происходят через один общий банковский счет.

В любом случае клиент кладет на счет (вводит в систему) опреде ленную сумму денег, а затем распоряжается ею в Сети путем дистанционного управления своим счетом или используя иные платежные инструменты (например, предоплаченные карты). К таким системам относятся WebMoney, "Рапида", e-port, КредитПилот, FakturaPAY и CyberCheck (первые четыре системы – комбинированные, последние две – банковские).

Наконец, можно выделить *третью группу* – системы, производящие процессинг кредитных карт, как правило, международных систем Visa, MasterCard, Kiners Club. В последнее время такие системы понемногу начинают работать и с дебетовыми картами (Visa Electron, Cirrus/Maestro, STB-Card). Два ярких представителя этой группы – CyberPlat и Assist.

Отличие систем первой и второй групп для пользователя не слишком заметно. Механизмы ввода денег в систему – одни и те же, платежи от клиента клиенту также допустимы и там, и здесь. Отличие ощущают клиенты – юридические лица, которым приходится каким-то образом проводить "электронные деньги" по бухгалтерским счетам. Системы первой и второй групп работают по различным правовым моделям, соответственно, и способы учета для них различны. Системы третьей группы (последние в списке, но отнюдь не по значимости) принципиально отличаются от первых двух тем, что покупателем в них может стать любой владелец кредитной карты соответствующего стандарта.

Характеристики электронных платежных систем. Успешная деятельность любой платежной системы при прочих равных условиях определяется признанием ее привлекательности двумя категориями пользователей, к которым все мы, так или иначе, принадлежим: покупателями и продавцами. И если для покупателей лучшей рекламой системы может стать табличка на сайте любимого интернет-магазина, то для продавцов должны существовать некие объективные параметры, характеризующие степень ее применимости и привлекательности.

Ведь если покупатель, пользуясь услугами той или иной системы, рискует, как правило, не слишком большой суммой денег, то для продавца крах системы может обернуться разорением.

К тому же ему, помимо покупателя, приходится иметь дело еще с *банками*, *налоговой инспекцией*, наконец, с собственным *бухгалтером*, которого надо убедить, что проблемы, возникающие при учете таких "нетрадиционных" платежей, решать можно и нужно.

Существуют определенные более или менее объективные характеристики, позволяющие оценивать системы и сравнивать их.

Характеристики можно разделить на *две категории*:

- "*пользовательские*", т.е. легко выявляемые при использовании системы,
- "*профессиональные*", для пользователя с первого взгляда неочевидные, однако от этого не менее важные.

Рассмотрим эти характеристики.

Пользовательские характеристики

Анонимность. Системы, поддерживающие анонимность, декларируют, что *никто не может отождествить платеж с личностью плательщика или установить структуру расход*ов конкретного клиента.

Эта характеристика не имеет смысла в случае использования кредитных карт – закон об анонимных банковских счетах вряд ли будет принят в обозримом будущем. Для систем "электронных денег" он, напротив, достаточно актуален. Пока что только о PayCash/Яндекс.Деньгах достоверно известно, что они поддерживают "несвязываемость" клиента с "купюрой" посредством алгоритма "слепой подписи" (WebMoney также декларирует это, однако без экспертизы алгоритма это – лишь слова).

Зато все интернет-платежные системы (ИПС), не связанные с кредитными картами либо банковскими счетами, поддерживают возможность анонимного подключения пользователя – и в большинстве случаев этого оказывается достаточно.

Отслеживаемость, или *трассируемость, платежей* – т.е. *возможность проследить судьбу платежа* и, в случае конфликта, доказать, что деньги были перечислены, а при необходимости – кем и когда это было сделано. Эта характеристика находится с анонимностью в неком "диалектическом" противоречии – как правило, при создании системы разработчикам приходится балансировать между ними.

Признанность системы. Чем *больше клиентов* у системы, чем больше физических и юридических лиц признают ее платежные средства – тем лучше для всех ее пользователей и, естественно, для хозяев.

Некоторые системы (e-port, CyberPlat) указывают на сайте точное число продавцов, пользующихся их услугами.

Другие ограничиваются размещением списка поставщиков. Как правило, путем несложных, но утомительных подсчетов можно все же определить число поставщиков товаров и услуг, поддерживающих систему.

Однако ситуацию осложняют два момента:

□ во-первых, списки не всегда полны (клиенты, особенно работающие по технологии B2B, могут не пожелать афишировать свои платежные инструменты);

□ во-вторых, категории, на которые в списках разбиты клиенты, часто перекрываются (интернет-магазин может находиться и в категории "Интернет-услуги", и в категории "Торговля ПО").

Конвертируемость, или *ликвидност*ь. Имея на руках наличные деньги, легко можно превратить их в любой другой платежный инструмент. Во что можно превратить электронные деньги?

Разные системы предоставляют разные *механизмы конвертации*, более или менее удобные для пользователей. Схема связей между различными эмитентами электронных денег, по которой в настоящее время клиент может перевести деньги из одной ИПС в другую, приведем далее.

Простота. Если для того, чтобы воспользоваться услугами платежной системы (скажем, оплатить телефонный счет), необходимо высшее образование и опыт работы с компьютером от трех лет, она, скорее всего, обречена. Сюда же относится простота интеграции клиентской части программного обеспечения в торговую систему продавца.

Надежность. Пользователи вправе рассчитывать, что их платежи не будут сорваны из-за аварии на сервере ИПС, продолжавшейся сутки, а записи о транзакциях не будут потеряны в результате сбоя базы данных. К сожалению, многие российские предприятия все еще склонны экономить на данной статье расходов; например, известны случаи, когда работа некоторых ИПС временно прекращалась из-за аварии у оператора связи, что свидетельствует о недостаточном резервировании каналов.

Безопасность. Сообщить, что система такая-то начала функционировать в Интернете – значит буквально вывесить объявление: "все желающие могут попробовать нас обокрасть". В желающих, как правило, недостатка не бывает. Кроме того, существуют еще кибертеррористы, ломающие все, до чего могут дотянуться.

Как правило, на сайте ИПС приводится информация об используемых алгоритмах шифрования, лицензиях ФАПСИ (они есть, например, у "Рапиды", КредитПилота, Cyber Plat), а иногда – о независимой экспертизе алгоритма шифрования (PayCash/Яндекс.Деньги).

Коммерческая оправданность. Пользоваться системой должно быть выгодно в сравнении с другими средствами платежа.
Далее приведем некоторые данные, которые позволят оценить этот параметр для каждой из систем.

Доверие к системе. Поскольку совершенных систем не существует, пользователю всегда приходится в какой-то мере полагаться на честность компании – владельца ИПС. Стопроцентных гарантий быть не может; единственное, чему можно доверять – опыт и здравый смысл.

Если оцениваемый доход, получаемый оператором от нормальной работы системы, превышает потенциальную выгоду от мошеннических операции, владельцу системы, скорее всего, на этом этапе его деятельности доверять можно.

С другой стороны, чем дольше система на рынке, тем меньше вероятность, что пользователи будут обмануты. Ситуация несколько упрощается в случае существования механизмов государственного контроля и регулирования работы систем такого рода. В России такие механизмы пока отсутствуют.

Профессиональные характеристики

Масштабируемость. Самое серьезное испытание – испытание успехом. Если бурный приток клиентов вызывает задержки платежей и сбои в ПО, ни о каком доверии речи, конечно, быть не может.

Некоторые компании приводят на сайтах данные о максимальной про изводительности систем и результаты независимых экспертных оценок. Нужно, чтобы эта практика стала стандартной.

Открытость, или ***возможность взаимодействия.*** Открытые системы (системы с открытым кодом и алгоритмом шифрования) вызывают больше доверия, хотя разобраться в этом способны только профессионалы.

Работа по открытым стандартам:

□ позволяет другим компаниям легко присоединяться к системе, увеличивая таким образом ее надежность и признанность;

□ увеличивает вероятность попыток недобросовестных фирм воспользоваться и кодом, и алгоритмом, ничего не платя авторам.

Поэтому, учитывая объем средств, вложенных в разработку, ни одна из систем не публикует всех кодов и алгоритмов, если они нестандартны. Большинство систем пользуется для защиты канала передачи стандартным протоколом SSL с длиной ключа 128 бит и паролем при входе в систему. Дополнительные алгоритмы (на базе RSA с длиной ключа 1024 бит) используют WebMoney и ЯндексДеньги для подписи и шифрования передаваемой информации, а также FakturaPAY и CyberCheck, имеющие дело с банковскими счетами.

Тип авторизации. За этой характеристикой скрывается еще одна классификация систем электронных денег – *on-line* и *offline*-системы.

1. *on-line системы* для проведения транзакций требуют *связи с центром авторизации*, который подтверждает аутентичность плательщика и его платежеспособность.

В принципе, это должно сильно снижать анонимность и неотслеживаемость, обеспечиваемые системой, поскольку такой центр наверняка ведет журнал транзакций. Уникальным алгоритмом обладает PayCash – его "платежные книжки" созданы с расчетом на невозможность установить связь между плательщиком и "купюрой", которой он расплатился.

2. *offline*-системы *допускают обмен "электронными деньгами"* по аналогии с обычными монетами – *без обращения к третьим лицам*.

В России пока нет действующих offline-систем интернет-платежей. Для Интернета, где и плательщик, и получатель постоянно находятся в состоянии online, это не столь актуально.

Гораздо более важна эта характеристика для *систем мобильных платежей*, построенных, скажем, на базе чиповых карт и допускающих платежи класса C2C, т.е. от одного частного клиента другому. Утверждается, например, что известная система Mondex работает именно по offline-принципу.

Это различие стирается с развитием индустрии карманных компьютеров и смартфонов, поскольку в ближайшее время неизбежно должны появиться версии "электронных кошельков" для этих устройств.

Не все приведенные характеристики универсальны с точки зрения разных категорий пользователей.

Одни более важны для *покупателя*:
например, *анонимность* и *простота*;
другие, прежде всего, интересуют *продавца*:
отслеживаемость, *надежность*.

В то же время большинство параметров одинаково ценны для всех клиентов ИПС.

К сожалению, информационная политика большинства ИПС такова, что далее приблизительно оценить некоторые из параметров оказывается не так-то просто.

3 Российские платежные системы

В настоящий момент в российской части сети Internet существует ряд платежных систем, практически в полной мере охватывающий круг функций, выполняемый западными платежными системами.

Однако общее состояние рыночной ниши платежных систем в России находится в *зародышевом состоянии*, объем участников и количество проводимых операций минимальны.

Тем не менее, наблюдается *прогресс*: совсем недавно не было ни одной платежной системы, а сегодня их число составляет около десятка. Хочется надеяться, что, как и уровень использования Интернета в России, так и, соответственно, число финансовых институтов и качество их услуг в российской части сети Internet будут расти теми же темпами и дальше.

Российские платежные системы можно разделить на ***группы***:

1. Платежные системы *с использованием кредитных карт*.

В их число входят CyberPlat, Assist, "Рапида", "ЭлИТ", WebPlus, Instant, RussianStory и др.

2. Системы *электронных денег* – PayCash и условно WebMoney.

3. Системы *Internet-банкинга* – "Телебанк" Гута-банка и "Домашний банк" Автобанка.

Остановимся на принципах и технологиях работы некоторых из отмеченных систем подробнее.

Платежные системы с использованием кредитных карт *CyberPlat* (http://www.cyberplat.ru/) – одна из первых российских платежных систем – система безналичных расчетов в Internet *реальными деньгами в реальном времени*.

Расчеты за покупки в интернет-магазинах могут выполняться как *со счетов клиентов в банке "Платина"*, так и с использованием *банковских кредитных карточек*, выпущенных любым российским/зарубежным банком. Весь обмен информацией осуществляется по сети Internet.

Зарегистрированный в системе CyberPlat *покупатель* может совершать покупки в интернет-магазинах, оплачивая их в интерактивном режиме (со сче та в банке "Платина" либо по банковской кредитной карточке).

Для зарегистрированного в системе CyberPlat *магазина* гарантируется оплата за покупки и исключается вероятность необоснованных отказов от оплаты покупок благодаря документированию всех сделок.

В системе предусмотрена эффективная защита от несанкционированного доступа. Передаваемая информация подписывается *электронными цифровыми подписями* участников системы, что исключает возможность мошеннического изменения содержания документов. Используется асимметричный алгоритм криптографического преобразования с открытым распределением ключей длиной 512 бит. Подделка подписи для ключа такой длины практически невозможна, так как требует огромных ресурсов.

Основными ***достоинствами*** системы являются:

□ моментальность взаиморасчетов за счет проведения online всех операций (время платежа составляет менее 2 с);

□ простота подключения к системе и простота технологии проведения финансовых и нефинансовых операций;

□ эффективная система защиты счета клиента и обеспечения конфиденциальности: взаимодействующие стороны используют электронные цифровые подписи (ЭЦП); надежность защиты клиента обеспечивается использованием 512-битного закрытого ключа; используется совершенная технология подтверждения подлинности сторон, проводящих операцию;

□ контроль над всеми операциями проведения платежа в режиме on-line и их документальное подтверждение;

□ документальное подтверждение каждого этапа операций; документы заверяются ЭЦП сторон и имеют юридическую силу;

□ управление своим счетом через Internet – возможность заплатить со счета в CyberPlat на любой другой счет в другом банке через внешние платежные системы.

В перспективе развития системы CyberPlat должна произойти ее интеграция с российскими платежными системами (STB CARD, UNIkN CARD), будет реализован прием цифровых сертификатов, создана агентская сеть по привлечению и обслуживанию клиентов, а также переход на SET-технологию.

Рассмотрим технологию оплаты покупки со счета в банке "Платина".

1. Покупатель через Интернет подключается к Web-серверу магазина, формирует корзину товаров и направляет магазину запрос на выставление счета.

2. Магазин в ответ на запрос покупателя направляет ему заверенный своей электронной цифровой подписью (ЭЦП) счет, в котором указывает:

- □ наименование товара (услуги);
- □ стоимость товара (услуги);
- □ код магазина;
- □ время и дату совершения операции.

С гражданско-правовой точки зрения этот счет является предложением заключить договор (офертой).

3. Покупатель заверяет своей ЭЦП предъявленный ему счет и отправляет его обратно в магазин, совершая тем самым акцепт. Договор считается заключенным с момента подписания покупателем выставленного ему счета. В системе счет, подписанный покупателем, становится чеком.

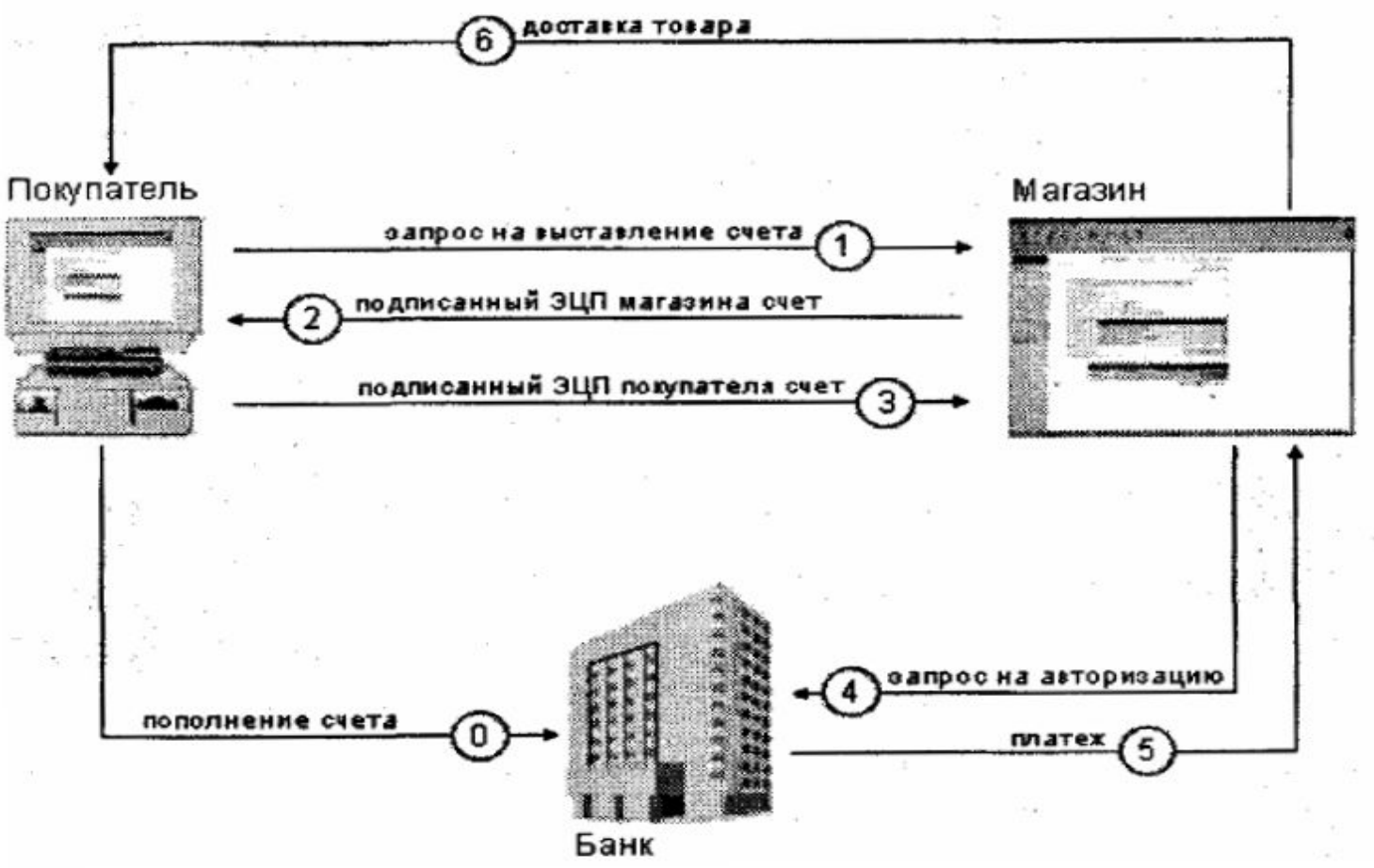


Схема работы платежной системы при оплате покупки со счета в банке "Платина"

4. Подписанный двумя ЭЦП (магазина и покупателя) чек направляется магазином в банк для авторизации.

5. Банк производит обработку подписанного чека:

- □ проверяет наличие в системе магазина и покупателя;
- □ проверяет ЭЦП покупателя и магазина;
- □ проверяет остаток и лимиты средств на счете покупателя;
- □ сохраняет копию чека в базе данных банка.

В результате проверок формируется разрешение или запрет проведения платежа.

1. При *разрешении платежа*:

- □ банк переводит денежные средства со счета покупателя на счет магазина;
- □ банк передает магазину разрешение на оказание услуги (отпуск товара);
- □ магазин оказывает услугу (отпускает товар).

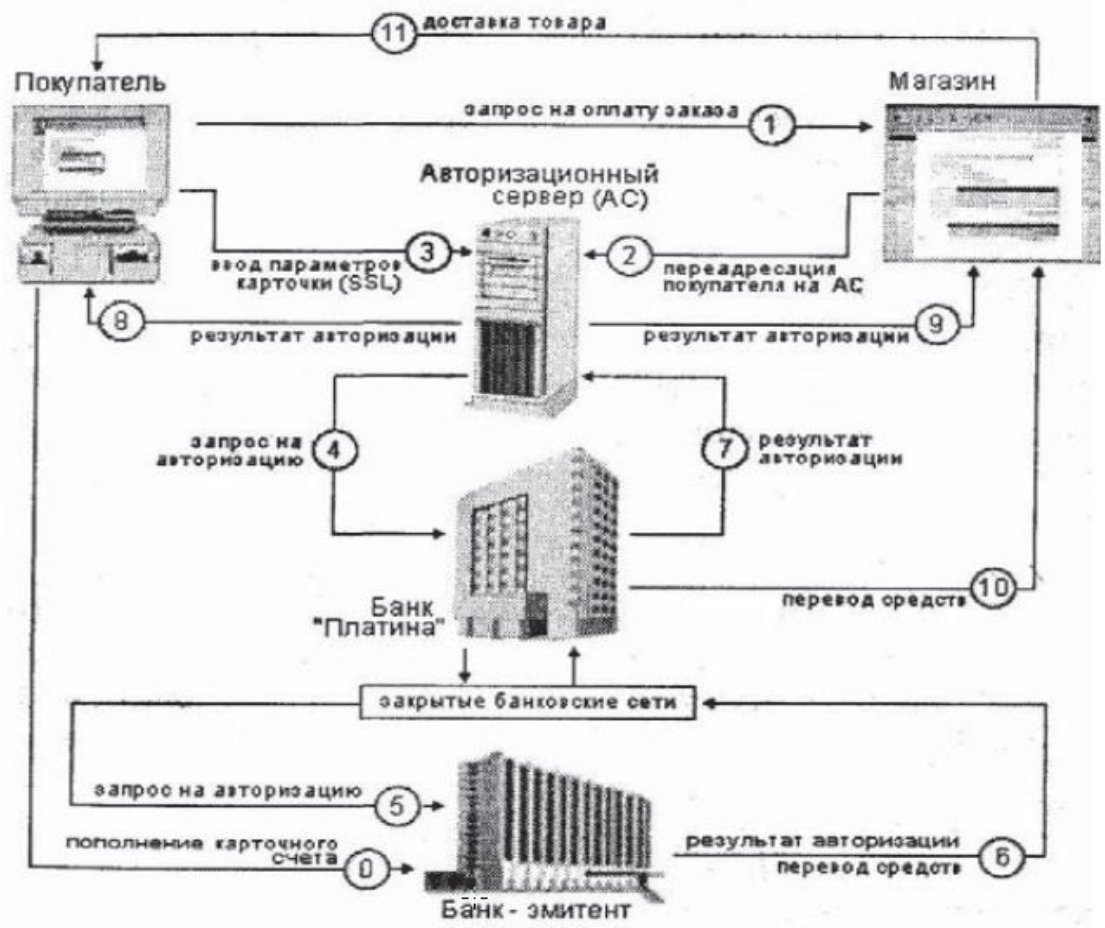
2. При *запрете платежа*:

- □ банк передает магазину отказ от проведения платежа;
- □ покупатель получает отказ с описанием причины.

Покупатель полностью контролирует процесс совершения покупки.

В качестве документального подтверждения совершенной сделки у каждой стороны остаются подписанные ЭЦП чеки, удостоверяющие факт совершения сделки и имеющие юридическую силу.

Другой вариант расчета – оплата по кредитной карточке:



Технология работы платежной системы CyberPlat при обслуживании держателей банковских пластиковых карточек

Основные ***этапы технологии***:

1. Покупатель через Интернет подключается к Web-серверу интернет-магазина, формирует корзину товаров и выбирает форму оплаты по кредитным карточкам.

2. Магазин формирует заказ и переадресует покупателя на сервер авторизации, одновременно туда же передаются код магазина, номер заказа и его сумма.

3. Сервер авторизации устанавливает с покупателем соединение по защищенному протоколу (SSL) и принимает от покупателя параметры его кредитной карточки (номер карточки, дата окончания действия карточки, имя держателя карточки в той транскрипции, как оно указано на карточке). Информация о карточке передается в защищенном виде только на сервер авторизации и не предоставляется магазину при операциях покупателя.

4. Авторизационный сервер производит предварительную обработку принятой информации и передает ее в банк.

5. Банк проверяет наличие магазина в системе, проверяет соответствие операции установленным системным ограничениям. По результатам проверок формируется запрет или разрешение проведения транзакции в карточную платежную систему.

6. При *запрете авторизации* банк передает серверу авторизации отказ от проведения платежа, сервер авторизации передает покупателю отказ с описанием причины, а магазину – отказ с номером заказа.

7. При *разрешении авторизации* запрос на авторизацию передается через закрытые банковские сети банку-эмитенту карточки покупателя или процессинговому центру карточной платежной системы, уполномоченному банком-эмитентом.

8. При *положительном результате авторизации*, полученном от карточной платежной системы, банк передает серверу авторизации положительный результат авторизации, сервер авторизации передает покупателю положительный результат авторизации, а магазину – положительный результат авторизации с номером заказа, магазин оказывает услугу (отпускает товар), банк осуществляет перечисление средств на счет магазина в соответствии с существующими договорными отношениями между банком и магазином.

9. При *отказе в авторизации* банк передает серверу авторизации отказ от проведения платежа, сервер авторизации передает покупателю отказ с описанием причины.

10. Сервер авторизации передает магазину отказ с номером заказа.

Держатель банковской кредитной карточки может ***заранее зарегистрироваться в платежной системе CyberPlat***.

Тогда при совершении покупки ему не требуется указывать данные своей кредитной карточки.

При регистрации в системе CyberPlat покупатель должен указать:

1. Свои *персональные данные* (фамилия, имя, отчество, паспортные данные, адрес электронной почты, почтовый адрес, телефон).

2. *Параметры своей карточки* (название платежной системы, к которой принадлежит карточка, номер карточки, дата окончания действия карточки, имя держателя карточки в той транскрипции, как оно указано на карточке).

Тарифы за пользование системой CyberPlat составляют:

□ для физических лиц клиентов банка "Платина" – *2%* от стоимости проведения платежей (минимум 5 руб.);

□ для держателей банковских кредитных карточек – 4% от стоимости проведения платежей (минимум 5 руб.).

Assist (http://www.assist.ru/) представляет собой систему, которая позволяет в реальном времени проводить авторизацию и обработку платежей, совершаемых при помощи кредитных карт или с лицевых счетов клиентов интернет-провайдеров при помощи любого компьютера, подключенного к Интернету.

В системе *Assist* безопасность платежей обеспечивается использованием шифрования конфиденциальной информации во время ее передачи от клиента в банк для обработки. Дальнейшая передача информации осуществляется по закрытым банковским сетям, взлом которых практически невозможен.

Обработка полученных конфиденциальных данных клиента (реквизиты карты, регистрационные данные и т.д.) производится в back-office системы CyberPlat банка "Платина".

Таким образом, никто, даже продавец, не может получить персональные и банковские данные клиента, включая информацию о его покупках, сделанных в других магазинах.

Для передачи информации о результатах обработки платежа в интернет-магазин используется цифровая подпись на основе асимметричного алгоритма криптографического преобразования с открытым распределением ключей длиной 512 бит. Подделка подписи для ключа такой длины, как уже отмечалось, практически невозможна.

Для шифрования информации на этапе передачи от клиента на сервер системы используется протокол SSL 3.0, сертификат сервера выдан компанией Verisign – признанным центром выдачи цифровых сертификатов. Схема расчетов с использованием кредитных карт выглядит точно так же, как и для системы CyberPlat.

Наибольший интерес в данном случае представляет схема расчетов на основе сертификатов. Клиенты интернет-провайдеров, подключенных к системе Assist, могут оплачивать товары и услуги в интернет-магазинах со своего лицевого счета у провайдера.

В этом случае расчеты происходят по следующей схеме.

1. Internet-провайдер генерирует и выдает своему клиенту цифровой сертификат для идентификации клиента в системе Assist в качестве покупателя. Провайдер передает в расчетный банк системы Assist информацию о выданных сертификатах.

2. Для совершения покупки покупатель через Интернет подключается к Web-серверу магазина, формирует корзину товаров и указывает, что оплата будет производиться со счета у интернет-провайдера.

3. Магазин формирует заказ и переадресует покупателя на авторизационный сервер системы Assist, одновременно на авторизационный сервер передаются код магазина, номер заказа и его сумма.

4. Сервер авторизации системы Assist устанавливает с покупателем соединение по защищенному протоколу (SSL) и принимает от покупателя цифровой сертификат, по которому определяет, к какому интернет-провайдеру принадлежит покупатель. После этого сервер авторизации передает принятую информацию в банк на авторизацию.

5. Банк осуществляет *контроль транзакции*: проверяет наличие в системе магазина и провайдера, проверяет остаток на счете интернет-провайдера и лимиты покупателя.

В результате проверок формируется разрешение/запрет проведения платежа.

6. При разрешении платежа банк переводит денежные средства со счета интернет-провайдера на счет магазина и передает авторизационному серверу Assist результат авторизации.

7. При запрете платежа банк передает серверу авторизации Assist отказ от проведения платежа с указанием причины отказа.

8. Сервер авторизации Assist передает *результат авторизации* покупателю и магазину.

9. В случае положительного результата авторизации интернет-магазин отпускает товар (оказывает услугу).

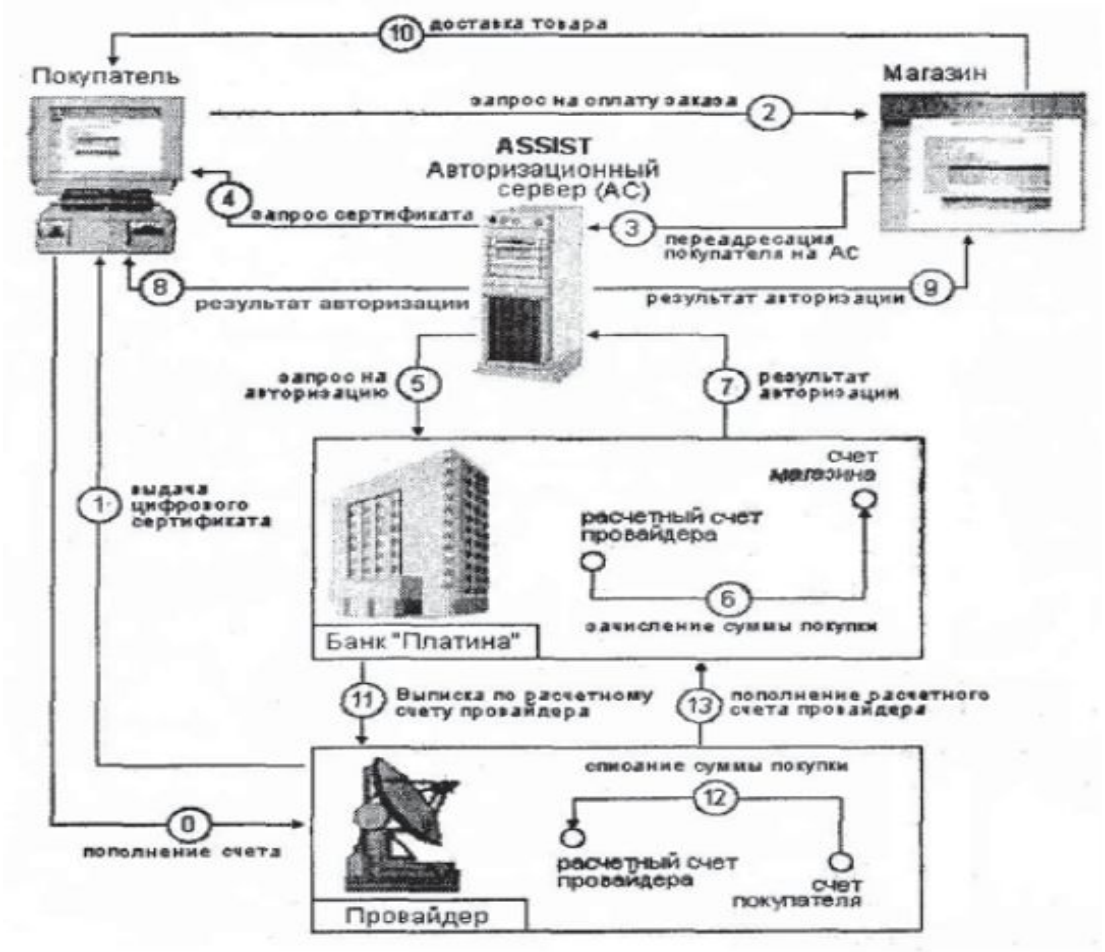


Схема расчета сертификатами платежной системы Assist

Кроме этой схемы, система Assist предоставляет возможность ***осуществления платежей и с помощью кредитных карт***.

Владелец банковской кредитной карточки VISA, Eurocard/ MasterCard, JCB, STB (далее – Покупатель) может оплачивать покупки в интернет-магазинах. Расчеты производятся по следующей схеме.

1. Покупатель через Интернет подключается к Web-серверу Магазина, формирует корзину товаров и выбирает форму оплаты по кредитным карточкам.

2. Магазин формирует заказ и переадресует Покупателя на авторизационный сервер системы Assist, одновременно на авторизационный сервер передаются код Магазина, номер заказа и его сумма.

3. Авторизационный сервер Assist устанавливает с Покупателем соединение по защищенному протоколу (SSL 3.0) и принимает от Покупателя параметры его кредитной карточки (номер карточки, дата окончания действия карточки, имя держателя карточки в той транскрипции, как оно указано на карточке). Информация о карточке передается в защищенном виде только на авторизационный сервер и не предоставляется Магазину при операциях Покупателя.

4. Авторизационный сервер Assist производит предварительную обработку принятой информации и передает ее в расчетный банк системы (далее – Банк).

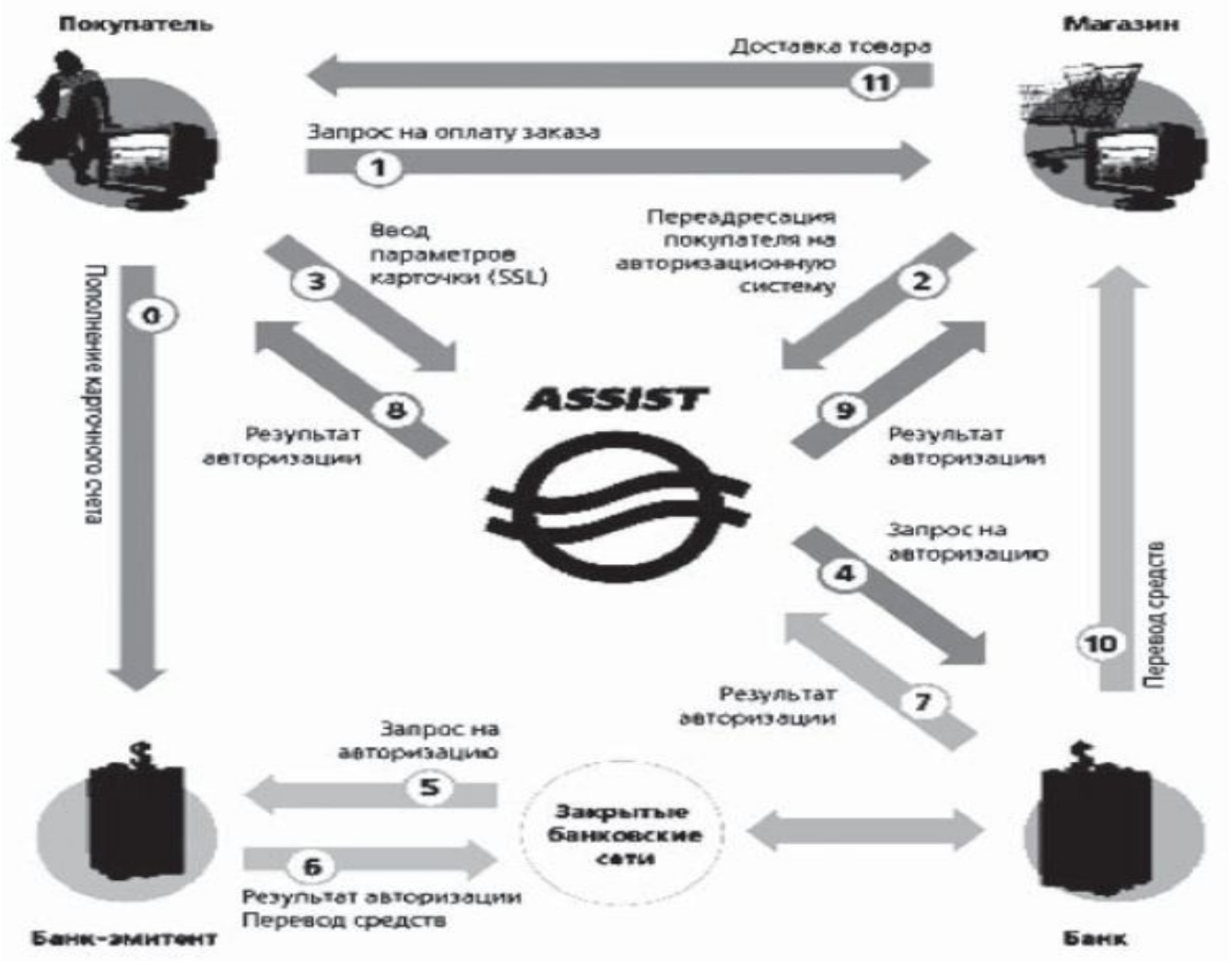


Схема расчетов кредитными картами

5. Банк проверяет наличие такого Магазина в Системе, проверяет соответствие операции установленным системным ограничениям.
По результатам проверок формируется запрет/разрешение проведения авторизации транзакции в карточную платежную систему.

6. При запрете авторизации:

□ Банк передает авторизационному серверу Assist отказ от проведения платежа;

□ авторизационный сервер передает Покупателю отказ с описанием причины;

□ авторизационный сервер передает Магазину отказ с номером заказа.

7. При разрешении авторизации запрос на авторизацию передается через закрытые банковские сети банку-эмитенту карточки Покупателя.

8. При положительном результате авторизации, полученном от карточной платежной системы:

□ банк передает авторизационному серверу Assist положительный результат авторизации;

□ авторизационный сервер передает Покупателю положительный результат авторизации;

□ авторизационный сервер передает Магазину положительный результат авторизации с номером заказа;

□ Банк осуществляет перечисление средств на счет Магазина в соответствии с существующими договорными отношениями между Банком и Магазином;

□ Магазин оказывает услугу (отпускает товар).

9. При отказе в авторизации:

□ Банк передает авторизационному серверу Assist отказ от проведения платежа;

□ авторизационный сервер передает Покупателю отказ с описанием причины;

□ авторизационный сервер передает Магазину отказ с номером заказа.

Получение выписок по транзакциям в системе Assist:

1. Покупатель заходит на авторизационный сервер и запрашивает выписку о проведенных в системе Assist транзакциях, указывая свой код и пароль (если он зарегистрировался в системе).

2. Авторизационный сервер Assist проверяет код Покупателя и его пароль.

3. При положительных результатах проверки авторизационный сервер направляет запрос Покупателя Банку.

4. Банк формирует выписку и передает ее авторизационному серверу.

5. Покупатель получает выписку от авторизационного сервера.