

**МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ, СТАТИСТИКИ И ИНФОРМАТИКИ**

Кафедра: Электронного бизнеса
(наименование кафедры)

Пособие

По дисциплине: Основы интернет-экономики.
Интернет-маркетинг.

Для специальностей: Маркетинг, Антикризисное управление, Бухучет, Анализ и аудит,
Менеджмент, Мировая экономика, Управление персоналом, Финансы и кредит.
(Название дисциплины)

(номер специальности)

Курс: 2
Семестр: 2
Аудиторные занятия: 32
Лекции: 16
Практические занятия : 16

Москва 2003г.

В пособии излагаются теоретические и методические основы организации современной Интернет-экономики. Рассматриваются процессы повсеместного распространения Интернета, современных информационных технологий и появления на их основе нового направления - Интернет-экономика. Описываются основные элементы инфраструктуры Интернет-экономики - устройство Сети, ее службы, методы обеспечения безопасности, платежные Интернет-системы. Освещаются вопросы построения системы маркетинга в Интернете - среда, организация маркетинговых исследований, вопросы построения товарной, ценовой, распределительной и коммуникативной политики.

Развитие информационных технологий

Одной из главных движущих сил происходящих сегодня революционных изменений в методах ведения бизнеса являются информационные технологии. Они стали незаменимым средством взаимодействия всех субъектов рынка, инструментом ведения бизнеса, применяемым для осуществления большинства бизнес процессов компаний.

Под термином информационные технологии понимается совокупность программно-технических средств вычислительной техники, а также приемов, способов и методов их применения для выполнения функций сбора, хранения, обработки, передачи и использования информации в конкретных предметных областях.

Понятие информационных технологий включает большое количество составляющих: аппаратные платформы, операционные системы, языки программирования и средства разработки приложений, сетевые технологии, базы данных и многие другие. Можно выделить несколько составляющих, развитие и совершенствование которых в наибольшей степени определило и продолжает способствовать применению информационных технологий для успешного ведения бизнеса:

1. Появление и повсеместное распространение глобальной компьютерной сети Интернет;
2. Создание аппаратных и программных комплексов, обеспечивших автоматизацию бизнес процессов компаний;

3. Развитие стандартов и средств взаимодействия информационных систем.

Рассмотрим каждое из отмеченных направлений более подробно.

Появление и развитие глобальной сети Интернет

Первым важным элементом, являющимся одной из основ предмета настоящей книги, является Интернет. Появление и развитие Интернета тесно связано с достижениями многих смежных областей. Это и развитие сетевых технологий, и совершенствование операционных систем, и развитие языков программирования, и многих других. За свою более чем тридцатилетнюю историю Интернет пережил много событий. Основополагающие из них описаны в представленной ниже краткой истории глобальной Сети от зарождения до ее коммерциализации.

Зарождение глобальной Сети

Родиной Интернета является США. Его зарождение произошло в конце 60-х годов из проекта сети с коммутацией пакетов ARPANET (Advanced Research Project Agency Network). Первоначально Интернет разрабатывался с целью обеспечения взаимодействия удаленных компьютеров и задумывался как децентрализованная территориально распределенная сеть с множеством альтернативных точек хранения и путей распространения информации. Предполагалось, что это позволит обеспечить надежное взаимодействие компьютеров Министерства обороны США даже в случае, если часть сети выйдет из строя вследствие военных действий, например, ядерных взрывов.

Развитие компьютерных сетей

В 1979 г. состоялась встреча, в которой приняли участие ряд университетов, DARPA и Национальный научный фонд США (National Science Foundation, NSF). На этой встрече было решено создать сеть CSnet (Computer Science Research Network), главным источником финансирования которой стал NSF. Чуть позже, в 1980 г. было предложено связать вместе ARPANet и CSnet через шлюз с использованием протоколов TCP/IP, чтобы все подмножества сетей CSnet располагали доступом к шлюзу в ARPANet. Это событие можно считать преобразованием Интернета в содружество независимых сетей, пришедших к соглашению относительно способа межсетевого общения.

Следующей составной частью Интернета стала сеть с названием Bitnet (Because It's Time Network). Эта сеть представляла собой среду, в которой обмен сообщениями и новостями осуществлялся через механизм списков рассылки Listserv, который напоминал используемое в Usenet разделение новостей на группы. Пользователи Bitnet выбирали подходящие им списки и подписывались на них. Статьи и сообщения рассылались только подписчикам, в отличие от Usenet, передававшей новости и сообщения от одного сервера новостей к другому.

В 1984 г. Сан-Франциско появилась другая важная сеть— FidoNet . За год до этого Том Дженнингс (Tom Jennings) написал программу, которая позволяла реализовать систему BBS на персональном компьютере, назвав ее FidoBBS. Пакет быстро приобрел популярность, и вскоре Fido bulletin boards распространились повсюду. Через некоторое время Дженнингс выпустил сетевой пакет FidoNet, с помощью которого две системы FidoBBS могли связываться между собой посредством модема и телефонной линии. В этом пакете была применена технология пакетной коммутации, улучшенная ARPANet, Usenet и другими сетями. В результате абоненты FidoBBS смогли посылать друг другу сообщения электронной почты и создавать дискуссионные группы, подобно Usenet или Bitnet. В 1987 г. пакет UUCP, первоначально разработанный для применения в среде UNIX, был «привязан» к IBM PC, что дало возможность совместить Usenet с FidoNet.

Во второй половине 80-х Национальный научный фонд США создал собственную высокоскоростную сеть с целью поддержки требований стандартов на качество связи в сетях, объединяющих большие компьютерные центры. NSFNet является в настоящее время одной из крупнейших сетей в сообществе Интернет. Вслед за NSF в Интернет включились NASA и DOE (Министерство энергетики США) в форме сетей NSINet и ESNet. В 1983 г. часть ARPANet, обслуживающая военные организации, выделилась в отдельную сеть Milnet, которая вскоре исчезла из поля зрения. Оставшаяся же часть ARPANet была постепенно замещена NSFNet, и в 1990 г. этот процесс был полностью завершен. На рис. 1.2 показана карта сети Интернет по состоянию на август 1987 г. (<http://www.cybergeography.org/atlas/historical.html>).

В результате всех преобразований исключительную привилегию управлять сетью NSFNet получила корпорация ANS. Также был выпущен документ, излагающий принципы допустимого использования (acceptable-use policy) системы

высокоскоростных магистралей NSF backbone. Согласно этим принципам практически любой желающий мог пользоваться NSF backbone до тех пор, пока это употребление непосредственно не было связано с коммерческими или личными интересами.

В 1990 г. Федеральный Совет по информационным сетям (Federal Networking Council) отменил правило, согласно которому для присоединения к Интернету была необходима рекомендация какого-либо государственного органа. Это решение послужило началом широкого притока в Интернет коммерческих организаций самого разного масштаба, поскольку теперь доступ в него можно было получить без каких бы то ни было серьезных оговорок или обоснований.

В 1992 г. фонд NSF официально заявил, что он является не более чем одним из клиентов ANS, и все ограничения, изложенные в принципах acceptable-use policy, распространяются только на собственный трафик NSF. Это явилось дополнительным стимулом для коммерческих организаций: согласно статистике NSF, в общем объеме регистрируемых IP-адресов доля адресов с окончанием .com (commerce) на 1994 г. составила 51,3 %. Для сравнения укажем, что доля научных и образовательных организаций составила 32,7 %, а доля военных и государственных организаций — 16 %.

World Wide Web

Одним из наиболее важных событий в истории Интернета, с точки зрения развития бизнеса, и, в частности, электронной коммерции, стало создание так называемой «всемирной паутины» — среды World Wide Web (WWW), в основу которой легла технология гипертекста.

История World Wide Web началась в марте 1989 г., когда Тим Бернс Ли (Tim Bernes Lee) выступил с проектом телекоммуникационной среды для проведения совместных исследований в области физики высоких энергий, а затем в 1991 г. Европейская лаборатория практической физики (CERN), находящаяся в Швейцарии, объявила на весь мир о создании новой глобальной информационной среды World Wide Web.

С помощью языка разметки гипертекста (Hypertext Markup Language, HTML), представляющего собой набор инструкций для форматирования документов, паутина WWW унифицировала и связала воедино весь грандиозный объем информации,

который находился в Интернете в форме текстов, изображений и звукового сопровождения.

Появление WWW и программ просмотра web-страниц — браузеров дало возможность пользователям работать в Интернете, используя навыки, полученные ими ранее при работе на PC с графическими «оболочками» типа MS Windows. При этом разработчику стало совершенно необязательно помещать всю графическую, текстовую и прочую информацию целиком в один документ. Составные части документа, а также его подразделы могут храниться на совершенно разных web-серверах, а с помощью URL-указателей, размещаемых в структуре документа, все эти части могут связываться и образовывать гипертекстовый документ.

Взаимодействие через web-браузер

Появление Интернета значительно удешевило ведение электронной коммерции за счет низкой себестоимости передачи информации и привело к возникновению ее качественно новых форм. Одной из таких форм стали системы уровня «бизнес-бизнес» (B2B) и «бизнес-потребитель» (B2C), в которых ключевым моментом является взаимодействие через web-браузер, а технологии EDI не используются или их применение носит вторичный характер.

Функционируют они следующим образом. Компания-продавец размещает на своем web-сайте (с открытым или ограниченным доступом) интерфейс, с помощью которого конечный потребитель или фирма-партнер может, например, сформировать и разместить заказ в информационной системе компании-продавца. После этого специальное программное обеспечение и система ERP компании-продавца сами обрабатывают заказ, проводя вторичные транзакции, необходимые, скажем, для перевода денег со счета на счет или формирования заказов у компании, занимающейся доставкой товара и т. д.

Системы электронной коммерции позволяют покупателю не общаться с продавцом, не тратить время на хождение по магазинам, а также иметь более полную информацию о товарах. Продавец же может быстрее реагировать на изменение спроса, анализировать поведение покупателей, экономить средства на персонале, аренде помещений и т. п.

Главные преимущества для продавца состоят в расширении круга покупателей, в который сразу попадают те компании, которым не в состоянии из-за большой стоимости внедрить EDI, в возможности использовать информационные технологии для осуществления продаж конечным потребителям, то есть выйти на рынок «бизнес-потребитель» (B2C), а также в устранении возможных посредников в торговле. В качестве одного из ярких примеров можно привести корпорацию Dell, которая одна из первых сделала ставку на виртуальную форму ведения бизнеса и быстро добилась успеха.

Интернет-маркетинг

Развитие информационных технологий, среди которых одно из ключевых мест занял Интернет, появление и бурный рост электронной коммерции стали основой для появления нового направления в современной концепции маркетинга взаимодействия — Интернет-маркетинга.

Под термином Интернет-маркетинг понимается теория и методология организации маркетинга в гипермедийной среде Интернета.

Интернет обладает уникальными характеристиками, значительно отличающимися от характеристик традиционных инструментов маркетинга. Одним из основных свойств среды Интернета является ее гипермедийная природа, характеризующаяся высокой эффективностью в представлении и усвоении информации, что значительно повышает возможности маркетинга в усилении взаимосвязи предприятий и потребителей.

Кроме того, роль, выполняемая Интернетом, не ограничиваются только коммуникативными функциями, а также включает в себя возможность заключения сделок, совершение покупок и проведение платежей, придавая ему черты глобального электронного рынка.

Особенности Интернет-маркетинга

Использование Интернета привносит новые особенности и преимущества по сравнению с маркетингом, основанном на традиционных технологиях. Вот некоторые из них:

Переход ключевой роли от производителей к потребителям

Одним из наиболее фундаментальных качеств, привнесенных Интернетом в мир современной коммерции, является переход ключевой роли от производителей к потребителям. Интернет сделал реальностью для компаний возможность привлечь внимание нового клиента всего за десятки секунд, проведенных им перед экраном компьютера. Однако в то же время он дал возможность тому же пользователю за несколько щелчков мыши перейти к любому из конкурентов. В такой ситуации внимание покупателей становится самой большой ценностью, а установленные взаимоотношения с клиентами главным капиталом компаний.

Глобализация деятельности и снижение транзакционных издержек

Интернет значительно изменяет пространственный и временной масштабы ведения коммерции. Он является глобальным средством коммуникации, не имеющим каких-либо территориальных ограничений, при этом стоимость доступа к информации не зависит от удаленности от нее, в противоположность традиционным средствам, где эта зависимость прямо пропорциональна. Таким образом, электронная коммерция позволяет даже самым мелким поставщикам достигать глобального присутствия и заниматься бизнесом в мировом масштабе. Соответственно, заказчики также получают возможность глобального выбора из всех потенциальных поставщиков, предлагающих требуемые товары или услуги независимо от географического расположения. Расстояние между продавцом и покупателем играет роль лишь с точки зрения транспортных издержек уже на этапе доставки товаров.

Временной масштаб в среде Интернета также значительно отличается от обычного. Высокая эффективность коммуникативных свойств Интернета обеспечивает возможность сокращения времени на поиск партнеров, принятие решений, осуществление сделок, разработку новой продукции, и т. д. Информация и услуги в Интернете доступны круглосуточно. Кроме того, его коммуникативные характеристики обладает высокой гибкостью, позволяющей легко производить изменения представленной информации, и, тем самым, поддерживать ее актуальность без временной задержки и затрат на распространение.

Названные эффекты также приводят к значительному сокращению транзакционных издержек, то есть издержек, связанных с налаживанием и поддержанием взаимодействия между компанией, ее заказчиками и поставщиками. При этом стоимость коммуникаций, по сравнению с традиционными средствами,

становится минимальной, а их функциональность и масштабируемость значительно возрастают.

Персонализация взаимодействия и переход к маркетингу «один-одному».

Используя средства электронного взаимодействия, компании могут получать подробную информацию о запросах каждого индивидуального заказчика и автоматически предоставлять продукты и услуги, соответствующие индивидуальным требованиям. Одним из простых примеров может служить персональное представление web-сайта для каждого из клиентов или партнеров компании. В результате Интернет позволяет перейти от массового маркетинга к маркетингу «один-одному». В таблице 1.1 приведены данные по сравнению характеристик массового маркетинга с маркетингом «один-одному».

Таблица 1.1. Сравнение массового маркетинга и маркетинга «один-одному»

Массовый маркетинг	Маркетинг «один к одному»
Усредненный покупатель	Отдельный покупатель
Анонимность покупателя	Характеристики покупателя
Стандартный продукт	Специальное маркетинговое предложение
Массовое производство	Специальное производство
Массовое распределение	Индивидуальное распределение
Массовая реклама	Индивидуальное обращение
Массовое продвижение	Индивидуальные стимулы
Одностороннее обращение	Двусторонние обращения
Масштабная экономика	Целевая экономика
Доля рынка	Доля покупателей
Все покупатели	Потенциально прибыльные покупатели

Привлечение покупателей	Удержание покупателей
-------------------------	-----------------------

Снижение трансформационных издержек

Снижение трансформационных издержек может достигаться за счет оптимального выбора структуры товарного ассортимента, сокращения времени на разработку и внедрение новой продукции, обоснованной политики ценообразования, снижения числа посредников, затрат на сбыт и т. д.

Например, одним из способов снижения трансформационных издержек может быть сокращение каналов распространения товаров. Причиной сокращения каналов распространения является возможность для фирм взять на себя функции, традиционно выполняемые специалистами промежуточных звеньев, так как Интернет обладает более эффективной возможностью взаимодействия с потребителями и одновременно позволяет отслеживать информацию о потребителях.

Особый случай — продукты и услуги, которые могут быть доставлены электронным способом. При этом путь доставки сокращается максимально. Электронный способ широко применяется для доставки цифровых продуктов индустрии развлечений (фильмы, видео, музыка, журналы и газеты), информации, средств обучения и эффективно используется компаниями, занимающимися разработкой и поставкой программного обеспечения.

Выводы

Существует ряд направлений, развитие и совершенствование которых в наибольшей степени определило и продолжает способствовать применению информационных технологий для успешного ведения бизнеса: появление и повсеместное распространение глобальной компьютерной сети Интернет; создание аппаратных и программных комплексов, обеспечивших автоматизацию бизнес процессов компаний; развитие стандартов и средств взаимодействия информационных систем.

Появление и коммерциализация Интернета привели к появлению новой категории бизнеса — электронному бизнесу, под которым понимается любая

активность с использованием возможностей глобальных информационных сетей для ведения коммерческой деятельности. Важнейшим составным элементом электронного бизнеса является электронная коммерция, в которую входят любые формы сделок, когда взаимодействие сторон осуществляется электронным способом.

По типу взаимодействующих субъектов электронный бизнес делится на следующие основные категории: бизнес-бизнес (business-to-business, B2B); бизнес-потребитель (business-to-consumer, B2C); бизнес-администрация (business-to-administration, B2A); потребитель-администрация (consumer-to-administration, C2A); потребитель-потребитель (consumer-to-consumer, C2C). Наиболее развитыми из них на сегодняшний день являются категории B2B и B2C, однако перспективы развития других категорий также достаточно велики.

Развитие информационных технологий, появление и бурный рост электронной коммерции стали основой для появления нового направления в современной концепции маркетинга взаимодействия — Интернет-маркетинга, под которым понимается теория и методология организации маркетинга в среде Интернета. Эпоха Интернет-маркетинга характеризуется следующими отличительными особенностями: глобализация сфер деятельности; окончательный переход ключевой роли от производителей к потребителям; персонализация взаимодействия и переход к маркетингу «один-одному»; снижение транзакционных и трансформационных издержек.

С информационной точки зрения, Интернет — это совокупность миллионов информационных центров, называемых web-сайтами, содержащих терабайты разнообразной информации и тесно связанные множеством взаимосвязей, образующих «всемирную паутину».

С социальной и экономической точки зрения, Интернет — это единая среда общения, коммуникаций, развлечения и ведения бизнеса.

С технической точки зрения Интернет — это совокупность десятков тысяч независимых сетей и миллионов компьютеров.

Так что же такое Интернет?

Определение Интернета, данное Федеральным Советом по информационным сетям (Federal Networking Council) 24 октября 1995 г., гласит: «Интернет — глобальная

информационная система, части которой логически взаимосвязаны друг с другом посредством уникального адресного пространства, основанного на протоколе IP (Internet Protocol) или его последующих расширениях, способная поддерживать связь посредством комплекса протоколов TCP/IP (Transmission Control Protocol/Internet Protocol), их последующих расширений или других совместимых с IP протоколов, и публично или частным образом обеспечивающая, использующая или делающая доступной коммуникационную службу высокого уровня». Другими словами, Интернет можно определить как взаимосвязь сетей, базирующуюся на едином коммуникационном протоколе— TCP/IP.

Таким образом, основу сети Интернет составляет семейство протоколов TCP/IP.

Но достаточно ли их, чтобы Интернет смог быть использован в маркетинге, электронной коммерции или просто для двух людей?

Конечно, нет. Для этого существует громадное количество компонентов, в конечном итоге составляющих среду, которая дает пользователям широчайший диапазон действий, и которая за небольшой отрезок времени длиной в десятилетие завоевала популярность и признание многих миллионов людей по всему миру.

Поэтому, для того чтобы далее можно было перейти непосредственно к рассмотрению всех составляющих Интернет-маркетинга, в этой главе мы рассмотрим совокупность вопросов, раскрывающих ряд базовых элементов функционирования Сети.

Принципы построения сети Интернет

Для начала рассмотрим общую схему построения сети Интернет (рис 2.1).

Основным и наиболее распространенным устройством доступа в Интернет для конечного пользователя является компьютер. Для расширения возможностей он может быть оснащен микрофоном, видеокамерой, звуковыми колонками и другими устройствами, превращающими его в мультимедийный центр. Компьютер может находиться дома, в офисе фирмы или в любом другом месте, обладающем современными средствами коммуникации.

Доступ в Интернет, который предоставляется организациями, называемыми поставщиками услуг Интернета (Internet Service Provider, ISP), пользователь может

получить, например, из дома через модем или из офиса через локальную сеть организации. Для подключения к поставщику услуг Интернета могут использоваться обычные телефонные линии, кабельные сети телевидения, радио каналы связи или спутниковую связь.

Поставщик обычно имеет одно или несколько подключений к магистральным каналам (backbones) или крупным сетям, которые образуют главную кровеносную систему Интернета.

Границы Интернета довольно расплывчаты. Любой компьютер, подключенный к нему, уже можно считать его частью, и уж тем более это относится к локальной сети предприятия, имеющего выход в Интернет.

Web-серверы, на которых располагаются информационные ресурсы, могут находиться в любой части Интернета: у поставщика услуг, в локальной сети предприятия и т. д., необходимо лишь соблюдение главного условия — они должны быть подключены к Интернету, чтобы пользователи Сети могли получить доступ к их службам. В качестве служб могут выступать электронная почта, FTP, WWW и другие, о которых будет рассказано чуть позже.

Информационной составляющей служб являются самые разнообразные источники. Это могут быть данные, поступающие от информационных агентств и с финансовых рынков, фотографии, документация, звуковые фрагменты, информация, присланная пользователями и т. д. Службы в совокупности с их информационной составляющей являются той главной целью, к которой стремятся пользователи, и которой они достигают посредством подключения к Интернету.

Семейство протоколов TCP/IP

Поскольку семейство протоколов TCP/IP является основой построения Интернета, рассмотрим эти протоколы более подробно.

В пределах каждой физической компьютерной сети подсоединенные к ней компьютеры используют ту или иную сетевую технологию: Ethernet, Token Ring, FDDI, ISDN, соединение типа «точка-точка», а в последнее время к этому списку добавились сеть ATM и беспроводные технологии. Между механизмами коммуникаций, зависящими от данных физических сетей, и прикладными системами встраивается

программное обеспечение, которое делает возможным соединение различных физических сетей друг с другом. При этом детали подобного соединения «скрыты» от пользователей, которым предоставляется возможность работать как бы в одной большой физической сети.

Для соединения двух и более сетей используются маршрутизаторы (routers) — компьютеры, которые физически соединяют сети друг с другом и с помощью специального программного обеспечения передают пакеты из одной сети в другую.

Технология Интернета не навязывает какой-то определенной топологии межсетевых соединений. Добавление новой сети к Интернету не влечет за собой ее подсоединения к некоторой центральной точке коммутации или установке непосредственных физических соединений со всеми уже входящими в Интернет сетями. Маршрутизатор «знает» топологию Интернета за пределами тех физических сетей, которые он соединяет, и, основываясь на адресе в сети назначения, передает пакет по тому или иному маршруту.

В Интернете используются универсальные идентификаторы (адреса) подсоединенных к Сети компьютеров, поэтому любые две машины имеют возможность взаимодействовать друг с другом. В нем также реализован принцип независимости пользовательского интерфейса от физической сети, то есть существует множество способов установления соединений и передачи данных, одинаковых для всех физических сетевых технологий.

С точки зрения конечных пользователей, Интернет представляет собой единую виртуальную сеть, к которой подсоединены все компьютеры — независимо от их реальных физических соединений.

Фундаментальным принципом Интернета является равнозначность всех объединенных с его помощью физических сетей: любая система коммуникаций рассматривается как компонент Интернета, независимо от ее физических параметров, размеров передаваемых пакетов данных и географического масштаба.

Семейство протоколов TCP/IP позволяет построить универсальную сеть, осуществляющую указанные выше принципы. Оно включает в себя протоколы 4-х уровней коммуникаций.

Уровень сетевого интерфейса отвечает за установление сетевого соединения в конкретной физической сети. На этом уровне работают драйвер устройства в операционной системе и соответствующая сетевая плата компьютера.

Сетевой уровень — основа TCP/IP. Именно на этом уровне реализуется принцип межсетевого соединения, в частности маршрутизация пакетов через Интернет. На сетевом уровне протокол реализует ненадежную службу доставки пакетов по сети от системы к системе без установления соединения (connectionless packet delivery service). Это означает, что будет выполнено все необходимое для доставки пакетов, однако эта доставка не гарантируется. Пакеты могут быть потеряны, переданы в неправильном порядке, продублированы и т. д. Служба, работающая без установления соединения, обрабатывает пакеты независимо друг от друга. Но главное, что именно на этом уровне принимается решение о маршрутизации пакета по межсетевым соединениям.

Надежную передачу данных реализует следующий, транспортный уровень, на котором два основных протокола, TCP и UDP, осуществляют связь между машиной — отправителем пакетов и машиной — адресатом пакетов.

Наконец, прикладной уровень — это приложения типа клиент-сервер, базирующиеся на протоколах нижних уровней. В отличие от протоколов остальных трех уровней, протоколы прикладного уровня занимаются деталями конкретного приложения и для них обычно не важны способы передачи данных по сети. Среди основных приложений TCP/IP, имеющих практически в каждой его реализации, — протокол эмуляции терминала Telnet, протокол передачи файлов FTP, протокол электронной почты SMTP, протокол управления сетью SNMP, используемый в системе World Wide Web протокол передачи гипертекста HTTP и др.

На рис. 2.3 показано, как осуществляется взаимодействие двух компьютеров из разных сетей с использованием стека протоколов TCP/IP. Программное обеспечение IP-протокола с помощью маршрутизатора передает пакеты из одной сети Ethernet в другую. Протоколы верхних уровней, прикладного и транспортного, осуществляют соединения между компьютерами, клиентом и сервером приложения, в то время как IP обеспечивает связь между конечной и промежуточной системами.

Поскольку в Интернете детали физических соединений скрыты от приложений, прикладной уровень совершенно «не заботится» о том, что клиент и сервер приложения работают в разных сетях, и что в качестве канального протокола в обеих сетях используется протокол Ethernet. Между конечными системами может быть несколько десятков маршрутизаторов и множество промежуточных физических сетей различных типов. Приложение в любом случае будет воспринимать этот конгломерат как единую физическую сеть. Это обуславливает основную силу и привлекательность технологии Интернета.

Коммуникационная система считается универсальной, если при помощи нее два любых компьютера могут взаимодействовать друг с другом. Для того чтобы добиться такой универсальности, необходимо установить глобальный метод идентификации компьютеров в распределенной системе для доступа к ним. В TCP/IP выбрана схема идентификации, аналогичная адресации в физических сетях. Каждому сетевому интерфейсу присваивается уникальный 32-битный адрес (IP-адрес). IP-адрес компьютера имеет определенную структуру. Она задает идентификатор сети, к которой подсоединен компьютер, и уникальный идентификатор самого компьютера. На рис. 2.4 показаны различные классы IP-адресов.

Для 32-битных IP-адресов принята десятичная нотация, в которой каждый из четырех байтов адреса записывается десятичным числом. Адреса класса C, например, охватывают диапазон от 192.0.0.0 до 223.255.255.255. Структура адресов различных классов делает достаточно очевидным их применение. Адреса класса C, в которых 21 бит отводится для идентификатора сети и только 8 бит для идентификатора оконечного узла сети (хоста), присваиваются компьютерам локальных сетей небольших организаций, которые объединяют до 255 машин. Более крупные организации могут получить адреса класса B, которые способны обслужить до 256 сетей, в состав которых входит до 64 тысяч рабочих станций. И наконец, адреса класса A присваиваются компьютерам, подключенным к ограниченному числу глобальных сетей очень большого масштаба, например, в Arpanet.

Компьютеры, подсоединенные к нескольким физическим сетям (multihomed), имеют несколько IP-адресов — по одному для каждого сетевого интерфейса. Соответственно, эти IP-адреса различаются своими сетевыми идентификаторами. Таким образом, адрес характеризует не отдельную машину, а ее сетевое соединение.

Помимо адресов, предназначенных для одного хоста (unicast), существуют также широковещательные (broadcast) и групповые (multicast) адреса.

Уникальный IP-адрес присваивается каждому сетевому интерфейсу. Назначение идентификаторов хостов обычно находится в ведении системного администратора или поставщика услуг Интернета, а выделение адресов сетям, объединенным в мировую Сеть, в юрисдикции специальной организации — InterNIC (Internet Network Information Center Internet).

В связи с бурным ростом Интернета 32-битная схема адресации нынешней версии IP — IPv4, уже не удовлетворяет потребности мировой Сети. Новая версия, IPv6, проект которой был обнародован в 1991 г., призвана решить эти проблемы. IPv6 обеспечит 128-битный формат IP-адреса и будет поддерживать автоматическое назначение адресов.

TCP/IP предоставляет пользователям возможность работать не только с адресами компьютеров, но и с их именами. Это обеспечивается при помощи распределенной базы данных — доменной системы имен (Domain Name System, DNS), которая обеспечивает отображение IP-адресов в имена хостов. Эта база данных является распределенной, поскольку ни один объект в Интернете не обладает всей информацией об именах компьютеров. Каждый объект поддерживает свою базу данных и имеет серверную программу, к которой могут обращаться другие системы (клиенты) в сети.

Открытость, масштабируемость, универсальность и простота использования — неоспоримые преимущества TCP/IP, но у этого семейства протоколов есть и очевидные недостатки. Столь привлекательная простота доступа оборачивается для Интернета серьезнейшей проблемой защиты информации, которая приобретает особую остроту сейчас, когда мировая Сеть все активнее используется для электронной коммерции. Неупорядоченность передачи пакетов и невозможность отследить маршрут их продвижения также являются важными проблемами, поскольку препятствуют реализации таких необходимых в современных коммуникациях возможностей, как передача мультимедийных данных в реальном времени. Наконец, как уже упоминалось, предоставляемый нынешней версией протокола IP объем адресного пространства, особенно в связи с его неэффективным использованием, уже с большим трудом позволяет удовлетворять потребности гигантской и все более разрастающейся Сети.

Многие указанные проблемы должны быть сняты реализацией уже упоминавшегося протокола IPv6. Помимо четырехкратного увеличения размера адреса, что обеспечит адресное пространство объемом около 4 квадриллионов адресов в сравнении с современными 4 млрд, новый стандарт обеспечивает осуществление встроенных функций защиты от несанкционированного доступа, поддержку передачи данных мультимедиа в реальном времени и возможности автоматического реконфигурирования адресов.

Контролем использования TCP/IP, определением основных направлений развития, разработкой и утверждением стандартов сегодня занимается несколько организаций. Основной из них является ISOC (Internet Society) — профессиональное сообщество, которое занимается общими вопросами эволюции и роста Интернета как глобальной инфраструктуры исследовательских коммуникаций.

Под управлением ISOC действует IAB (Internet Architecture Board) — организация, в ведении которой находится технический контроль и координация Интернета. IAB координирует направления исследований и новых разработок для TCP/IP и является конечной инстанцией при определении новых стандартов для Интернета.

В IAB входят две основные группы: IETF (Internet Engineering Task Force) и IRTF (Internet Research Task Force). IETF — инженерная группа, которая занимается решением ближайших технических проблем Интернета. Она делится на девять подгрупп в соответствии с основными областями (приложения, маршрутизация и адресация, защита информации и т. д.) и определяет спецификации, которые затем становятся стандартами Интернета. В частности, протоколы IPv6 и DHCP являются плодом усилий IETF. В свою очередь, IRTF координирует долгосрочные исследовательские проекты по протоколам TCP/IP и технологии Интернета в целом.

Разнообразная документация, связанная с Интернетом, предложения по стандартам и сами официальные стандарты протоколов TCP/IP публикуются в серии технических сообщений Internet Request for Comments, или RFC. RFC могут быть короткими или длинными, излагать глобальные концепции или описывать детали того или иного проекта, формулировать официальный стандарт или давать предложения по новым протоколам.

Система доменных имен

Как упоминалось ранее, для того чтобы обращение ко всем ресурсам Интернета было наиболее простым и прозрачным с точки зрения пользователей, в Сети действует система доменных имен (Domain Name System, DNS). Она предназначена для того, чтобы любой ресурс помимо уникального IP-адреса имел легко запоминающееся доменное имя. Служба доменных имен призвана соотносить IP-адреса с доменным именем машины, и наоборот.

Доменное имя любого ресурса состоит из следующих основных частей: названия зоны, собственного названия домена и названия имени машины. Например: `www.rbc.ru`. Это доменное имя говорит, что ресурс расположен в географическом домене `ru`, имеет собственное название `rbc` и функциональное имя `www`, то есть выполняет функции WWW-сервера.

Имена зон условно можно разделить на «организационные» и «географические». В старшей зоне (доменах первого уровня) зарегистрированы следующие организационные зоны:

- `com` — commercial (коммерческие);
- `edu` — educational (образовательные);
- `gov` — government (правительственные);
- `mil` — military (военные);
- `net` — network (организации, обеспечивающие работу сети);
- `org` — organization (некоммерческие организации).

Последнее время активно обсуждается введение новых доменов первого уровня. Уже введены в строй и существует возможность регистрации доменов в двух новых зонах: `biz` и `info`. Зона `info` открыта для всех желающих, а `biz` предназначена для регистрации коммерческих организаций. Также предлагается введение таких общих доменов, как `name` и `pro`, специализированных — `museum`, `coop`, `aero` и ряда других.

Каждая страна (государство) имеет свой географический домен из двух букв. Вот домены некоторых из стран:

- `ca` — Canada (Канада);
- `de` — Germany (Германия);
- `fi` — Finland (Финляндия);

- fr — France (Франция);
- jp — Japan (Япония);
- ru — Russia (Россия);
- ua — Ukraine (Украина);
- uk — United Kingdom (Англия).

В зонах государств опять же имеются организационные и географические зоны. Организационные зоны в большинстве своем повторяют структуру организационных зон верхнего уровня, разве что вместо com может использоваться имя со. Географические зоны выделяются по городам, областям и другим территориальным образованиям. Непосредственно в них размещаются домены организаций или домены персональных пользователей.

С левого конца доменного имени находятся имена машин. Имена бывают собственные и функциональные. Имена собственные каждый придумывает в меру своей фантазии, а имена функциональные вытекают из функций, выполняемых компьютером, например:

- www — HTTP-сервер (WWW-сервер);
- ftp — FTP-сервер.

Процессом оформления и поддержания доменных имен занимаются ряд специализированных организаций. Регистрацией доменов в зоне com (коммерческие серверы), edu (образовательные учреждения), org (некоммерческие организации), net (сетевые проекты) занимается организация InterNIC (Internet Network Information Center), находящаяся в США по адресу www.internic.net. В Европе ее функцию взяла на себя организация RIPE, имеющая адрес www.ripe.net. В России регистрацией доменов в зоне ru занимается RIPN с адресом www.ripn.net.

Организации или физическому лицу, желающим зарегистрировать свой домен, следует обращаться к администратору какого-либо уже существующего домена.

В любом случае первоначально необходимо проверить, зарегистрировано ли уже то имя, которое вы желаете взять. Это можно сделать по адресам www.register.com (для доменов com, org, net и edu) и www.ripn.net/nic/whois/ (для зоны ru). Если выбранное имя уже зарегистрировано, то остается попытаться придумать другое. Также можно

попробовать выйти на организацию или частное лицо, владеющее данным доменом, и попытаться его перекупить.

Процедура получения домена второго уровня в зоне ru достаточно проста, но требует соблюдения ряда требований, которые в целом соответствуют общепринятым мировым стандартам. Порядок регистрации и делегирования установлен «Правилами и рекомендациями администрирования домена ru». РосНИИРОС осуществляет регистрацию доменов второго уровня ru и делегирует право на их администрирование на основании заявки.

Заявка должна быть заполнена по форме, в которой содержится информация об одном имени домена, а также данные о лицах, которые будут заниматься администрированием домена и его техническим сопровождением, а также о владельце домена.

Зарегистрировать доменное имя можно самостоятельно, изучив инструкции на вышеуказанных серверах. Другой возможностью может быть обращение к поставщику услуг, который возьмет на себя хлопоты по регистрации доменного имени. Главное в этом случае проследить, чтобы домен был зарегистрирован именно на вас или вашу компанию, а не на поставщика.

Службы Интернета

Службы Интернета — это системы, предоставляющие услуги пользователям Интернета. К ним относятся: электронная почта, WWW, телеконференции, списки рассылки, FTP, IRC, а также другие продукты, использующие Интернет как среду передачи информации.

Услуги, предоставляемые Интернетом, можно разделить на две основные категории.

1. Отложенные (off-line) — основным признаком этой группы является наличие временного перерыва между запросом и получением информации.
2. Прямые (on-line) — характерны тем, что информация по запросу возвращается немедленно. Если от получателя информации требуется немедленная реакция на нее, то такая услуга носит интерактивный характер.

Электронная почта

Самой первой и самой распространенной службой Интернета является электронная почта (e-mail). Эта служба предоставляет услуги отложенного чтения. Пользователь посылает сообщение, и адресат получает его на свой компьютер через некоторый промежуток времени. Электронное письмо состоит из заголовков, содержащих служебную информацию (об авторе письма, получателе, пути прохождения по сети и т. д.), и содержимого письма.

Электронное письмо можно снабдить цифровой подписью и зашифровать. Скорость пересылки составляет в среднем несколько минут. При этом стоимость электронной почты минимальна и не зависит от расстояния. Основными достоинствами электронной почты являются простота, дешевизна и универсальность.

Телеконференции

Телеконференции — вторая по распространенности служба Интернета, предоставляющая отложенные услуги.

Служба телеконференций состоит из множества тематических телеконференций — групп новостей (newsgroup), поддерживаемых серверами новостей. Сервер новостей — это компьютер, который может содержать тысячи групп новостей самых разнообразных тематик. Каждый сервер новостей, получивший новое сообщение, передает его всем узлам, с которыми он обменивается новостями. Группа новостей — это набор сообщений по определенной теме. Новости разделены по иерархически организованным тематическим группам, и имя каждой группы состоит из имен подуровней. Например, конференция comp.sys.linux.setup принадлежит группе «компьютеры», подгруппе «операционные системы», конкретнее — системе Linux, а именно — ее установке.

Существуют как глобальные иерархии, так и иерархии, локальные для какой-либо организации, страны или сети. Набор групп, получаемых сервером телеконференций, определяется его администратором и их наличием на других серверах, с которыми данный сервер обменивается новостями.

Доступ к группам новостей осуществляется через процедуру подписки, которая состоит в указании координат сервера новостей и выбора интересующих пользователя

групп новостей. Следует заметить, что каждый сервер новостей имеет определенный набор конференций, и, если интересующая тематика на нем не найдена, можно попробовать использовать другой сервер. Данная процедура, а также работа с группами новостей осуществляется с помощью программного обеспечения, поддерживающего эти функции, например, широко распространенным приложением компании Microsoft — Outlook Express.

В обсуждении темы телеконференции может участвовать множество людей, независимо от того, где они находятся физически. Обычно, хотя это и не является правилом, за порядком в конференциях следят специальные люди, так называемые модераторы. В их обязанности входит поддержание порядка в конференции в соответствии с установленными в ней правилами поведения и ее тематикой.

Наряду с описанной формой служб телеконференции широкое распространение получили WWW-телеконференции, также называемые форумами. Отличие состоит в том, что они работают через web-интерфейс, и размещаются не централизованно на серверах новостей, а на web-сайтах.

Списки рассылки

Списки рассылки (mail lists) — служба, не имеющая собственного протокола и программы-клиента и работающая исключительно через электронную почту.

Идея работы списка рассылки состоит в объединении под одним адресом электронной почты адресов многих людей — подписчиков списка рассылки. Когда письмо посылается на этот адрес, сообщение получают все подписчики данного списка рассылки. Ведущими списка рассылки, как правило, являются люди, хорошо владеющие его тематикой. Они отвечают за подготовку и рассылку очередных выпусков. Получателями писем являются люди, собственноручно подписавшиеся на список. Кроме того, у них есть право и возможность в любой момент отменить свою подписку.

Существуют открытые рассылки (для всех желающих), закрытые (для людей определенного круга), бесплатные (существующие за счет энтузиазма создателей, спонсорской поддержки, платных рекламодателей) и платные.

В зависимости от числа подписчиков список рассылки обслуживается на сервере программами различной сложности. Эти программы могут обеспечивать или не обеспечивать полную функциональность, которая заключается в автоматической подписке клиентов и приеме их отказа от подписки, проверке корректности электронных адресов, ведении архива сообщений, обработке почтовых ошибок, поддержке работы в режиме дайджеста (когда подписчик получает не каждое сообщение отдельным письмом, а все сообщения за какой-то срок в одном письме), проверке сообщений администратором списка перед рассылкой и т. д.

Чаты

Под словом чат (от английского chat) подразумеваются службы Интернета, позволяющие проводить текстовые дискуссии в режиме реального времени. От традиционной формы разговора их отличает то, что они ведутся в текстовом виде — путем набора текста на клавиатуре. Самым популярным открытым стандартом, лежащим в основе чатов, является IRC (Internet Relay Chat), .

IRC — это многопользовательская, предназначенная для чата многоканальная сеть, с помощью которой пользователи могут беседовать в режиме реального времени независимо от своего месторасположения.

Не смотря на то, что IRC существует достаточно много лет, в коммерческой деятельности современных компаний, например, в работе центров обслуживания потребителей, этот стандарт практически не применяется. Основным его предназначением остается обсуждение самого широкого круга вопросов между пользователями Интернета.

В свое время чаты, в основе которых лежал стандарт IRC, получили достаточно широкое распространение. Однако сегодня все более популярными становятся чаты, проводимые на отдельных web-сайтах и основывающиеся либо на языке HTML, либо на языке Java. Это позволяет пользователям Интернета участвовать в них без установки дополнительного программного обеспечения, используя только стандартный браузер, тем самым число потенциальных участников становится максимальным. С другой стороны, возможность установки на корпоративном сайте компании системы, обеспечивающей работу чата, позволяет широко использовать эту службу в коммерческих целях, например для обсуждения с потребителями тех или иных

вопросов деятельности предприятия, обсуждения продукции, системы обслуживания и т. д.

Интернет-пейджеры

Промежуточное положение между электронной почтой и чатами по динамичности и интерактивности общения занимают Интернет-пейджеры или службы мгновенных сообщений. Интернет-пейджеры постепенно становятся одними из самых популярных средств общения в Сети и по широте использования скоро смогут достичь электронную почту. Службы мгновенных сообщений позволяют общаться в режиме реального времени, совмещая в себе преимущества электронной почты и телефона. Частью процесса обмена в подобных системах могут становиться текстовый диалог, передача графики, голосовая и видео связь, обмен файлами. Примером подобных программ служат ICQ, MSN, AOL Instant Messenger и другие подобные им.

FTP

FTP (file transfer protocol) — протокол передачи файлов, но при рассмотрении FTP как службы Интернета имеется в виду не просто протокол, а именно служба доступа к файлам в файловых архивах. Одна из причин достаточно высокой ее популярности объясняется огромным количеством информации, накопленной в FTP-архивах за десятилетия эксплуатации компьютерных систем. Другая причина кроется в простоте доступа, навигации и передачи файлов по FTP.

FTP — служба прямого доступа, требующая полноценного подключения к Интернету.

World Wide Web

WWW (World Wide Web) — служба прямого доступа, требующая полноценного подключения к Интернету и позволяющая интерактивно взаимодействовать с представленной на web-сайтах информацией. Это самая современная и удобная служба Интернета. Она основывается на принципе гипертекста и способна представлять информацию, используя все возможные мультимедийные ресурсы: видео, аудио, графику, текст и т. д. Взаимодействие осуществляется по принципу клиент-сервер с использованием протокола передачи гипертекста (Hyper Text Transfer Protocol, HTTP). С помощью протокола HTTP служба WWW позволяет обмениваться документами в

формате языка разметки гипертекста — HTML (Hyper Text Markup Language), который обеспечивает надлежащее отображение содержимого документов в браузерах пользователей.

Принцип гипертекста, лежащий в основе WWW, состоит в том, что каждый элемент HTML-документа может являться ссылкой на другой документ или его часть, при этом документ может ссылаться как на документы на этом же сервере, так и на других серверах Интернета. Ссылки WWW могут указывать не только на документы, свойственные службе WWW, но и на прочие службы и информационные ресурсы Интернета. Более того, большинство программ-клиентов WWW — браузеров (browsers), обозревателей, или навигаторов, не просто понимают такие ссылки, но и являются программами-клиентами соответствующих служб: FTP, сетевых новостей Usenet, электронной почты и т. д. Таким образом, программные средства WWW являются универсальными для различных служб Интернета, а сама информационная система WWW выполняет по отношению к ним интегрирующую функцию.

Необходимо подчеркнуть, что Интернет и WWW это не тождественные понятия. Узкое определение Интернета представляет его как взаимосвязь компьютерных сетей на базе семейства протоколов TCP/IP, в пространстве которой становится возможным функционирование протоколов более высокого уровня, в том числе протокола передачи гипертекста (HTTP) — протокола World Wide Web, гипертекстового сервиса доступа к удаленной информации. Кроме World Wide Web, на этом уровне (он называется прикладным или уровнем приложений) действуют и другие протоколы, например электронной почты (POP3, SMTP, IMAP), общения в режиме реального времени (IRC) и групп новостей (NNTP).

Таким образом, World Wide Web — это одна из служб Интернета, которая предлагает простой в использовании интерфейс и дает возможность пользователям, даже не слишком хорошо знающим компьютер, получать доступ к web-службам в любой части Интернета.

Новые службы Интернета

В отдельную группу можно выделить службы Интернета, не имеющие сегодня такого широкого распространения, как те, о которых было рассказано ранее и не имеющие всеми признанных единых стандартов. В их основе также лежит

использование Интернета как среды передачи информации. В частности, к этой группе можно отнести:

- средства передачи голоса по каналам связи Интернета, предоставляющие услуги телефонной и факсимильной связи;
- программные средства для проведения видео- и аудио- конференций через Интернет;
- системы широковещательной передачи мультимедийной информации.

Службы поиска информации

Особую группу составляют службы Интернета, поддерживаемые одной из групп его участников и причисляемые в данной категории благодаря глобальному характеру предоставляемых ими услуг по поиску информации. Поиск информации является сегодня одной из ключевых проблем Интернета, так как количество представленных в нем web-страниц сегодня оценивается более чем в несколько сотен миллионов. Кроме того, в основе проблем поиска информации лежат такие причины, как множественность и фрагментарность источников, большое количество различных способов хранения данных, дефицит времени на выборку и обработку информации, стоимость получения информации, ненадежность данных, постоянное обновление и добавление информации.

Ниже перечислены основные инструменты поиска информации в Интернете, которым удастся в значительной степени преодолевать вышеназванные трудности:

- Поисковые машины (spiders, crawlers). Основная функция поисковых машин состоит в исследовании Интернета с целью сбора данных о существующих в нем web-сайтах и выдаче по запросу пользователя информации о web-страницах, наиболее полно удовлетворяющих введенному запросу.
- Каталоги. Представляют собой иерархически организованную тематическую структуру, в которую, в отличие от поисковых машин, информация заносится по инициативе пользователей. Добавляемая страница жестко привязывается к принятым в каталоге категориям.
- Мета-средства поиска. Мета-средства поиска позволяют усовершенствовать процесс путем запуска одновременно нескольких поисковых средств. Этот способ значительно повышает скорость, однако не позволяет воспользоваться возможностями

построения сложных запросов, предлагаемыми большинством современных систем поиска.

Более подробно о поисковых системах и каталогах рассказывается в следующей главе «Взаимодействие с индивидуальными потребителями» в разделе, описывающем навигационные web-сайты.

Методы обеспечения безопасности в сети Интернет

Одним из важнейших условий широкого применения Интернета было и остается обеспечение адекватного уровня безопасности для всех транзакций, проводимых через него. Это касается информации, передаваемой между пользователями, информации, сохраняемой в базах данных торговых систем, информации, сопровождающей финансовые транзакции.

Понятие безопасность информации можно определить как состояние устойчивости информации к случайным или преднамеренным воздействиям, исключающее недопустимые риски ее уничтожения, искажения и раскрытия, которые приводят к материальному ущербу владельца или пользователя информации. Поскольку Сеть полностью открыта для внешнего доступа, то роль этих методов очень велика. Большая значимость фактора безопасности также отмечается многочисленными исследованиями, проводимыми в Интернете.

Решить проблемы безопасности призвана криптография — наука об обеспечении безопасности данных. Криптография и построенные на ее основе системы призваны решать следующие задачи.

- **Конфиденциальность.** Информация должна быть защищена от несанкционированного доступа как при хранении, так и при передаче. Доступ к информации может получить только тот, для кого она предназначена. Обеспечивается шифрованием.

- **Аутентификация.** Необходимо однозначно идентифицировать отправителя, при однозначной идентификации отправитель не может отказаться от послания. Обеспечивается электронной цифровой подписью и сертификатом.

- Целостность. Информация должна быть защищена от несанкционированного изменения как при хранении, так и при передаче. Обеспечивается электронной цифровой подписью.

В соответствии с названными задачами основными методами обеспечения безопасности выступают шифрование, цифровая подпись и сертификаты.

Шифрование

Осуществляя сделки в Сети, в первую очередь необходимо убедиться, что важная информация надежно скрыта от посторонних лиц. Этому служат технологии шифрования, преобразующие простой текст в форму, которую невозможно прочесть, не обладая специальным шифровальным ключом. Благодаря данным технологиям можно организовать безопасную связь по общедоступным незащищенным каналам Интернета.

Любая система шифрования работает по определенной методологии, включая в себя один или более алгоритмов шифрования (математических формул), ключи, используемые этими алгоритмами, а также систему управления ключами.

Согласно методологии шифрования сначала к тексту применяются алгоритм шифрования и ключ для получения из него зашифрованного текста. Затем зашифрованный текст передается к месту назначения, где тот же самый алгоритм и ключ используются для его расшифровки, чтобы получить первоначальный текст. В методологию шифрования также входят процедуры создания ключей и их распространения.

Наиболее распространены алгоритмы шифрования, которые объединяют ключ с текстом. Безопасность систем такого типа зависит от конфиденциальности ключа, используемого в алгоритме шифрования, а не от конфиденциальности самого алгоритма, который может быть общедоступен и благодаря этому хорошо проверен. Но основная проблема, связанная с этими методами, состоит в безопасной процедуре генерации и передачи ключей участникам взаимодействия.

В настоящее время существует два основных типа криптографических алгоритмов:

1. классические, или симметричные алгоритмы, основанные на использовании закрытых, секретных ключей, когда и шифрование, и дешифрирование производятся с помощью одного и того же ключа;

2. алгоритмы с открытым ключом, в которых используются один открытый и один закрытый ключ, то есть операции шифрования производятся с помощью разных ключей. Эти алгоритмы называются также асимметричными.

Каждая методология требует собственных способов распределения ключей и собственных типов ключей, а также алгоритмов шифрования и расшифровки ключей.

Симметричные методы шифрования

Технология шифрования с секретным ключом (симметричный алгоритм) требует, чтобы оба участника зашифрованной переписки имели доступ к одному и тому же ключу. Это необходимо, так как отправитель использует ключ для зашифровки сообщения, а получатель применяет его же для расшифровки. Как следствие, возникает проблема безопасной передачи этого ключа.

Алгоритмы симметричного шифрования используют ключи не очень большой длины и могут быстро шифровать большие объемы данных.

Порядок использования систем с симметричными ключами выглядит следующим образом:

1. Безопасно создается, распространяется и сохраняется симметричный секретный ключ.
2. Отправитель использует симметричный алгоритм шифрования вместе с секретным симметричным ключом для получения зашифрованного текста.
3. Отправитель передает зашифрованный текст. Симметричный секретный ключ никогда не передается по незащищенным каналам связи.
4. Для восстановления исходного текста, получатель применяет к зашифрованному тексту тот же самый симметричный алгоритм шифрования вместе с тем же самым симметричным ключом, который уже есть у него.

Некоторые из алгоритмов симметричных систем шифрования: ГОСТ №28147-89, DES (Data Encryption Standard), тройной алгоритм DES, Международный алгоритм шифрования IDEA, RC2, RC3, RC5, CAST.

Асимметричные методы шифрования

Для решения проблемы распространения ключей при использовании симметричных методов шифрования на основе результатов, полученных классической и современной алгеброй, были предложены системы с открытым ключом, или асимметричные криптосистемы. Суть их состоит в том, что каждым адресатом генерируются два ключа, связанные между собой по определенному правилу. Хотя каждый из пары ключей подходит как для шифрования, так и для дешифрирования, данные, зашифрованные одним ключом, могут быть расшифрованы только другим.

Один ключ объявляется открытым, а другой закрытым. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне. Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный текст не может быть расшифрован тем же открытым ключом. Дешифрирование сообщения возможно только с использованием закрытого ключа, известного лишь самому адресату.

Криптографические системы с открытым ключом используют так называемые необратимые или односторонние функции.

Понятие односторонней функции было введено в теоретическом исследовании о защите входа в вычислительные системы. Функция $f(x)$ называется односторонней (one-way function), если для всех значений x из ее области определения легко вычислить значения $y=f(x)$, но вычисление обратного значения практически неосуществимо. То есть по заданному значению y_0 нельзя найти такое значение x_0 , для которого $f(x_0)=y_0$. «Практически неосуществимо» в данном случае означает, что требуется такой огромный объем вычислений, который при существующем уровне развития техники невозможно реализовать.

Множество классов необратимых функций порождает все разнообразие систем с открытым ключом.

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах. Известно несколько криптосистем с открытым ключом. Наиболее разработана на сегодня система RSA, предложенная еще в 1978 г. Алгоритм RSA назван по первым буквам фамилий его авторов: Р. Л. Райвеста (R. L. Rivest), А. Шамира (A. Shamir) и Л. Адлемана (L. Adleman). Этот алгоритм стал

мировым фактически признанным стандартом для открытых систем и рекомендован МККТТ (Международный Консультативный Комитет по телефонии и телеграфии). Также используются алгоритмы: ЕСС (криптосистема на основе эллиптических кривых), Эль-Гамаль.

Следует отметить, что алгоритмы систем шифрования с открытым ключом можно использовать в качестве следующих инструментов:

- как самостоятельные средства защиты передаваемых и хранимых данных;
- как средства для распределения ключей (алгоритмы систем шифрования с открытым ключом более трудоемки, чем традиционные криптосистемы, поэтому на практике часто бывает рационально передать ключи, объем информации в которых незначителен с их помощью, а потом с помощью обычных алгоритмов осуществлять обмен большими информационными потоками);
- как средства аутентификации пользователей (для создания электронной цифровой подписи).

Все асимметричные криптосистемы являются объектом атак, в которых применяется прямой перебор ключей, поэтому для обеспечения эквивалентного уровня защиты в них должны использоваться гораздо более длинные ключи, чем в симметричных криптосистемах.

Для того чтобы избежать низкой скорости алгоритмов асимметричного шифрования, методы шифрования с открытым ключом часто используют для шифрования небольших объемов информации, например, для шифрования секретного ключа, на основе которого далее производится криптографическое закрытие информации симметричными методами.

Цифровая подпись

Шифрование передаваемых через Интернет данных позволяет защитить их от посторонних лиц. Однако для полной безопасности должна быть уверенность в том, что второй участник транзакции является тем лицом, за которое он себя выдает. В бизнесе наиболее важным идентификатором личности заказчика является его подпись. В электронной коммерции применяется электронный эквивалент традиционной подписи — цифровая подпись. С ее помощью можно доказать не только то, что

транзакция была инициирована определенным источником, но и то, что информация не была испорчена во время передачи.

Как и в шифровании, технология электронной подписи использует либо секретный ключ (в этом случае оба участника сделки применяют один и тот же ключ), либо открытый ключ (при этом требуется пара ключей — открытый и личный). И в данном случае более просты в использовании и более популярны методы с открытым ключом (такие, как RSA)

Хэш-функции являются одним из важных элементов криптосистем на основе ключей и используются для обнаружения факта модификации сообщения, то есть для электронной подписи. Их относительно легко вычислить, но почти невозможно расшифровать. Хэш-функция имеет исходные данные переменной длины и возвращает строку (иногда называемую дайджестом сообщения — MD) фиксированного размера, обычно 128 бит.

Существует несколько защищенных хэш-функций: Message Digest 5 (MD-5), Secure Hash Algorithm (SHA) и др. Они гарантируют, что разные документы будут иметь разные электронные подписи, и что даже самые незначительные изменения документа вызовут изменение его дайджеста.

Рассмотрим, как работает технология цифровой подписи, использующая алгоритм RSA. Предположим, вы хотите послать сообщение. В этом случае порядок работы следующий:

1. При помощи хеш-функции вы получаете дайджест — уникальным образом сжатый вариант исходного текста.
2. Получив дайджест сообщения, вы шифруете его с помощью личного ключа RSA, и дайджест превращается в цифровую подпись.
3. Вы посылаете вместе с самим сообщением цифровую подпись.
4. Получив послание, получатель расшифровывает цифровую подпись с помощью вашего открытого ключа и извлекает дайджест сообщения.
5. Получатель, применяя для сообщения ту же хэш-функцию, что и вы, получает свой сжатый вариант текста и сравнивает его с дайджестом, восстановленным из подписи. Если они совпадают, то это значит, что подпись правильная и сообщение действительно поступило от вас. В противном случае сообщение либо отправлено из другого источника, либо было изменено после создания подписи.

При аутентификации личности отправителя открытый и личный ключи играют роли, противоположные тем, что они выполняли при шифровании. Так, в технологии шифрования открытый ключ используется для зашифровки, а личный — для расшифровки. При аутентификации с помощью подписи все наоборот. Кроме того, подпись гарантирует только целостность и подлинность сообщения, но не его защиту от посторонних глаз. Для этого предназначены алгоритмы шифрования. Например, стандартная технология проверки подлинности электронных документов DSS (Digital Signature Standard) применяется в США компаниями, работающими с государственными учреждениями. Однако у технологии RSA более широкие возможности в силу того, что она служит как для генерации подписи, так и для шифрования самого сообщения. Цифровая подпись позволяет проверить подлинность личности отправителя: она основана на использовании личного ключа автора сообщения и обеспечивает самый высокий уровень сохранности информации.

Сертификаты

Как было сказано выше, основной проблемой криптографических систем является распространение ключей. В случае симметричных методов шифрования эта проблема стоит наиболее остро, поэтому при шифровании данных для передачи ключей через Интернет чаще всего используются асимметричные методы шифрования.

Асимметричные методы более приспособлены для открытой архитектуры Интернета, однако и здесь использование открытых ключей требует их дополнительной защиты и идентификации для определения связи с секретным ключом. Без такой дополнительной защиты злоумышленник может выдать себя за отправителя подписанных данных или за получателя зашифрованных данных, заменив значение открытого ключа или нарушив его идентификацию. В этом случае каждый может выдать себя за другое лицо. Все это приводит к необходимости верификации открытого ключа. Для этих целей используются электронные сертификаты.

Электронный сертификат представляет собой цифровой документ, который связывает открытый ключ с определенным пользователем или приложением. Для заверения электронного сертификата используется электронная цифровая подпись доверенного центра — ЦС (Центра Сертификации). Исходя из функций, которые выполняет ЦС, он является основным компонентом всей инфраструктуры открытых ключей (ИОК или PKI — Public Key Infrastructure). Используя открытый ключ ЦС,

каждый пользователь может проверить достоверность электронного сертификата, выпущенного ЦС, и воспользоваться его содержимым.

Для того чтобы сертификатам можно было доверять, независимая организация, выполняющая функции ЦС и являющаяся их источником, должна быть достаточно авторитетной. В настоящее время наиболее известным источником сертификатов являются компании Thawte (www.thawte.com) и VeriSign (www.verisign.com), однако существуют и другие системы, такие как World Registry (IBM), Cyber Trust (GTE) и Entrust (Nortel). В России дистрибьютором сертификатов SSL компании Thawte сегодня является «РосБизнесКонсалтинг» (www.rbc.ru).

Технология цифровых сертификатов работает следующим образом. Чтобы воспользоваться сертификатом, потенциальный покупатель должен, прежде всего, получить его в надежном источнике. Для этого ему необходимо каким-то образом доказать подлинность своей личности, возможно, явившись в эту организацию и предъявив соответствующий документ, а также передать источнику сертификатов копию своего открытого ключа. После этого при желании купить что-либо через Интернет, ему будет достаточно добавить к заказу свою электронную подпись и копию сертификата. Отдел обслуживания покупателей фирмы, в которой он совершил покупку, проверяет сертификат, чтобы убедиться, что к заказу приложен подлинный открытый ключ, а также выясняет, не аннулирован ли сертификат.

Следует отметить, что технология цифровых сертификатов является двунаправленной. Это значит, что не только фирма может проверить подлинность заказа покупателя, но и сам покупатель имеет возможность убедиться, что он имеет дело именно с той фирмой, за которую она себя выдает. Осуществив взаимную проверку, обе стороны спокойно заключают сделку, так как обладают подлинными открытыми ключами друг друга и, соответственно, могут шифровать передаваемые данные и снабжать их цифровой подписью. Такой механизм обеспечивает надежность сделки, ибо в этом случае ни одна из сторон не сможет отказаться от своих обязательств.

Протоколы и стандарты безопасности

Описанные выше методы обеспечения безопасности являются основой построения большинства Интернет-систем. Это могут быть системы обмена

информацией или платежные системы. Важность вопросов безопасности для их организации очень велика. Так, согласно проводимым исследованиям, одной из основных причин медленного роста электронной коммерции сегодня остается озабоченность покупателей надежностью средств, применяемых при расчетах в Интернете. Основные причины обеспокоенности связаны со следующими факторами.

- Отсутствие гарантии конфиденциальности — кто-либо может перехватить передаваемые данные и попытаться извлечь ценную информацию, например, данные о кредитных картах. Это может произойти как во время передачи информации, так и непосредственно после совершения покупки через торговые web-сайты.

- Недостаточный уровень проверки (аутентификации) участников операции — покупатель, посещая электронный магазин, не уверен, что представленная на нем компания именно та, за кого она себя выдает, а у продавца нет возможности проверить, что покупатель, сделавший заказ, является законным обладателем кредитной карты.

- Нет гарантии целостности данных — даже если отправитель данных может быть идентифицирован, то третья сторона может изменить их во время передачи.

Наиболее распространенными механизмами, призванными устранить указанные факторы и обеспечить безопасность проведения электронных платежей через Интернет сегодня являются:

- протокол SSL (Secure Socket Layer), обеспечивающий шифрование передаваемых через Интернет данных;

- стандарт SET (Secure Electronic Transactions), разработанный компаниями Visa и MasterCard и обеспечивающий безопасность и конфиденциальность совершения сделок при помощи пластиковых карт.

Протокол SSL и стандарт SET

Протокол SSL — один из существующих протоколов обмена данными, обеспечивающий шифрование передаваемой информации. В настоящее время это наиболее распространенный метод защиты электронных транзакций в Интернете.

Протокол SSL является стандартом, основанным на криптографии с открытыми ключами. Протокол обеспечивает защиту данных, передаваемых в сетях TCP/IP по

протоколам приложений за счет шифрования и аутентификации серверов и клиентов. Это означает, что шифруется вся информация, передаваемая и получаемая web-браузером, включая URL-адреса, все отправляемые сведения (такие, как номера кредитных карт), данные для доступа к закрытым web-сайтам (имя пользователя и пароль), а также все сведения, поступающие с web-серверов.

Протокол SSL позволяет решить часть названных проблем безопасности, однако его роль в основном ограничивается обеспечением шифрования передаваемых данных. Поэтому для комплексного решения перечисленных выше проблем была разработана спецификация и создан набор протоколов, известные как стандарт SET (Secure Electronic Transaction) — безопасные электронные транзакции.

Официальной датой рождения стандарта SET является 1 февраля 1996 г. В этот день Visa International и MasterCard International совместно с рядом технологических компаний объявили о разработке единого открытого стандарта защищенных расчетов через Интернет с использованием пластиковых карт. В декабре 1997 г. была создана некоммерческая организация SETCo LLC, призванная координировать работы по развитию стандарта и осуществлять тестирование и сертификацию предлагаемого на рынке программного обеспечения для обеспечения контроля над соответствием этого программного обеспечения спецификациям SET.

Благодаря использованию цифровых сертификатов и технологий шифрования, SET позволяет как продавцам, так и покупателям производить аутентификацию всех участников сделки. Кроме того, SET обеспечивает надежную защиту номеров кредитных карт и другой конфиденциальной информации, пересылаемой через Интернет, а открытость стандарта позволяет разработчикам создавать решения, которые могут взаимодействовать между собой. Также важным фактором, обеспечивающим продвижение SET, является его опора на существующие карточные системы, ставшие привычным финансовым инструментом с отлаженной технологией и правовым механизмом.

В основе системы безопасности, используемой SET, лежат стандартные криптографические алгоритмы DES и RSA. Инфраструктура SET построена в соответствии с инфраструктурой открытого ключа (Public Key Infrastructure, PKI) на базе сертификатов, соответствующих стандарту X.509, утвержденному организацией по стандартизации (ISO).

Главная особенность SET — регламентация использования системы безопасности, которая устанавливается международными платежными системами. Требования Visa и Europay к центру обработки на основе SET включают, во-первых, традиционные требования к обработке пластиковых карт (защита помещений, контроль над доступом, резервное энергоснабжение, аппаратная криптография и т. п.), и, во-вторых, специфические дополнения — межсетевые экраны (firewalls) для защиты каналов Интернета. Такой подход позволяет использовать единые методики оценки рисков при проведении электронных платежей вне зависимости от способа аутентификации клиента (традиционная карта с магнитной полосой, смарт-карта или цифровой сертификат). Это позволяет участникам платежной системы разрешать спорные ситуации по отработанным механизмам и сконцентрироваться на развитии своего электронного бизнеса.

SET обеспечивает следующие требования защиты операций электронной коммерции:

- секретность данных оплаты и конфиденциальность информации заказа, переданной вместе с данными об оплате;
- сохранение целостности данных платежей, которая обеспечивается при помощи цифровой подписи;
- специальную криптографию с открытым ключом для проведения аутентификации;
- аутентификацию держателя кредитной карты, которая обеспечивается применением цифровой подписи и сертификатов держателя карты;
- аутентификацию продавца и его возможности принимать платежи по пластиковым картам с применением цифровой подписи и сертификатов продавца;
- подтверждение того, что банк продавца является действующей организацией, которая может принимать платежи по пластиковым картам через связь с обрабатывающей системой, что обеспечивается с помощью цифровой подписи и сертификатов банка продавца;
- готовность оплаты транзакций в результате аутентификации сертификата с открытым ключом для всех сторон;
- безопасность передачи данных посредством использования криптографии.

SET позволяет сохранить существующие отношения между банком, держателями карт и продавцами, и объединяется с действующими системами, опираясь на

открытость, международные стандарты платежных систем, лежащие в его основе, а также технологии и правовые механизмы, существующие в финансовой отрасли.

Для получения информации о распространении SET, включая информацию о банках, имеющих сертификаты Visa и Europay/MasterCard, и торговых/сервисных компаниях, принимающих платежи через SET, можно обратиться на сайт set-sites.com или сайты международных платежных систем.

Платежные Интернет-системы

Интернет гигантскими шагами движется к тому, чтобы стать не только системой передачи информации, но и выполнять функции электронных платежных систем.

Платежная система в Интернете — это система проведения расчетов между финансовыми, коммерческими организациями и пользователями в процессе покупки/продажи товаров и услуг через Интернет. Именно платежная система позволяет превратить службу по обработке заказов или электронную витрину в полноценный магазин со всеми стандартными атрибутами: выбрав товар или услугу на сайте продавца, покупатель может осуществить платеж, не отходя от компьютера.

Оплата в системе электронной коммерции может производиться в случае соблюдения ряда условий:

- Соблюдение конфиденциальности. При проведении платежей через Интернет покупатель хочет, чтобы его данные (например, номер кредитной карты) были известны только организациям, имеющим на это законное право.
- Сохранение целостности информации. Информация о покупке никем не может быть изменена.
- Проведение процедуры аутентификации. Покупатели и продавцы должны быть уверены, что все стороны, участвующие в сделке, являются теми, за кого они себя выдают.
- Обеспечение авторизации. Процесс, в ходе которого требование на проведение транзакции одобряется или отклоняется платежной системой. Эта процедура позволяет определить наличие средств у покупателя.
- Наличие гарантии рисков продавца. Осуществляя торговлю в Интернете, продавец подвержен множеству рисков, связанных с отказами от товара и недобросовестностью покупателя. Величина рисков должна быть согласована с поставщиком услуг

платежной системы и другими организациями, включенными в торговые цепочки, посредством специальных соглашений.

· Минимизация платы за транзакцию. Плата за обработку транзакций заказа и оплаты товаров, естественно, входит в их стоимость, поэтому снижение цены транзакции увеличивает конкурентоспособность. Важно отметить, что транзакция должна быть оплачена в любом случае, даже при отказе покупателя от товара.

Все указанные условия должны быть реализованы в платежной системе Интернета. Более подробно эти требования будет обсуждаться при рассмотрении конкретных методов платежных систем, которые, в сущности, представляют собой электронные версии традиционных платежных систем.

Классификация платежных систем

Все платежные системы можно разделить на два основных направления:

1. кредитные системы или, как их иногда называют, системы управление счетами через Интернет;
2. дебетовые схемы — системы выпуска электронных денежных обязательств, позволяющие владельцам пользоваться ими как видом бессрочных денежных обязательств.

К первому виду систем относятся системы управления банковскими счетами через Интернет, предлагаемые различными банками в России и за рубежом, а также системы с использованием кредитных карт. Кредитные карты являются ни чем иным, как средством управления счетом, переданным банком владельцу счета во временное пользование.

По сути, любая система управления счетом заменяет только личный визит клиента в банк, а все остальные действия, связанные с реальным переводом денежных средств осуществляются по существующим банковскими каналам. Единственным существенным преимуществом следует считать то, что при личном визите платежные документы будут приняты банком только в часы его работы, а при передаче через Интернет можно обеспечить их круглосуточный прием.

Ко второму виду систем относятся платежные системы на основе смарт-карт и, так называемые, «электронные наличные». В отличие от первого рода систем при использовании электронных денежных обязательств между участниками сделки

происходит передача информации, представляющей самостоятельную финансовую ценность. Эта информация может быть тут же проверена на подлинность и платежеспособность стороной, принимающей платеж или выпустившей эти обязательства, и тут же использована для следующего платежа или переведена в другие, не электронные платежные средства.

В настоящий момент в России реально работают только несколько платежных инструментов и поддерживающие их технологические решения. Выбор адекватных платежных инструментов, являющийся ключевым вопросом для развития рынка платежей в Интернете, должен быть обусловлен целым рядом критериев, в число которых входят: удобство пользования, надежность и скорость проведения операции, безопасность, невысокая стоимость инструмента и его поддержки для всех участников платежей — покупателей, продавцов, банков.

Кредитные системы

Как было сказано выше, к кредитным системам относятся системы, позволяющие оказывать банковские услуги через Интернет, и системы с использованием кредитных карт. Системы первого вида достаточно подробно представлены в главе 5, «Товар и товарная политика в Интернете», поэтому здесь подробно рассмотрим системы второго вида — платежные системы на основе кредитных карт.

Обзор систем на основе кредитных карт

Лидирующее положение среди существующих платежных систем занимают системы на основе пластиковых карт и, прежде всего, кредитных карт. Успех применения кредитных карт для расчетов в Интернете связан с привычностью такого вида оплаты, во многом схожего с оплатой в реальном мире, и большинство транзакций в Интернете сегодня совершаются с использованием именно этого вида платежного средства.

Для начала рассмотрим основные понятия, связанные с организацией и функционированием платежных систем на основе пластиковых карт.

Пластиковая карта — это персонифицированный платежный инструмент, предоставляющий пользующемуся картой лицу возможность безналичной оплаты товаров и услуг, а также получения наличных средств в отделениях банков и

банковских автоматах (банкоматах). Принимающие карту предприятия торговли или оказания услуг и отделения банков образуют сеть точек ее обслуживания.

Пластиковая карта представляет собой пластину стандартных размеров (85,6 мм 53,9 мм 0,76 мм), изготовленную из специальной устойчивой к механическим и термическим воздействиям пластмассы. Одна из ее основных функций — обеспечение идентификации использующего ее лица как субъекта платежной системы. Для этого на пластиковую карту наносятся логотипы банка-эмитента и платежной системы, обслуживающей карту, имя держателя карты, номер его счета, срок действия карты и др. Кроме этого, на карте может присутствовать фотография держателя и его подпись.

На сегодняшний день наиболее распространенными являются карты с магнитной полосой — в обращении находится свыше двух миллиардов карт подобного типа. Магнитная полоса располагается на обратной стороне карты и, согласно стандарту ISO 7811, состоит из трех дорожек. Из них первые две предназначены для хранения идентификационных данных, а на третью можно записывать информацию (например, текущее значение лимита дебетовой карты). Однако из-за невысокой надежности многократно повторяемого процесса записи/считывания, запись на магнитную полосу, как правило, не практикуется, и такие карты используются только в режиме считывания информации. На лицевой стороне карты с магнитной полосой обычно указывается: логотип банка-эмитента, логотип платежной системы, номер карты (первые 6 цифр — код банка, следующие 9 — банковский номер карты, последняя цифра — контрольная, последние четыре цифры нанесены на голограмму), срок действия карты, имя держателя карты; на оборотной стороне — магнитная полоса, место для подписи.

Гарантом выполнения платежных обязательств, возникающих в процессе обслуживания пластиковых карт, является выпустивший их банк-эмитент. Поэтому карты на протяжении всего срока действия остаются собственностью банка, а клиенты — держатели карт — получают их лишь в пользование. Характер гарантий банка-эмитента зависит от платежных полномочий, предоставляемых клиенту и фиксируемых классом карты.

При выдаче карты клиенту осуществляется ее персонализация — на нее заносятся данные, позволяющие идентифицировать карту и ее держателя, а также осуществить

проверку платежеспособности карты при приеме ее к оплате или выдаче наличных денег.

Процесс утверждения продажи или выдачи наличных по карте называется авторизацией. Для ее проведения точка обслуживания делает запрос к платежной системе о подтверждении полномочий и финансовых возможностей предъявителя карты. Наиболее распространена автоматическая авторизация, когда карта помещается в электронный терминал (Point Of Sale или POS-терминал), данные считываются с карты, кассиром вводится сумма платежа, а держателем карты со специальной клавиатуры — персональный идентификационный номер (ПИН-код). После этого терминал осуществляет авторизацию либо устанавливая связь с базой данных платежной системы (авторизация в режиме подключения), либо осуществляя дополнительный обмен данными с самой картой (авторизация в автономном режиме). В случае выдачи наличных денег процедура носит аналогичный характер с той лишь особенностью, что деньги выдаются специальным устройством — банкоматом, который и проводит авторизацию.

При осуществлении расчетов держатель карты ограничен рядом требований. Характер ограничений и условия их использования могут быть весьма разнообразными. Однако в большинстве случаев ситуация сводится к двум основным сценариям.

Держатель дебетовой карты должен заранее внести на свой счет в банке-эмитенте некоторую сумму. Ее размер и определяет предел доступных средств. При осуществлении расчетов с использованием карты синхронно уменьшается и остаток. Контроль осуществляется при проведении авторизации, которая при использовании дебетовой карты является обязательной. Для возобновления (или увеличения) лимита держателю карты необходимо вновь внести средства на свой счет.

Для обеспечения платежей держатель карты может не вносить предварительно средства, а получить в банке-эмитенте кредит. Подобная схема реализуется при оплате посредством кредитной карты. В этом случае лимит связан с величиной предоставленного кредита, в рамках которого держатель карты может производить расходы. Кредит может быть как однократным, так и возобновляемым. Возобновление кредита в зависимости от договора с держателем карты происходит после погашения либо всей суммы задолженности, либо некоторой ее части.

Выпуском карт и гарантом выполнения финансовых обязательств, связанных с использованием выпущенных им пластиковых карт как платежного средства, является банк-эмитент. Однако он не занимается деятельностью, обеспечивающей ее прием предприятиями торговли и сферы услуг. Эти задачи решает банк-эквайер, осуществляющий весь спектр операций по взаимодействию с точками обслуживания карт: обработку запросов на авторизацию; перечисление на расчетные счета точек средств за товары и услуги, предоставленных по картам; прием, сортировку и пересылку документов (бумажных и электронных), фиксирующих совершение сделок с использованием карт; распространение стоп-листов (перечней карт, операции по которым по тем или иным причинам приостановлены) и др. Кроме того, банк-эквайер может осуществлять выдачу наличных по картам как в своих отделениях, так и через принадлежащие ему банкоматы. Банк может совмещать функции эквайера и эмитента. Следует отметить, что основными, неотъемлемыми функциями банка-эквайера являются финансовые функции, связанные с выполнением расчетов и выплат точкам обслуживания. Что же касается перечисленных выше технических атрибутов его деятельности, то они могут быть делегированы эквайером специализированным сервисным организациям — процессинговым центрам.

Выполнение эквайерами своих функций влечет за собой расчеты с эмитентами. Каждый банк-эквайер осуществляет перечисление средств точкам обслуживания по платежам держателей карт банков-эмитентов, входящих в данную платежную систему. Поэтому соответствующие средства (а также, возможно, средства, возмещающие выданную наличность) впоследствии должны быть перечислены эквайеру этими эмитентами. Оперативное проведение взаиморасчетов между эквайерами и эмитентами обеспечивается наличием в платежной системе расчетного банка (одного или нескольких), в котором банки — члены системы открывают корреспондентские счета.

Как говорилось ранее, кредитные карты сегодня являются доминирующим средством платежей в Интернете. Основная причина этого в широкой распространенности данного платежного средства во всем мире и неизменность принципов его использования при переносе из традиционного мира в мир виртуальный. Вместе с тем, использование кредитных карт для проведения платежей связано с определенными техническими недостатками, что позволяет мошенникам пользоваться чужими денежными средствами и товарами и, тем самым, подрывает авторитет

карточных систем как средства платежа через Интернет. Рассмотрим основные недостатки более подробно.

Сделки через Интернет, относящиеся в международной классификации сделок к типу mo/to (mail order/telephone order – сделки, совершаемые по почте, телеграфу или телефону), были достаточно распространены еще во времена, предшествующие Интернету в странах с развитыми карточными платежными системами, но в силу специфики товаров, выставляемых на продажу в Интернете, оказались мало защищенными от мошенничества, будучи перенесенными в него. При оформлении сделок mo/to с получением номера карты вне Интернета, у продавца всегда есть возможность провести аутентификацию (определение личности) клиента при доставке товара. Правила торговли по картам предполагают обязательную аутентификацию покупателя как держателя предъявленной карты, будь то платеж в магазине с прокатыванием карты, когда кассир удостоверяется в том, что берет оплату именно с держателя карты, или доставка товара по заказу, сделанному по телефону, когда служба доставки несет ответственность за доставку товара именно заказчику. В полной мере соблюсти эти правила в Интернете не представляется возможным. В Интернете с его главным и специфическим товаром — информацией, которая может быть получена непосредственно в момент платежа, встает проблема идентификации человека, предъявившего карту. Продавец способен провести только авторизацию карты, но не может подтвердить личность человека, предоставившего информацию о карте через Интернет.

Основные опасности, подстерегающие держателя карты в Интернет:

- возможность просмотра посторонними лицами передаваемой через Интернет информации о карте;
- возможность предъявления данных о карте и ее владельце в поддельный магазин, собирающий эту информацию с криминальными целями;
- возможность утраты данных о карте, переданных держателем магазину, в случае взлома или иных причин.

Частичным решением указанных проблем может быть использование описанного ранее протокола SSL. Однако и он 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 торговца или личности пользователя как продавцом, так и покупателем. Фирма может предоставить о себе недостоверную информацию, а покупатель произвести покупку, а затем отказаться от оплаты — доказать, что это именно он пользовался своей картой практически невозможно из-за отсутствия подписи.

Самым надежным вариантом является применение специальных средств, например, рассмотренного выше стандарта SET. Сегодня использование систем на базе SET является наиболее безопасным вариантом, но в силу различных причин он еще не получил достаточного распространения.

Еще одним из ограничений использования пластиковых карт является нижний предел производимых покупок, составляющий около \$3–5. Так как за проведение каждой транзакции эмитент карты берет порядка 1,5–3 % от ее суммы, но не менее 20 центов, то производить оплату товаров в нижнем ценовом диапазоне становится невыгодно.

Схема проведения платежей при помощи кредитных карт

Кредитные системы на основе кредитных карт являются аналогами обычных систем, работающих с ними. Отличие состоит в проведении всех транзакций через Интернет, и как следствие, в необходимости дополнительных средств безопасности и аутентификации.

Как было описано выше, одним из самых надежных стандартов проведения платежей при помощи кредитных карт является стандарт SET. В виду высоких затрат на его внедрение многие финансовые институты пытаются разработать частные решения. Одно из таких решений предложено компанией Assist.

Система платежей в Интернете, разработанная Assist (www.assist.ru) запущена в коммерческую эксплуатацию в марте 1999 г. компанией Рексофт. Система позволяет в реальном времени с любого компьютера, подключенного к Интернету, осуществлять авторизацию и проведение платежей, совершаемых при помощи кредитных карт. Необходимо отметить, что на момент написания настоящей книги данная система проходила сертификацию на соответствие стандарту SET. Это позволяет

предположить, что к моменту выхода книги из печати система Assist будет первой в России, удовлетворяющей этому стандарту.

Никакого дополнительного программного обеспечения, кроме браузера, для работы с системой в качестве пользователя устанавливать не требуется. Серверным программным обеспечением является DynaSite. Для обеспечения безопасности передаваемых данных от покупателя в Assist используется протокол SSL. Сертификат сервера выдан компанией Verisign. Система не анонимна, но конфиденциальная информация о кредитной карте клиента (реквизиты) в Интернет-магазин не передаются.

В проведении платежей через Интернет с помощью кредитных карт участвуют следующие стороны, ряд из которых отображены на представленной ниже схеме.

- Покупатель. Клиент, имеющий компьютер с web-браузером и доступом в Интернет.
- Банк-эмитент. В банке-эмитенте находится расчетный счет покупателя. Банк-эмитент выпускает карты и является гарантом выполнения финансовых обязательств клиента.
- Продавцы. Под продавцами понимаются электронные магазины, предлагающие товары и услуги и принимающие заказы покупателей на покупку.
- Банки-эквайеры. Банки, обслуживающие продавцов. У каждого продавца есть единственный банк, в котором он держит свой расчетный счет.
- Платежная система. Электронные компоненты, являющиеся посредниками между остальными участниками.
- Традиционная платежная система. Комплекс финансовых и технологических средств для обслуживания карт данного типа. Среди основных задач, решаемых платежной системой, — обеспечение использования карт как средства платежа за товары и услуги, пользование банковскими услугами, проведение взаимозачетов и т. д. Участниками платежной системы являются физические и юридические лица, объединенные отношениями по использованию кредитных карт.

- Центр обработки платежной системы. Организация, обеспечивающая информационное и технологическое взаимодействие между участниками традиционной платежной системы.

- Расчетный банк платежной системы. Кредитная организация, осуществляющая взаиморасчеты между участниками платежной системы по поручению центра обработки.

Схема расчетов при помощи кредитных карт VISA, Eurocard/MasterCard, Diners Club, JCB, American Express (AMEX) выглядит следующим образом:

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

2. Магазин формирует заказ и переадресует покупателя на авторизационный сервер системы Assist, одновременно на него же 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 карты (номер карты, дата окончания действия карты, имя держателя карты в той транскрипции, как оно указано на ней). Информация о карте 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.

5. Банк проверяет наличие такого магазина в системе, проверяет соответствие операции установленным системным ограничениям. По результатам проверок формируется запрет или разрешение на проведение авторизации транзакции в карточную платежную систему. При запрете авторизации расчетный банк системы передает авторизационному серверу Assist отказ от проведения платежа, при этом сервер передает покупателю отказ с описанием причины, а магазину — отказ с номером заказа, и на этом процедура заканчивается.

6. При разрешении авторизации запрос на нее передается через закрытые банковские сети банку-эмитенту карты покупателя или центру обработки карточной

платежной системы, уполномоченному банком-эмитентом. При отказе в авторизации банк передает авторизационному серверу Assist отказ от проведения платежа, а тот покупателю отказ с описанием причины, а магазину — отказ с номером заказа, и на этом процедура заканчивается.

7. В случае положительного результата, полученного от карточной платежной системы, банк передает авторизационному серверу Assist положительный результат авторизации.

8. Авторизационный сервер отправляет покупателю положительный результат авторизации, а магазину — его же с номером заказа.

9. Банк осуществляет перечисление средств на счет магазина в соответствии с существующими договорными отношениями между ним и магазином.

10. Магазин оказывает услугу (отпускает товар).

Для пользователей возможность работы с системой предоставляется бесплатно.

В случае Интернет-магазинов стоимость подключения к системе зависит от того, с каким расчетным банком заключен договор у магазина. Assist, со своей стороны, не взимает дополнительной платы за проведение транзакций. Расчетным банком взимается плата за следующие услуги.

- Подключение к системе — \$100–250. В эту сумму входит регистрация торговой точки в платежных системах (VISA, Europa и т. д.).
- Комиссионное вознаграждение за проведенные транзакции — 3–5 % от суммы платежа.

Абонентская плата с Интернет-магазинов не взимается, расчеты осуществляются в течение трех дней со дня проведения авторизации.

Дебетовые системы

Попытки кардинально устранить отмеченные недостатки платежных систем в Интернете на основе кредитных карт привели к разработке альтернативных видов платежных систем — так называемых «дебетовых систем», наиболее широкое распространение среди которых получили сегодня «электронные деньги».

Дебетовые схемы платежей в Интернете построены аналогично их традиционным прототипам: чековым и обычным денежным схемам. В схему вовлечены две независимые стороны: эмитенты и пользователи. Под эмитентом понимается субъект, управляющий платежной системой. Он выпускает некие электронные единицы, представляющие собой платежные средства (например, деньги на счетах в банках). Пользователи систем выполняют две главные функции. Они производят и принимают платежи через Интернет, используя выпущенные электронные единицы.

Электронные чеки

Электронные чеки являются аналогом обычных бумажных чеков, представляющие собой предписания плательщика своему банку перечислить деньги со своего счета на счет получателя платежа. Операция происходит при предъявлении получателем чека в банке. Основных отличий здесь два. Во-первых, выписывая бумажный чек, плательщик ставит свою настоящую подпись, а в виртуальном варианте — подпись электронная. Во-вторых, сами чеки выдаются в электронном виде.

Проведение платежей состоит из нескольких этапов:

1. Плательщик выписывает электронный чек, подписывает электронной подписью и пересылает его получателю. В целях обеспечения большей надежности и безопасности номер чекового счета можно закодировать открытым ключом банка.
2. Чек предъявляется к оплате платежной системе. Далее, либо здесь, либо в банке, обслуживающем получателя, происходит проверка электронной подписи.
3. В случае подтверждения подлинности электронной подписи поставляется товар или оказывается услуга. Со счета плательщика деньги перечисляются на счет получателя.

Российской системой, использующей описанную схему функционирования, является CyberPlat.

CyberPlat (www.cyberplat.ru) — универсальная межбанковская система платежей через Интернет. Система разработана специалистами банка «Платина» (www.platina.ru) и фирмой «Инист» (www.inist.ru). На сегодняшний день системой владеет компания Cyberplat.com. Фактически, CyberPlat является одной из первых российских систем, производящих электронные платежи через Интернет. На начало 2001 г. к системе

CyberPlat было подключено более ста пятидесяти Интернет-магазинов, а количество клиентов системы превышало 400 тыс. Оборот системы за 2000 г. составил 208 млн руб. (\$7,5 млн).

Система CyberPlat объединяет различные инструменты для ведения бизнеса в Интернете:

- CyberCheck — подсистема обслуживания транзакций класса B2B. CyberCheck обеспечивает конфиденциальность, надежность и юридическую чистоту взаимодействия сторон, а также полное отсутствие отказов от заявленных платежей. Это осуществляется механизмами поддержки электронного документооборота с применением электронной цифровой подписи с длиной ключа 512 бит. Благодаря перечисленным свойствам, подсистема используется в схемах класса B2B. Основой обеспечения безопасности в системе CyberCheck служит электронная цифровая подпись, применяемая для подписания договоров и соглашений, на основе которых происходят все переводы. Пользователь, подписавший документ, несет ответственность за выполнение описанных в нем обязательств. Для подписи в системе применяется асимметричный алгоритм криптографического преобразования с открытым ключом 512 бит;

- CyberPOS — подсистема обслуживания транзакций класса B2C для платежей по пластиковым картам международных и российских платежных систем;

- Inetnet-Banking — подсистема управления счетом в банке-участнике системы через Интернет.

Электронные деньги

Электронные деньги полностью моделируют реальные деньги. При этом эмиссионная организация — эмитент — выпускает их электронные аналоги, называемые в разных системах по-разному. Далее, они покупаются пользователями, которые с их помощью оплачивают покупки, а затем продавец погашает их у эмитента. При эмиссии каждая денежная единица заверяется электронной подписью, которая проверяется выпускающей структурой перед погашением.

Главное отличие электронных денег от реальных состоит в том, что первые предоставляют, по сути, электронные денежные обязательства выпустившей их

стороны, но настоящими деньгами с юридической точки зрения являться не могут. Применяющийся же термин «деньги» показывает, что электронные деньги в значительной степени наследуют свойства реальных наличных денег, главное из которых — анонимность, то есть на них не указано, кто и когда их использовал. Некоторые системы, по аналогии, позволяют покупателю получать электронную наличность так, чтобы нельзя было определить связь между ним и деньгами. Это осуществляется с помощью метода слепой подписи.

Стоит еще отметить, что при использовании электронных денег отпадает необходимость в аутентификации, поскольку система основана на выпуске денег в обращение.

1. Покупатель заранее обменивает реальные деньги на электронные. Хранение наличности у клиента может осуществляться двумя способами, что определяется используемой системой:

1. на жестком диске компьютера;
2. на смарт-картах.

Разные системы предлагают разные схемы обмена. Некоторые открывают специальные счета, на которые перечисляются средства со счета покупателя в обмен на электронные купюры. Некоторые банки могут сами эмитировать электронную наличность. При этом она эмитируется только по запросу клиента с последующим ее перечислением на компьютер или карту этого клиента и снятием денежного эквивалента с его счета. При реализации же слепой подписи покупатель сам создает электронные купюры, пересылает их в банк, где при поступлении реальных денег на счет они заверяются печатью и отправляются обратно клиенту. Наряду с удобствами такого хранения, у него имеются и недостатки. Порча диска или смарт-карты может обернуться невозвратимой потерей электронных денег.

2. Покупатель перечисляет на сервер продавца электронные деньги за покупку.

3. Деньги предъявляются эмитенту, который проверяет их подлинность.

4. В случае подлинности электронных купюр счет продавца увеличивается на сумму покупки, а счет покупателя уменьшается на эту же сумму и ему отгружается товар или оказывается услуга.

Наличные электронные деньги 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 сводится к минимуму, и такие системы могут эффективно использоваться для обеспечения микроплатежей — платежей менее \$1, где традиционные системы на основе кредитных карт экономически невыгодны. По общему мнению, именно микроплатежи в состоянии обеспечить основной оборот продаж информации в Интернете.

Эмитировать электронные наличные могут как банки, так и небанковские организации. Среди компаний, развивающих системы цифровых наличных, можно назвать NetCash, Citibank, DigiCash, Mondex. В России это — PayCash, WebMoney. Однако до сих пор не выработана единая система конвертирования разных видов электронных денег. Поэтому только сами эмитенты могут гасить выпущенную ими электронную наличность. Кроме того, использование подобных денег от нефинансовых структур не обеспечено гарантиями со стороны государства. Однако малая стоимость транзакции делает электронную наличность очень привлекательным инструментом платежей в Интернете.

Электронные деньги на базе смарт-карт

Как было сказано выше, электронные денежные обязательства могут храниться, переноситься и использоваться как при помощи специально разработанных электронных устройств, так и при помощи обыкновенного персонального компьютера.

Среди первых можно назвать так называемые смарт-карты (Smart Card) — пластиковые карты со встроенным микропроцессором, по виду похожие на обычные кредитные карты. Смарт-карта, по сути, представляет собой микрокомпьютер и содержит все соответствующие основные аппаратные компоненты: центральный процессор, ОЗУ, ПЗУ, ППЗУ, ЭСППЗУ. Параметры наиболее мощных современных микропроцессорных карт сопоставимы с характеристиками персональных компьютеров начала восьмидесятых. Операционная система, хранящаяся в ПЗУ микропроцессорной карты, принципиально ничем не отличается от операционной системы ПК и предоставляет большой набор сервисных операций и средств безопасности. Операционная система поддерживает файловую систему, базирующуюся в запоминающем устройстве ЭСППЗУ (емкость которого обычно находится в диапазоне 1–8 Кбайт, но может достигать и 64 Кбайт) и обеспечивающую регламентацию доступа

к данным. При этом часть данных может быть доступна только внутренним программам карты, что вместе со встроенными криптографическими средствами делает микропроцессорную карту высокозащищенным инструментом, который может быть использован в финансовых приложениях, предъявляющих повышенные требования к защите информации. Именно поэтому микропроцессорные карты в настоящее время рассматриваются как наиболее перспективный вид пластиковых карт. Кроме того, смарт-карты являются наиболее перспективным типом пластиковых карт также и с точки зрения функциональных возможностей. Вычислительные возможности смарт-карт позволяют использовать, например, одну и ту же карту и в операциях с авторизацией в режиме подключения и в качестве электронного «Кошелька». Их широкое внедрение в системах VISA и Europay/MasterCard начнется уже в ближайшие годы, а в течение десятилетия смарт-карты должны полностью вытеснить карты с магнитной полосой.

Из наиболее развитых международных проектов, использующих смарт-карты, можно отметить проект Mondex. Первый крупномасштабный пилотный проект платежной схемы Mondex реализован в г. Суиндон, Великобритания (июль 1995 г.). Сейчас Mondex поддерживается компаниями AT&T, Chase Manhattan, Dean Witter Discover, First Chicago NBD, MasterCard, Michigan National Bank, Wells Fargo и др.

В настоящее время в России развитием проекта с использованием различных смарт-карт как регионального платежного средства, занимается множество региональных банков. Самым крупным проектом внедрения смарт-карт в нашей стране является проект Сбербанка России — Сберкарт. Эта система предлагает использовать смарт-карты как для традиционных расчетов, так и для расчетов через Интернет с помощью специального устройства — считывателя карт, подключаемого к компьютеру через порты USB или COM. Деньги хранятся в виде записей в памяти компьютера, размещенного на карте, и могут передаваться с одного «Кошелька» в другой через специальное устройство — кассу. В случае необходимости при помощи другого специального устройства — банкомата, электронные деньги могут быть помещены на банковский счет, получены наличными в кассе или банкомате. Торговля через Интернет при помощи смарт-карт Сбербанка совершается при помощи специального устройства для ее связи с компьютером.

Основными барьерами на пути широкого распространения смарт-карт в качестве платежного инструмента в Интернете сегодня является достаточно низкое их распространение по сравнению с обыкновенными магнитными картами, а также необходимость наличия периферийного считывающего устройства, подключаемого к компьютеру. Основными требованиями, предъявляемыми к устройствам для считывания смарт-карт, является удобство использования, удовлетворение всех требований безопасности и низкая стоимость. Сегодня стоимость подобных устройств составляет более \$40.

Электронные деньги на базе персональных компьютеров

Альтернативой смарт-картам при осуществлении внедрения идеи электронных денег является использование персональных компьютеров и специализированного программного обеспечения, реализующего все необходимые для этого функции.

Одной из первых систем является eCash — система электронных платежей фирмы DigiCash. Система разработана на основе патентов Дэвида Чаума (David Chaum) и предназначена для представления денежных купюр различного достоинства в цифровой форме. В этом виде электронная монета (как последовательность цифр) может быть послана по Интернету, продиктована по телефону, отправлена по факсу или в письме. Однако основное применение цифровых денег — осуществление платежей через Интернет. Цифровая монета в виде последовательности данных может сохраняться пользователем на жестком диске своего компьютера и передаваться по сети или электронной почте. Продавец, получив через Интернет цифровую монету, предъявляет ее в банк для авторизации. После авторизации соответствующая цифровой монете сумма заносится на расчетный счет продавца.

Существенным недостатком платежной системы Чаума можно считать необходимость клиентам доверять банку. В платежной системе Чаума, нет механизмов, позволяющих независимо от банка проверить, использовалась ли ранее цифровая монета или нет. Клиент вынужден полагаться на правдивость ответа банка, что подспудно указывает на возможность обмана путем присваивания банками цифровых денег клиентов. Следует отметить, что этот недостаток не является отличительным свойством монет Чаума, а выражает основное свойство сертификатов на предъявителя. Сертификаты на предъявителя не имеют никакой связи с лицом предъявляющим его, при помощи которой оно могло бы доказать свои права на сертификат. Таким образом,

в системе Чаума возможны конфликты, неразрешимые средствами самой системы. Внесистемное решение этой проблемы может привести к удорожанию платежной системы в целом, так как для обработки конфликтов требуются особые организационные меры (страховые фонды, черные списки и т. п.). Другим существенным недостатком платежной системы Чаума является невозможность получения сдачи. Это вынуждает клиентов дополнительно обращаться в банк за разменом монет, чтобы заплатить продавцу точно требуемую сумму, что, в конечном итоге, усложняет элементарную операцию покупки, не говоря уже об увеличении базы данных использованных монет, которую надо проверять при каждом новом платеже.

Основной областью применения платежной системы является электронная коммерция. Для того чтобы разрешать конфликты периодически возникающие в торговой системе, покупатель должен иметь возможность доказать факт оплаты конкретного товара. В системе Чаума отсутствуют встроенные средства интегрирования с торговой системой. Поэтому у покупателя кроме программы «Кошелек» (клиента платежной системы) должно быть характерное для данной системы программное обеспечение покупателя (клиента торговой системы), которое должно связывать перевод денег с соответствующим переходом права собственности на товар или услугу.

Надо отметить, что при несомненной оригинальности защищенных рядом патентов идей, заложенных в описанной платежной системе, неэффективная маркетинговая стратегия компании DigiCash, заключающаяся в политике уполномоченных банков — «одна страна один электронный банк», сузила привлекательность данной платежной системы и, в конце концов, привела компанию к банкротству. В настоящее время продолжателем дела DigiCash компания eCash осуществляет операции только через Deutsche Bank, хотя в 1997–1999 г. систему цифровых монет поддерживали около десяти банков Западной Европы и США.

Указанные недостатки преодолены в одной из Российских систем, реализующих идею «электронных денег» — системе PayCash (www.paycash.ru), совместной разработке банка «Таврический» и группы компаний «Алкор-Холдинг».

PayCash позволяет множеству различных банков одновременно оперировать в одной электронной платежной системе, взаимодействуя на основе универсальных денежных единиц, принимаемых в оборот любым из этих банков. Кроме банков в

системе существуют рядовые пользователи. Пользователями могут выступать юридические и физические лица или программные продукты, представляющие их, например, Интернет-магазины. С точки зрения банка все пользователи системы полностью равноправны.

В системе PayCash принципиально невозможен случайный или преднамеренный обман любого участника платежной системы банком или другим участником благодаря тому, что каждая операция обязательно сопровождается электронными цифровыми подписями всех ее участников. Специальное программное обеспечение — «Кошелек» — фактически хранит (наряду с собственными электронными деньгами) договоры купли продажи, подписанные электронными цифровыми подписями участников операции. Денежные средства пользователя (покупателя или продавца) могут находиться на счете в банке системы PayCash или непосредственно на компьютере пользователя в «Кошельке». Счет системы PayCash может управляться только через Интернет при помощи того «Кошелька», с помощью которого он был открыт — сам банк не может управлять этим счетом. На владельца «Кошелька» накладывается полная ответственность за его сохранность как средства управления счетом и совершения сделок при помощи электронных денег. На денежные средства, находящиеся на счете, могут начисляться банковские проценты, например, как на депозитные счета.

Непосредственно электронные деньги в системе PayCash появляются в момент перевода денег со счета системы на платежную книжку в «Кошельке» пользователя. Использование процедуры слепой подписи обеспечивает возможность пользователям платежной системы получать электронные денежные обязательства, которые не могут быть не признаны банком.

Специальная процедура позволяет использовать эти денежные обязательства частями по мере необходимости. Клиент может неоднократно пополнять платежную книжку в банке и выполнять с ее помощью платежи на любую сумму в пределах находящихся на ней средств, не задумываясь о необходимости их размена. Любые изменения состояния платежной книжки делаются только по инициативе владельца и обязательно подтверждаются банком. Неподтвержденные банком изменения через определенное время или по инициативе пользователя отменяются, и на платежной книжке восстанавливается прежняя сумма.

Необходимо отметить, что любая операция в системе PayCash обязательно подтверждается электронными цифровыми подписями ее участников. Кроме непосредственно электронных денег «Кошелек» передает информацию, на основании которой производится та или иная операция.

Рассмотрим более подробно, как происходит взаимодействие участников системы между собой, а также с самой системой:

1. Покупатель переводит деньги в банк системы, устанавливает на своем компьютере программное обеспечение электронного «Кошелька» и получает эмитированные банком цифровые сертификаты.

2. Покупатель выбирает товар в электронном магазине и отправляет ему заказ.

3. «Кошелек» продавца отправляет «Кошельку» покупателя требование об оплате, содержащее подписанный электронной цифровой подписью текст договора.

4. «Кошелек» покупателя предъявляет своему владельцу текст договора. Если покупатель соглашается платить (при достаточном количестве денег у него), то «Кошелек» покупателя отправляет «Кошельку» продавца электронные деньги и подписанный электронной цифровой подписью покупателя договор.

«Кошелек» принимает платежи только на основании договоров, переданных потенциальным покупателям. Для него можно определить период, в течение которого он будет принимать платежи по отосланным договорам, таким образом, магазин может удалять из своей базы данных устаревшие неоплаченные заказы. После проверки этих условий продавец отправляет электронные деньги в банк для авторизации.

5. Банк, получив от него электронные деньги, проводит их авторизацию.

6. В случае положительного результата авторизации банк зачисляет соответствующую сумму денег на счет продавца в системе PayCash. Сообщение об этом передается «Кошельку» продавца вместе с электронным чеком для покупателя.

7. Получив ответ из банка, «Кошелек» передает магазину данные авторизации и сообщение об успешном зачислении денег на счет продавца. Электронный чек из банка пересылается «Кошельку» покупателя.

При совершении операции покупки при помощи системы PayCash вместе с электронными деньгами передается и договор купли продажи между участниками сделки. В процессе платежа этот договор оказывается автоматически подписанным электронными цифровыми подписями владельцев «Кошельков», принимающих и передающих деньги согласно этому договору. Таким образом, у покупателя в «Кошельке» остается экземпляр электронного документа, подтверждающего товарные обязательства продавца, с его электронной цифровой подписью.

Система PayCash предполагает возможность участия в ней неограниченного числа банков, каждый из которых может выпустить собственные электронные деньги, которые могут находиться в одном «Кошельке». При этом управление счетами в разных банках будет осуществляться с помощью одного и того же программного обеспечения.

Для демонстрационных целей в рамках системы PayCash наряду с реально работающим банком работает демонстрационный банк. Демонстрационный банк оперирует с игрушечными деньгами, которые можно заказать и получить на сайте совершенно бесплатно.

Выводы

- Интернет — глобальная компьютерная сеть, базирующаяся на едином стеке протоколов — TCP/IP. TCP/IP обеспечивает соединение различных физических сетей друг с другом. При этом детали этого соединения «скрыты» от пользователей, что дает им возможность работать как бы в одной большой физической сети.

- Системы, предоставляющие услуги пользователям Интернета, называются службами Интернета. К ним относятся: электронная почта, WWW, телеконференции, списки рассылки, FTP, IRC, Интернет-пейджеры, а также другие, использующие Интернет как среду передачи информации.

- Одним из важнейших условий широкого применения Интернета было и остается обеспечение адекватного уровня безопасности для всех транзакций, проводимых через него. Решить проблемы безопасности призвана криптография — наука об обеспечении безопасности данных. Криптография и построенные на ее основе системы решают задачи конфиденциальности, аутентификации и целостности

информации. Основными методами обеспечения безопасности при этом выступают шифрование, цифровая подпись и сертификаты.

- Наиболее распространенными механизмами, обеспечивающими безопасность в среде Интернет, являются протокол SSL (Secure Socket Layer), выполняющий шифрование передаваемых через Интернет данных и стандарт SET (Secure Electronic Transactions), разработанный компаниями Visa и MasterCard и обеспечивающий безопасность и конфиденциальность совершения сделок при помощи пластиковых карт.

- Основной движущей силой развития Интернета в качестве глобального электронного рынка служат электронные платежные системы, делающие возможным проведение расчетов между финансовыми, коммерческими организациями и пользователями Интернета в процессе покупки/продажи товаров и услуг через него. Платежные системы делятся на два основных направления: кредитные системы и дебетовые системы.

Вопросы для обсуждения

1. Назовите факторы, оказавшие влияние на повсеместное распространение и использование Интернета? Какие из них оказали самое существенное влияние и почему?

2. Первоначально, самой распространенной службой Интернета была электронная почта. Развитие сети Интернет добавило в список самых популярных служб, прежде всего, службу WWW, телеконференции, чаты и ряд других. Попробуйте дать прогноз пути дальнейшего развития Интернета и его служб. Какие службы будут пользоваться наибольшей популярностью и почему? Как будет преобразовываться среда Интернет под воздействием современных информационных технологий? Как будет выглядеть Интернет через несколько лет?

3. Проблема обеспечения безопасности в Интернете на протяжении всего срока его существования, а тем более, коммерческого использования, была одной из основных. Вместе с тем, многие эксперты отмечают, что эта проблема больше связана с психологическим восприятием опасности, чем объективной ее оценкой. Также большое влияние на восприятие этой проблемы оказывает отсутствие широкой практики и традиций использования Интернета в качестве средства покупки и оплаты

товаров. Как Вы оцениваете уровень безопасности при работе в Интернете и совершении через него покупок? Какие меры могут быть предприняты компаниями или правительственными организациями для решения этой проблемы?

4. Платежные системы действуют в Интернете уже достаточно давно, по крайней мере, если судить по динамике развития, характерной для глобальной Сети. Сегодня только в Российском сегменте Интернета реально работает более десятка таких систем. Несмотря на это, число клиентов и организаций, пользующихся их услугами, остается достаточно ограниченным. С чем Вы это связываете? Назовите основные параметры и характеристики платежных систем Интернета, которые в первую очередь определяют их успешность развития и эффективность? В какой степени эти параметры достигнуты существующими Российскими примерами?

5. Согласно приведенной в главе классификации, существующие платежные системы делятся на два вида — кредитные и дебетовые. Системы какого вида на Ваш взгляд имеют наибольшие перспективы развития и почему?