МЕТОДЫ И СРЕДСТВА ЭЛЕКТРОННОГО БИЗНЕСА

Тексты лекций и материалы
семинарских занятий.
Очная и заочная форма обучения - 2021

Чмырь И.А.

СОДЕРЖАНИЕ

Удалённое чтение лекций проводится по расписанию занятий в сервисе Zoom.
Идентификатор персональной конференции лектора: **3394775925**.
Код доступа: **9JHWLS.**

ПРЕДИСЛОВИЕ

Дисциплина «Методы и средства электронного бизнеса» является продолжением и развитием дисциплины «Электронная коммерция». Многие важные понятия, которые используются в дисциплине «Методы и средства электронного бизнеса», введены и определены в дисциплине «Электронная коммерция». Для того чтобы вспомнить определения этих понятий и контекст, в котором они используются, в конспект лекций по дисциплине «Методы и средства электронного бизнеса» включены ссылки на разделы и подразделы конспекта лекций по дисциплине «Электронная коммерция». Во всех случаях, когда в конспекте встречается ссылка на материал дисциплины «Электронная коммерция» необходимо перечитывать соответствующие разделы и подразделы.

В последние годы часто обсуждаются вопросы, связанные с цифровым бизнесом и цифровой экономикой. Как считают многие специалисты, реализация идей цифрового бизнеса и развитие цифровой экономики являются радикальным средством повышения производительности труда и ускорения развития экономики. В ряде стран цифровая экономика является национальным приоритетом экономических реформ. Однако, часто, те люди, которые принимают решения о внедрении цифровой экономики, поверхностно знакомы с тем, что входит в объём понятия «цифровая экономика». Дисциплины «Электронная коммерция» и «Методы и средства электронного бизнеса», в совокупности, могут рассматриваться как введение в проблематику цифрового бизнеса и цифровой экономики.

Потребность в дипломированных специалистах в области цифровой экономики растёт. Такие специалисты не могут быть «чистыми компьютерщиками» или «чистыми экономистами». Необходимо сочетание знаний, как в области информационных технологий и компьютерных сетей, так и в области методов и средств электронного бизнеса.

В дисциплине «Методы и средства электронного бизнеса» используется свой, специфический набор понятий и терминов. В конспекте лекций эти термины выделены курсивом и приведен их перевод на английский язык. Необходимо запомнить и русскоязычные и англоязычные наименования этих терминов и их аббревиатуры, поскольку и те другие могут встретиться в литературе и на страницах Web-сайтов.

При подготовке сообщений на семинарских занятиях и поиске дополнительной информации в Web, необходимо знакомится как с русскоязычными, так и с англоязычными публикациями. Многие вопросы этой дисциплины более полно освящены в англоязычных статьях. При поиске информации на английском языке, в качестве ключевых слов, следует использовать англоязычные термины и словосочетания, приведенные в конспекте. Чтение англоязычных публикаций, при подготовке к семинарским занятиям, может рассматриваться как дальнейшее совершенствование знаний и навыков в области английского языка.

В конспекте лекций шрифтом Arial выделены наименования коммерческих компаний, неприбыльных организаций, а также наименования аппаратных и программных средств и систем. Web-сайты компаний, наименования которых выделены шрифтом Arial, необходимо посетить. Полезно, также, читать статьи, посвященные компаниям, аппаратным и программным средствам, наименования которых выделенным шрифтом Arial, в онлайновой энциклопедии Wikipedia.

1. ЭЛЕКТРОННАЯ КОММЕРЦИЯ ТИПА БИЗНЕС-БИЗНЕС

1.1. Приобретение материалов, логистика и поддерживающие деятельности

Раздел посвящен тому, каким образом компании используют технологию электронной коммерции для улучшения таких первоочередных деятельностей как приобретение материалов и доставка конечного продукта (логистика), а также всех поддерживающих деятельностей (финансы и администрирование, трудовые ресурсы и технологическое развитие). Улучшение эффективности перечисленных деятельностей оказывает существенное влияние на уменьшение стоимости конечного продукта и, в итоге, на увеличение прибыли компании.

Описание первоочередных и поддерживающих деятельности стратегического бизнес-блока смотри в конспекте лекций по дисциплине «Электронная коммерция» (подраздел 1.6.1 и рис. 1.8).

1.1.1. Аутсорсинг и офшоринг

Эластичность и гибкость является важной характеристикой таких первоочередных деятельностей как приобретение материалов и логистика, а также всех поддерживающих деятельностей бизнес-блока. Стратегия приобретения материалов или стратегия логистики, которая хорошо работала в прошлом году, может быть неэффективной в текущем году.

Экономическая организация общества развивается в направлении от иерархической формы, используемой со времён Индустриальной революции, к более гибкой сетевой форме. Сетевая форма экономической организации становится возможной в том случае, когда стоимость транзакций уменьшается за счёт использования компаниями технологии электронной коммерции.

Аутсорсинг (outsourcing) является характерным признаком сетевой формы экономической организации. Аутсогсингом, в общем случае, называется передача стороннему подрядчику некоторых деятельностей компании. Примером компании, специализирующейся на аутсорсинге является американская Paychex. Компания Paychex оказывает услуги по обслуживанию наёмных работников для тысяч сторонних компаний и организаций. Эти услуги включают составление платёжных ведомостей, подбор кадров, медицинское страхование и др.

Когда аутсорсинг осуществляется подрядчиком, находящимся в другой стране, он часто называется *офшоринг* (offshoring). Аутсорсинг и офшоринг используются компаниями в течение десятилетий. В ранних системах аутсорсинга и офшоринга деятельности, которые передавались сторонним подрядчикам, обычно носили производственный характер. Например, компании Apple или Motorola разрабатывали и проектировали мобильные телефоны, а затем передавали их производство и сборку сторонним подрядчикам в азиатских странах. Технология электронной коммерции позволяет осуществлять офшоринг многих непроизводственных деятельностей, таких как приобретение материалов, технологическое развитие, делопроизводство и информационный менеджмент. Этот тип офшоринга часто называют *офшорингом бизнес-процесса* (business process offshoring). Офшоринг может осуществляться и неприбыльными организациями. В этом случае доходы, которые получают сторонние подрядчики, используются для поддержки обучения или благотворительности в экономически слабо развитых странах.

1.1.2. Приобретение материалов

Приобретение материалов включает: (1) выбор поставщиков; (2) оценку поставщиков; (3) выбор материалов; (4) размещение заказов, а также (5) разрешение проблем, которые могут возникнуть после получения заказанных материалов. Проблемы, которые могут возникнуть включают: поставку материалов после оговоренного срока, неправильное количество поставленных материалов, дефектные материалов и т.п. Путем монито-

ринга элементов транзакции по приобретению материалов, менеджер, ответственный за их приобретение, вносит существенный вклад, как в качество конечного продукта, так и в снижение расходов.

Стратегический бизнес-блок компании функционирует внутри индустриальной ценностной цепи (см. подраздел 1.6.2 в конспекте лекций по дисциплине «Электронная коммерция»). Часть индустриальной ценностной цепи, которая предшествует некоторому стратегическому бизнес-блоку, называется *цепью поставок бизнес-блока* (business unit's supply chain). Цепь поставок включает первоочередные деятельности, осуществляемые предшественниками бизнес-блока в индустриальной ценностной цепи. Например, цепь поставок для производителя автомобилей включает первоочередные деятельности выполняемые поставщиками каждого компонента автомобиля (двигателя, стального листа, стекла, жгутов электрических кабелей и тысяч других).

Отделы по приобретению материалов большинства компаний, традиционно нацелены на приобретение материалов по наиболее низкой цене. Обычно, персонал этих отделов осуществляет приобретение материалов, используя следующую стратегию. Всем потенциальным поставщикам предлагается подготовить коммерческие предложения с описанием характеристик и стоимости поставляемых материалов. Затем осуществляется выбор предложения с наименьшей ценой, которое, тем не менее, удовлетворяет требуемым стандартам качества. Отмеченный процесс выбора поставщика порождает конкурентную среду с большим количеством потенциальных поставщиков. Внимание фокусируется исключительно на стоимости индивидуальных материалов и игнорируется вся сеть поставок, включая дополнительные расходы компании на работу с чрезмерно большим количеством поставщиков. Часто, вместо словосочетания «приобретение материалов» используется термин «*снабжение*» (procurement), который подразумевает более широкий список деятельностей. Понятие «снабжение», в общем случае, включает все деятельности по приобретению плюс мониторинг элементов транзакции и развитие отношений с ключевыми поставщиками.

При описании снабженческой деятельности используют термин «*управление снабжением/поставками*» (supply management). Персонал компании, занятый управлением поставками, должен обладать высоким уровнем профессиональных знаний о материалах. Эти знания необходимы для выбора и оценки квалифицированных и надёжных поставщиков. Часть снабженческой деятельности, целью которой является идентификация поставщика и определение его квалификации, называется *поиск источников* (sourcing).

Снабженческая деятельность с использованием технологии электронной коммерции носит наименование *электронное снабжение* (e-procurement), а использование технологии электронной коммерции для идентификации и определении квалификации поставщика – *электронным поиском источников* (e-sourcing). Профессионалы, занятые электронным поиском источников используют как Web-сайты поставщиков, так и Web-сайты, созданные специально для помощи при поиске источников.

Бизнес-процесс по приобретению материалов намного сложнее, чем процесс приобретения товаров и услуг обычными покупателями. На рис. 1.1 изображены деятельности типичного бизнес-процесса по приобретению материалов.

Процесс приобретения материалов включает много деятельностей. В этот процесс вовлечено большое количество специалистов, которые должны согласовывать свою индивидуальную деятельность с общим процессом. В больших компаниях отдел по приобретению материалов, занятый управлением снабжением, включает сотни специалистов. Денежный эквивалент всех приобретенных материалов называется *расходами* (spend) компании. Расходы больших компаний исчисляются миллиардами долларов. Поэтому *управление расходами* является важной функцией управления компанией и является одним из ключевых элементов её прибыльности. Расходы основных международных производственных компаний превышают 50 миллиардов долларов в год. Эти компании ежегодно приобретают миллионы наименований материалов. Использование электронного снабжения позволяет этим компаниям каждый год экономить миллиарды долларов.

Рис. 1.1. Деятельности типичного бизнес-процесса по приобретению материалов

Прямые и непрямые материалы

Предприятия различают *прямые* (direct) и *непрямые* (indirect) материалы. К прямым материалам относятся те материалы, которые становятся частью конечного продукта. Например, производители стали рассматривают железную руду, которую они приобретают, в качестве прямого материала. Снабжение компании прямыми материалами является важной частью любого производственного процесса, поскольку стоимость прямых материалов, как правило, составляет значительную часть стоимости конечного продукта.

Большие производственные компании, такие, например, как производители автомобилей, используют два способа приобретения прямых материалов. Первый способ приобретения прямых материалов называется *наполнительное приобретение* или *контрактное приобретение* (contract purchasing). Контрактное приобретение означает, что компания заключает долгосрочные контракты на приобретение материалов, которые ей понадобятся в течение некоторого времени. Например, предприятие, производящее автомобили, прогнозирует количество автомобилей, которые оно планируют выпустить в течение года и заключают долгосрочные контракты с двумя или тремя сталелитейными заводами для приобретения стального листа, необходимого для производства этих автомобилей. Поскольку долгосрочные контракты заключаются заблаговременно, и их оплата гарантируется, то производитель автомобилей может получить низкие цены и выгодные условия поставки прямых материалов. Часто, реальное потребление прямых материалов не совпадает, в точности, с их прогнозируемым количеством. Если, например, реальное

потребление стального листа выше, чем прогнозируемое, то компания должна приобретать дополнительный стальной лист. Приобретение дополнительного стального листа осуществляется на плохо организованном рынке, который включает сталелитейные заводы, склады, перекупщиков (перепродающих контракты) и компании, имеющие избыток стального листа (компании у которых реальное потребление оказалось ниже, чем прогнозируемое). Этот рынок называется *рынком наличных товаров* или *спотовым рынком* (spot market). Приобретение прямых материалов на спотовом рынке является вторым способом приобретения прямых материалов.

К непрямым материалам относятся все остальные материалы, которые необходимы для производства и которые приобретает компания: ручной инструмент, запасные части для производственного оборудования и т.п. Производители ручного инструмента, запасных частей и других непрямых материалов, как правило, продают их при помощи Web-сайтов. Бóльшая часть непрямых материалов относится к предметам потребления. Предметом потребления (или сырьевым товаром) мы называем товар или услугу, которые трудно отличить от товара или услуги, продаваемых различными продавцами, поскольку их свойства стандартизованы и хорошо известны. Поэтому выбор поставщика для таких непрямых материалов осуществляется исключительно по критерию стоимости. Непрямые материалы, которые необходимы для производства часто называют материалами для *технического обслуживания и ремонта* (ТОиР). В англоязычной литературе – Maintenance, Repair & Overhaul (MRO). Отделам снабжения сложно учитывать расходы, связанные с приобретением материалов, необходимых для ТОиР, поскольку приобретается большое количество товаров, имеющих невысокую стоимость. Для решения задачи учёта этих материалов некоторые компании снабжают своих менеджеров специальными *закупочными картами* (purchasing cards или p-cards). Закупочные карты имеют сходство с обычными платежными картами и, с одной стороны, предоставляют менеджерам свободу выбора, а с другой, позволяют легко осуществлять учёт всех купленных материалов.

Многие компании включают в список непрямых материалов также все товары или услуги, которые непосредственно не связаны с производственным процессом, но необходимы для работы офисов. Например, компьютерное оборудование и программное обеспечение, расходные материалы, используемые в офисе, а также командировочные расходы.

В небольших компаниях приобретением прямых и непрямых материалов занимается один централизованный отдел снабжения. В больших компаниях приобретение прямых и непрямых материалов осуществляется различными отделами.

Сегодня, практически все компании приобретают непрямые материалы при помощи технологии электронной коммерции, которая исключает расходы на изготовление и рассылку печатных каталогов, ведение телефонных переговоров и позволяет быстро актуализировать информацию в базах данных. По оценкам некоторых аналитиков *стоимость обработки заказа на приобретение материалов, необходимых для ТОиР, через Web-сайт в десять раз дешевле, чем в том случае, когда это осуществляется по телефону с использованием печатных каталогов*.

Наиболее крупными международными компаниями, осуществляющими онлайновую продажу материалов для ТОиР, являются компании McMaster-Carr и W.W. Grainger. Каталог Web-сайта W.W. Grainger содержит более 900 тысяч наименований. Лидерами онлайновых продаж офисных непрямых материалов являются компании Office Depot и Staples.

1.1.3. Логистическая деятельность

Классическая задача логистики заключается в доставке нужных товаров в нужном количестве в нужное место и в нужное время. Управление логистикой является важной деятельностью, как компании продавца, так и компании покупателя. Компании должны быть уверены в том, что продукты, которые они продают своим клиентам, доставляются вóвремя, а материалы, которые они покупают у своих поставщиков для создания собственных продуктов, поступают тогда, когда они необходимы. Управление перемещением

материалов по мере их движения от склада исходных материалов через производственный процесс и превращение в готовую продукцию также является важной частью логистики.

Логистическая деятельность включает управление перемещением прибывающих материалов и управление перемещение убывающих готовых продуктов. Таким образом, получение материалов, их складирование, инвентаризация, диспетчеризация и управление транспортом, а также дистрибуция готовой продукции являются компонентами логистической деятельности. Технология электронной коммерции предоставляет всё возрастающее количество методов и средств для эффективного управления этими деятельностями, обеспечивая, при этом, снижение стоимости транзакций и постоянную связь между компаниями, вовлеченными в логистические связи. Автоматизированные склады с Web-поддержкой позволяют компаниям ежегодно экономить миллионы долларов. Крупные транспортные компании, такие как Schneider National, Ryder System, Inc. и J.B. Hunt позиционируют себя не только как перевозчики грузов, но и как компании, занимающиеся информационным менеджментом.

Например, система Track and Trace компании Schneider предоставляет информацию о транспортировке груза в реальном масштабе времени непосредственно на Web-браузер заказчика. Система отображает информацию о том, какой транспорт осуществляет доставку груза, где находится груз в данный момент времени и когда он будет доставлен в место назначения. Компания J.B. Hunt, оперирующая тысячами грузовиков, трейлеров, контейнеров и другим мобильным имуществом, создала Web-сайт который позволяет клиентам самостоятельно следить за доставкой груза. Передав функцию мониторинга доставки груза своим клиентам, компания J.B. Hunt может оперировать с гораздо меньшим количеством персонала, обслуживающего запросы клиентов. Компания также обнаружила, что клиенты осуществляют мониторинг более эффективно, чем персонал компании. Это позволяет компании еженедельно экономить более 12000 долларов.

Некоторые транспортные компании специализируются на предоставлении своим заказчикам комплекса логистических услуг от доставки и адресного хранения груза до управления заказами и отслеживание транспортировки груза. Такие компании называются *третьей стороной-провайдером логистических услуг* (3ПЛУ). В англоязычной литературе – third-party logistics provider (3PL). Например, упомянутая выше транспортная компания Ryder заключила с компанией Whirlpool (производитель и продавец бытовой техники) многолетний контракт на оперирование деятельностью этой компании по доставке всех приобретаемых материалов или комплектующих и является примером 3ПЛУ для компании Whirlpool.

Логистические компании, эксплуатирующие собственные системы слежения за перемещением груза, используют спутниковые системы навигации (GPS или ГЛОНАСС) для получения информации о движущемся транспортном средстве в реальном масштабе времени. Эта информация включает не только местоположение грузовика или трейлера, но и данные о его текущей скорости, положении дроссельной заслонки, потреблении топлива и т.п. Для покрытия дополнительных расходов, связанных с внедрением подобных систем, такие компании, как правило, работают как 3ПЛУ провайдеры.

Водители грузовиков также получают выгоду от использования мобильных компьютеров, сопряженных со спутниковыми системами навигации. В недалеком прошлом водитель-дальнобойщик полагался исключительно на бумажные карты и сведения, получаемые по радио для того чтобы избежать задержек, связанных с «пробками», погодными условиями и дорожными работами. Сегодня, специальные приложения для мобильных компьютеров предупреждают водителя обо всех подобных рисках. Такие мобильные приложения предоставляют информацию о перманентных неудобствах (узкий участок дороги, резкий поворот, участок дороги, запрещённый для проезда коммерческого транспорта), а также временных неудобствах (напряженный трафик, дорожные работы, полицейские радары, контролирующие скорость). Приложения могут, также, информировать водителя о «хороших» ценах на топливо на заправочных станциях и на еду в придорожных кафе.

1.1.4. Поддерживающие деятельности

Поддерживающие деятельности стратегического бизнес-блока включают деятельности, направленные на решения финансовых и административных задач, оперирование трудовыми ресурсами и деятельности, направленные на технологическое развитие компании.

Деятельности, направленные на решение финансовых и административных задач включают: осуществление платежей поставщикам; обработка платежей, полученных от клиентов; планирование капитальных расходов; а также планирование и составление бюджета гарантирующего наличие достаточных денежных средства для погашения долгов в соответствующие сроки. Административная деятельность также включает деятельности по управлению компьютерной инфраструктурой и базой данных компании.

Оперирование трудовыми ресурсами включает: рекрутирование и приём на работу новых работников; обучение и оценивание наёмных работников; администрирование пособиями и вознаграждениями; ведение учёта в соответствии с правительственным инструкциями.

Технологическое развитие включает: объединение исследователей в виртуальные рабочие группы; коллективное использование результатов научных исследований; публикация результатов исследований в электронной форма; связь с внешними компаниями, предоставляющими услуги в области научно-исследовательских и опытно-конструкторских работ – НИОКР (Research and Development – R&D). В таблице, на рис. 1.2, приведены, перечисленные выше, категории поддерживающих деятельностей.

Финансы и администрирование	**Трудовые ресурсы**	**Технологическое развитие**
Осуществление платежей поставщикам.	Приём на работу новых работников.	Создание виртуальных научно-исследовательских рабочих групп.
Обработка платежей, полученных от клиентов.	Обучение наёмных работников.	Коллективное использование результатов исследований.
Планирование капитальных расходов.	Оценивание наёмных работников.	Публикация результатов исследований в электронной форме.
Планирование и составление бюджета.	Администрирование пособиями и вознаграждениями.	Связь с внешними компаниями, предоставляющими услуги в области НИОКР
Управлению компьютерной инфраструктурой и базой данных.	Ведение учёта в соответствии с правительственным инструкциями.	

Рис. 1.2. Категории поддерживающих деятельностей

Оперирование трудовыми ресурсами, составление платёжных ведомостей и пенсионных планов относятся к тем областям, которые регламентируются большим количеством инструкций и правил, разобраться в которых может только эксперт. Поэтому небольшие и средние, по размеру, компании, при управлении трудовыми ресурсами часто прибегают к аутсорсингу. Сегодня, большое количество компаний работают как онлайновые аутсорсинг-провайдеры услуг по управлению трудовыми ресурсами. Примером компании, которая предлагает полный список онлайновых услуг по управлению трудовыми ресурсами является компания CheckPoint HR. Компания Advantage Payroll специализируется на оказании онлайновых услуг по составлению платежных ведомостей. Перечисленные компании воспроизводят свои функции на Web-сайте, который доступен как сотрудникам компании клиента, так и её наёмным работникам. Наёмные работники могут получить доступ к информации о своих пособиях и вознаграждениях, ответы на часто

задаваемые вопросы и, даже, самостоятельно рассчитать возможные варианты вознаграждений.

Одной из поддерживающих деятельностей, которая ассоциирована со множеством первоочередных деятельностей является обучение. Во многих коммерческих компаниях обучением занимается Отдел кадров (Human Resources Department), однако некоторые компании передают функцию по управлению обучением в отдельное подразделение. Например, страховые компании тратят значительные ресурсы на обучение методам продажи продуктов компании. В большинстве страховых компаний этим обучением занимается Отдел продажи и маркетинга (Sales and Marketing Department). Путём размещения обучающих материалов на сервере своей интранет сети, страховая компания обеспечивает их распределение среди всех офисов, занимающихся продажей, а также координирует использование обучающих материалов из центрального офиса.

Шведская телекоммуникационная компания Ericsson использует сеть экстранет для распространения информации, предназначенной для текущих и бывших наёмных работников компании и её бизнес партнёров. Общее количество наёмных работников компании Ericsson, разбросанных по всему миру, составляет около 120 тысяч человек. Одна из частей этой сети содержит Web-сайт, который позволяет текущим работникам компании, пенсионерам и другим получателям денежных средств, в соответствии с медицинской и пенсионной программам, эффективно отслеживать состояние своих пенсий и пособий. Другая часть сети включает Web-сайт, спроектированный для поддержки системы *управления знаниями* (knowledge management – KM). Управление знаниями предполагает преднамеренной накопление, классификацию и распространение знаний о компании, её продуктах и развитии. Этот тип знаний создается в течение длительного времени личностями, работающими на компанию или с компанией и, часто, их трудно извлекать и собирать.

Менеджеры компании Ericsson уверены, что их сеть управления знаниями генерирует новые идеи, помогает решать проблемы и улучшает бизнес-процессы, повсеместно в этой большой международной компании. Проектировщики системы управления знаниями компании Ericsson считают, что одной из наиболее сложных задачей, при проектировании системы, является задача направления информации, собранной при помощи сети экстранет, в те проекты и работы для которых она необходима и полезна. Много полезной информации о направлении Управление знаниями содержится на страницах сайта KMWorld.

1.1.5. Электронное правительство

Правительство выполняет множество важных функций, регламентирующих жизнь и деятельность как отдельных личностей, так и коммерческих компаний и некоммерческих организаций. Правительство, также осуществляет деятельность аналогичную деятельности коммерческих компаний. Например, правительство нанимает на работу сотрудников, покупает материалы у снабженцев и осуществляет выплату пособий. Бóльшую часть функций выполняемых правительством можно осуществлять при помощи технологии электронной коммерции. Например, граждане могут скачивать с правительственного Web-сайта бланки налоговых деклараций, формы заявлений на получение паспорта и другие документы. Государственные органы получают от своих граждан разнообразные оплаты и налоги и могут использовать Интернет для того чтобы сделать этот процесс более эффективным. Использование правительством и правительственными органами Интернет технологий для выполнения своих функций часто называют *электронным правительством* (e-government).

В США, правительственное агенство под наименованием Служба Финансового Управления (Financial Management Service – FMS) ответственна за сбор триллионов долларов в виде налогов, лицензий и других платежей. FMS также выплачивает триллионы долларов в виде социальной помощи соответствующим категориям граждан, а также в виде возвращаемых налогов и других выплат. Агенство поддерживает Web-сайт Pay.gov, позволяющий выполнять бóльшую часть из отмеченных платежей в онлайне.

Правительства многих стран с развитой экономикой используют концепцию электронного правительства для снижения административных затрат и более эффективного и быстрого обслуживания своих граждан. С этой целью они создают Web-сайты, которым передают часть своих функций. Примером эффективно работающего Web-сайта электронного правительства небольшого государства может служить сингапурский сайт Singapore Government Online.

Правительство штата Калифорния создало единый Web-сайт CA.GOV, обеспечивающий гражданам и коммерческим компаниям доступ к информации и широкому спектру правительственных услуг на уровне штата Калифорния. При помощи этого сайта граждане могут получать множества услуг – от обновления водительских прав до резервирования площадки для палаточного лагеря. Для коммерческих компаний сайт предлагает полные тексты законов, регулирующих коммерческую деятельность в штате Калифорния и информацию о том, как вести коммерческую деятельность с правительственными агенствами штата. Сайт не только снабжает коммерческие компании текстами законов, но позволяет, в онлайне, решать множество проблем, требующих участия правительственных агенств.

Идея электронного правительства непрерывно развивается и эволюционирует. Сайты, реализующие функции электронного правительства, оказывают услуги федерального уровня, регионального уровня, уровня отдельных городов и, даже, небольших поселений.

1.1.6. Сетевая форма экономической организации: сеть поставок

Ранее были рассмотрены три формы экономической организации: рыночная, иерархическая и сетевая (см. подраздел 1.5 в конспекте лекций по дисциплине «Электронная коммерция»). При изучении того, каким образом в современных компаниях реализуются такие первоочередные деятельности как приобретение материалов и логистика, а также все поддерживающие деятельности становится очевидным, что имеет место тенденция сдвига экономической организации от иерархической формы к сетевой. Традиционная модель приобретения материалов предполагает, что одна иерархически структурированная компания, обсуждает условия поставки материалов с несколькими конкурирующими поставщиками, каждый из которых также представляет собой иерархически структурированную фирму. Для сетевой формы экономической организации более типичным является такая модель, которая предполагает, что Отдел снабжения компании обсуждает со своими поставщиками условия формирования стратегического альянса (см. подраздел 1.5.4 в конспекте лекций по дисциплине «Электронная коммерция»). Например, некоторая компания может вступить со своим поставщиком в стратегический альянс, и поставить своей целью снижение общей стоимости конечного продукта. Технологию, позволяющую снизить общую стоимость продукта, может разрабатывать третья фирма, используя результаты исследований, проведенных четвёртой фирмой.

Ранее было отмечено, что компании часто используют аутсорсинг и передают сторонним фирмам некоторые из своих поддерживающих деятельностей. Такой аутсорсинг, также, является примером того, как компании движутся к сетевой форме экономической организации. Рассмотрим, в качестве примера, компанию, которая передала одной сторонней фирме деятельность по составлению платёжных ведомостей, другой – деятельность по администрированию выплат пособий и вознаграждений, а третьей – работу по хранению и манипулированию всеми документами. Фирма, занимающаяся хранением и манипулированием документами, хранит документы, получаемые как от фирмы, составляющей платёжные ведомости, так и от фирмы, занимающейся пособиями и вознаграждениями. Фирма, специализирующаяся на составлении платёжных ведомостей может составлять платёжные ведомости также и для фирмы, специализирующейся на администрировании пособиями и вознаграждениями. Четвёртая фирма может обслуживать остальные три и заниматься онлайновым резервным копированием их файлов. Фирмы, рассмотренные в примере, связаны между собой в сетевую структуру, однако они оперируют в своих рыночных сегментах и могут образовывать аналогичные сетевые структуры с другими партнерами.

Исследователи, изучающие взаимодействие между компаниями в условиях сетевой формы экономической организации, используют термин *«сеть поставок»* (supply web) вместо термина «цепь поставок», поскольку, в этом случае, индустриальная ценностная цепь не состоит из единственной цепи компаний, связанных поставками материалов, а представляет собой сетевую конфигурацию, образованную стратегическими альянсами и/или договорами аутсорсинга.

Технология электронной коммерции является одной из основных причин трансформации иерархической формы экономической организации в сетевую. Она позволяет существовать и эффективно работать небольшим высокоспециализированным компаниям. Сеть небольших и высокоспециализированных фирм легко адаптируется к новым условиям, поскольку может реагировать на изменения в экономическом окружении гораздо быстрее, чем крупная иерархически структурированная компания.

1.2. Электронный обмен данными между удалёнными компьютерами (EDI)

Ранее было отмечено, что технология, называемая *электронный обмен данными между удаленными компьютерами*, или сокращенно EDI (electronic data interchange), является одной из предтеч технологии электронной коммерции (см. подраздел 1.2.1 в конспекте лекций по дисциплине «Электронная коммерция»). Напомним, что EDI означает обмен деловой информацией в общепринятой стандартной форме непосредственно между компьютерами двух компаний-партнёров. Компании, осуществляющие обмен деловой информацией в общепринятой стандартной форме, называют EDI-совместимыми. Бóльшая часть данных, которыми обмениваются EDI-совместимые компании, представляет собой информацию, необходимую для выполнения транзакций, однако эти данные могут включать и запросы, имеющие отношение к транзакции. Данные, необходимые для выполнения транзакций это электронные версии таких документов как заказ, счёт-фактура, запрос котировки, транспортная накладная и т.д. Эти данные составляют более 75% от всей информации, циркулирующей между EDI-совместимыми компаниями. EDI можно рассматривать как первую форму электронной коммерции, которая широко использовалась компаниями в промышленно развитых странах ещё за 20 лет до того как появился сам термин «электронная коммерция».

Понимание технологии EDI важно, поскольку большинство систем электронной коммерции типа «бизнес-бизнес» базируются либо на EDI, либо на технологиях, унаследованных от EDI. Это понимание важно ещё и потому, что EDI сегодня является единственной и общепринятой технологией, используемой для осуществления онлайновых транзакций в системах типа «бизнес-бизнес».

1.2.1. Ранние системы обмена деловой информацией

Появление больших коммерческих компаний в конце 19-го и в начале 20-го века породило потребность в разработке системы информационного сопровождения бизнес транзакций, осуществляемых между компаниями. В 1950-е годы компании начали использовать компьютеры для сохранения данных о внутренних операциях. Однако, обмен информацией, необходимой для выполнения транзакций с внешними партнерами, осуществлялся в виде бумажных документов (заказ, счёт-фактура, транспортная накладная, чек, извещение о перечислении средств и т.п.) поскольку компьютеры компаний-партнеров не были соединены и не могли обмениваться информацией непосредственно. Создание этих бумажных документов (вручную или при помощи компьютерных устройств печати), отправка их по почте, а затем ввод в компьютер документов, полученных в ответ, выполнялись медленно, неэффективно, и ненадежно. К 1960-м годам компании, с большим объемом взаимных транзакций, начали обмениваться информацией о транзакциях, нанесенной на компьютерные носители данных в виде колод перфорированных бумажных карт или катушек с магнитными лентами. В период с 1960-х по 1970-е годы телекоммуникационные технологии передачи цифровых данных по проводам позволили компаниям пе-

редавать большую часть информации о транзакциях в электронной форме, используя телефонные линии связи.

Хотя передача информации о транзакциях по телефонным линиям, связывающим компьютеры компаний-партнеров, существенно сократила время выполнения транзакций и уменьшила количество ошибок, это не являлось окончательным решением проблемы создания технологии EDI, поскольку каждая из компаний-партнеров должна была разрабатывать собственное программное обеспечение для преобразования и обработки полученных данных. Только крупные компании могли позволить себе такие инвестиции. Поэтому небольшие компании не могли участвовать в электронных транзакциях с крупными компаниями.

В 1968 году большое количество компаний, занимающихся фрахтом и транспортировкой грузов в США, объединились для создания безбумажной системы обмена информацией о транзакциях в области грузоперевозок. В результате был создан стандартизованный информационный набор, который включал все элементы данных, которые перевозчики обычно включают в транспортную накладную, счёт-фактуру, путевой лист и другие документы. Вместо того, чтобы печатать бумажные формы, перевозчики могли представлять всю информацию о перевозке в виде стандартизованного компьютерного файла и пересылать его на компьютер любой компании-партнера, которая приняла общий стандарт. Компания-партнер, получив данные в стандартизованной форме, передавала их в свою собственную информационную систему. Стандартизация данных позволила участвовать в электронных транзакциях не только крупным, но и небольшим транспортным компаниям.

Хотя отмеченный стандарт обмена данными в области грузоперевозок был полезным, его преимуществами и выгодами могла пользоваться только ограниченная группа участников в одной специфической индустрии. Однако, большинство компаний, осуществляющих транзакции, работают в разных индустриях. Например, производители в области машиностроения покупают материалы у сталелитейных предприятий, производителей и продавцов краски и электрооборудования и т.п. Практически все компании должны приобретать материалы для своих офисов, а также услуги транспортных компаний. Поэтому полное решение проблемы электронных транзакций и создание технологии EDI требовало разработки таких стандартов, которыми могли бы пользоваться компании всех индустрий.

1.2.2. Появление более широкого стандарта: рождение EDI

В США координацией деятельности по разработке, внедрению и поддержки стандартов занимается *Американский национальный институт стандартов* (American National Standards Institute – ANSI). Институт ANSI не занимается разработкой стандартов, но предоставляет комитетам полномочия по их созданию. В 1979 году ANSI создал новый комитет для разработки унифицированных стандартов EDI. Этот комитет был назван *Аккредитованный комитет стандартов* (Accredited Standards Committee X12 – ASC X12). Комитет ASC X12 и его подкомитеты включал профессионалов в области информационных технологий, представлявших сотни коммерческих компаний, деятельность которых координировалась *Ассоциацией по стандартам обмена данными* (Data Interchange Standards Association – DISA). В настоящее время стандарт ASC X12 включает спецификации для нескольких сотен транзакционных наборов для конкретных случаев обмена деловой информацией.

Стандарт ASC X12 был быстро принят основными компаниями в США, но компании в других странах продолжали использовать свои собственные национальные стандарты. В середине 1980-х годов Комиссия по Экономике Организации Объединенных Наций пригласила североамериканских и европейских экспертов для разработки общего EDI стандарта с учетом успешного опыта применения стандарта ASC X12. В 1987 году Организация Объединенных Наций опубликовала свой первый стандарт под наименованием *EDI для администрирования, коммерции и транспорта* (EDI for Administration, Commerce, and Transport – EDIFACT, или UN/EDIFACT). Начиная с 2000 года группы

специалистов из DISA и UN/EDIFACT несколько раз предпринимали попытки разработать единый и общий стандарт, однако эти попытки не увенчались успехом. Сегодня, в электронной коммерции типа «бизнес-бизнес» используются оба стандарта. Поэтому компании, занимающиеся международной электронной коммерцией, вынуждены, либо использовать универсальное программное обеспечение, базирующееся на обоих стандартах, либо использовать дополнительные программы для конвертации данных из одного стандарта в другой. В таблице, на рис. 1.3, приведены несколько, наиболее часто используемых транзакционных наборов и их идентификаторы для ASC X12 и UN/EDIFACT стандартов.

Описание транзакционных наборов	**Идентификаторы**	
	ASC X12	**UN/EDIFACT**
Транзакционные наборы при оформлении заказа		
Заказ на приобретение	850	ORDERS
Подтверждение о получении заказа	855	ORDRSP
Изменение заказа	860	ORDCHG
Запрос о цене	840	REQOTE
Ответ на запрос о цене	843	QUOTES
Транзакционные наборы при поставке		
Уведомление об отгрузке	856	DESADV
Транспортная накладная	858	IFTMCS
Получение консультации	861	RECADV
Продажа и платёжные транзакционные наборы		
Счёт-фактура	810	INVOIC
Фрахтовый счёт	859	IFTFCC
Платёжное поручение (извещение о перечислении средств)	820	REMADV

Рис. 1.3. Часто используемые транзакционные наборы EDI

1.2.3. Как работает EDI

Хотя базовая идея, лежащая в основе EDI, проста и понятна, внедрение этой технологии может быть сложным даже в весьма простых ситуациях. В качестве примера рассмотрим ситуацию, когда некоторой компании требуется замена одного из металлорежущих станков. Рассмотрим шаги, которые необходимо выполнить для приобретения станка, при использовании бумажных документов и затем опишем, этот же процесс при использовании EDI. В обоих случаях предположим, что поставщик осуществляет доставку станка своим собственным транспортом, а не пользуется услугами сторонней транспортной компании.

Процесс приобретения оборудования на основе бумажных документов

В описанном, ниже, примере покупатель и продавец не используют технологию EDI и, следовательно, каждый шаг процесса сопровождается созданием бумажного документа, который передаётся в отдел, выполняющий последующий шаг. Перемещение документов между подразделениями покупателя и продавца осуществляется при помощи факса, обычной почты или курьера. На рис. 1.4 показаны информационные потоки, которые образуются в процессе приобретения станка при использовании бумажных документов.

Как только менеджер производственного подразделения компании принимает решение о замене металлорежущего станка, начинается следующий процесс.

1. Менеджер производственного подразделения заполняет форму *заявки на закупку* (purchase requisition) и передает ее в *отдел закупок* (purchasing department). Заявка описывает станок, который необходимо приобрести.

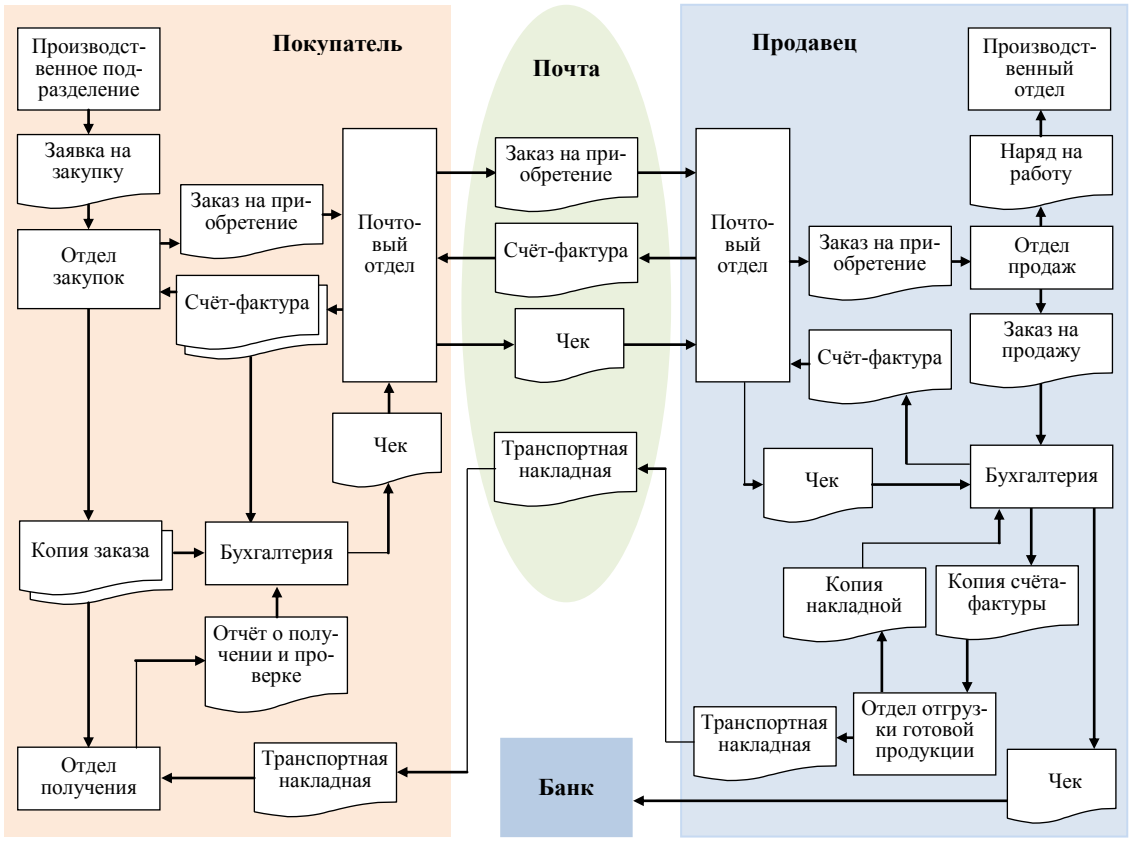

Рис. 1.4. Информационные потоки при приобретении оборудования с использованием бумажных документов

2. Отдел закупок контактирует с продавцами для обсуждения цены и сроков поставки. После того как отдел закупок выбрал продавца, он готовит *заказ на приобретение* (purchase order) и передаёт его в *почтовый отдел* (mail room).
3. Отдел закупок направляет один экземпляр заказа в *отдел получения* (receiving department) для того, чтобы этот отдел мог включить получение станка в свой план по получению оборудования, и ещё один экземпляр заказа в *бухгалтерию* (accounting department) для того чтобы известить бухгалтерию о финансовых затратах, связанных с заказом.
4. Почтовый отдел покупателя отсылает заказ, полученный из отдела закупок, выбранному продавцу по почте или курьером.
5. Почтовый отдел продавца получает заказ и направляет его в *отдел продаж* (sales department).
6. Отдел продаж продавца готовит *заказ на продажу* (sales order) и направляет его в бухгалтерию, а также *наряд на работу* (work order) и направляет его в производственный отдел. Наряд на работу содержит спецификации станка и уполномочивает производственный отдел приступить к работе.
7. После того как завершается изготовление станка, производственный отдел уведомляет об этом бухгалтерию и отправляет станок на отгрузку.
8. Бухгалтерия направляет оригинал счёта-фактуры в почтовый отдел и копию счёта-фактуры в отдел *отгрузки готовой продукции* (shipping department).
9. Почтовый отдел продавца отсылает счёт-фактуру покупателю по почте или курьером.
10. Отдел отгрузки готовой продукции продавца использует свою копию счёта-фактуры для создания *транспортной накладной* (bill of lading) и отсылает её покупателю вместе со станком.

11. Почтовый отдел покупателя получает счёт-фактуру примерно в то же время, когда в отдел получения прибывает станок вместе с транспортной накладной.
12. Почтовый отдел покупателя направляет копию счёта-фактуры отделу закупок, информирующую отдел закупок о том, что станок получен, а оригинал счёта-фактуры в бухгалтерию.
13. Отдел получения покупателя проверяет станок на соответствие исходному заказу на приобретение и транспортной накладной. Если станок находится в хорошем состоянии и удовлетворяет спецификациям, как заказа, так и транспортной накладной, то отдел заполняет *отчёт о получении и проверке груза* (receiving report) и доставляет станок в производственное подразделение.
14. Отдел получения направляет заполненный отчет о получении и проверке станка в бухгалтерию.
15. Бухгалтерия сравнивает данные заказа на приобретение, отчёта о получении и оригинала счёта-фактуры. Если данные совпадают, то бухгалтерия готовит чек на оплату и направляет его в почтовый отдел.
16. Почтовый отдел покупателя отсылает чек продавцу по почте или курьером.
17. Почтовый отдел продавца получает чек и направляет его в бухгалтерию.
18. Бухгалтерия продавца сравнивает данные полученного чека с данными счёта-фактуры, транспортной накладной и заказа на продажу. Если все данные совпадают, бухгалтерия направляет чек в свой банк и регистрирует получение платежа.

Процесс приобретения оборудования на основе EDI

Информационные потоки при приобретении станка с использованием EDI технологии, изображены на рис. 1.5.

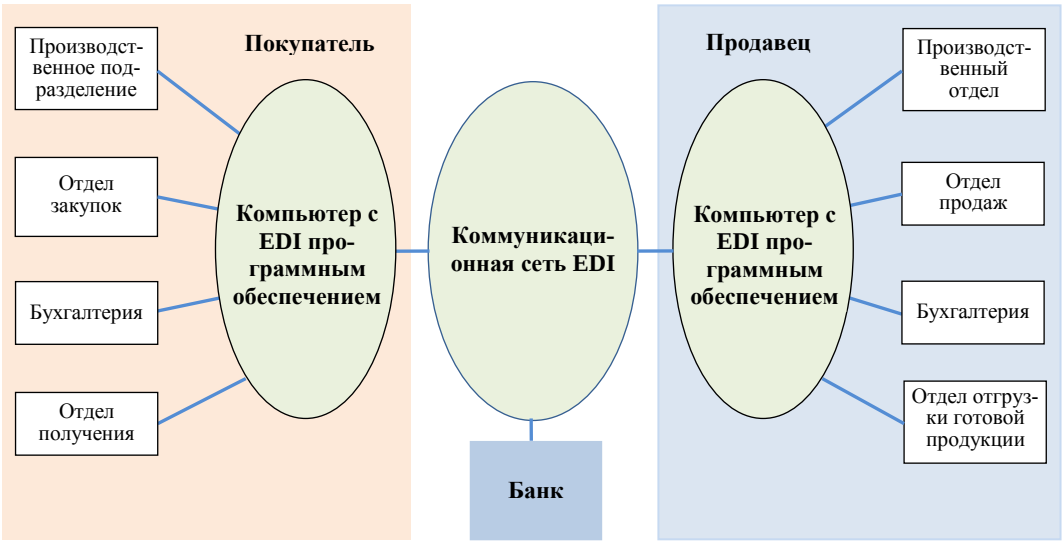

Рис. 1.5. Информационные потоки при приобретении оборудования с использованием технологии EDI. Линии обозначают электронные каналы коммуникации

Использование технологии EDI приводит к тому, что почтовые отделы, как на стороне покупателя, так и на стороне продавца, ликвидируются. Их функции выполняет коммуникационная сеть, связывающая компьютеры компаний, а бумажный документооборот заменяется обменом данных в электронной форме между отделами компаний и работой программного обеспечения EDI. Если компания использует EDI, а менеджер производственного подразделения принимает решение о замене металлорежущего станка, начинается следующий процесс.

1. Менеджер производственного подразделения отсылает электронную заявку в отдел закупок. Заявка описывает станок, который необходимо приобрести.
2. Отдел закупок контактирует с продавцами станков по телефону, при помощи электронной почты или непосредственно через Web-сайты продавцов для обсуждения цены и сроков поставки. После выбора продавца, отдел закупок посылает сообщение, которое конвертируется в транзакционный набор 850 «заказ на приобретение» (см. рис. 1.3), затем через коммуникационную сеть передаётся в компьютер продавца и направляется в его отдел продаж. Далее заказ автоматически отсылается в компьютерную систему производственного отдела и в систему автоматизированного учёта бухгалтерии. Каждая из отмеченных компьютерных систем дополняет данные заказа информацией, необходимой для выполнения функций соответствующего подразделения. Например, компьютерная система производственного отдела дополняет заказ спецификациями, необходимыми для начала работ по производству станка.
3. Отдел закупок покупателя отсылает ещё два сообщения: (1) в отдел получения (для того, чтобы отдел мог включить получение станка в план по получению оборудования) и (2) в бухгалтерию с информацией о согласованной стоимости станка.
4. После того как завершается изготовление станка, производственный отдел продавца уведомляет об этом бухгалтерию продавца и отправляет станок в отдел отгрузки готовой продукции.
5. Отдел отгрузки готовой продукции отсылает электронные сообщения в свою бухгалтерию и покупателю, информирующие о том, что станок готов к отгрузке. Сообщение, которое отправляется покупателю, предварительно преобразуется в транзакционный набор 856 «уведомление об отгрузке» (см. рис. 1.3).
6. Бухгалтерия продавца отсылает бухгалтерии покупателя и его отделу получения электронную счёт-фактуру в транзакционный набор 810 «счёт-фактура» (см. рис. 1.3).
7. Когда отдел получения покупателя получает станок, он проверяет его на соответствие информации, содержащейся в счёте-фактуре. Если станок находится в хорошем состоянии и удовлетворяет спецификациям покупателя, то отдел получения отсылает сообщение бухгалтерии, подтверждающее, что станок получен и соответствует спецификациям. Затем станок доставляется в производственное подразделение покупателя.
8. Бухгалтерия покупателя сравнивает данные заказа на приобретение и данные полученного счёта-фактуры. Если данные совпадают, то бухгалтерия покупателя отсылает своему банку поручение перевести соответствующие денежные средства на банковский счёт продавца. Для передачи поручения банку также используется коммуникационная сеть EDI.

Сравнение и анализ процессов приобретения оборудования с использованием бумажных документов (рис. 1.4) и технологии EDI (рис. 1.5) позволяет отметить, что в обоих случаях структурные подразделения обмениваются информацией, имеющей один и тот же характер. Однако технология EDI не только устраняет бумажные документы, но упрощает и существенно ускоряет обмен информацией как между отделами внутри коммерческих компаний, так и между компаниями. Два ключевых элемента драматически изменяют весь процесс приобретения оборудования, в случае EDI: (1) коммуникационная сеть для обмена транзакционными наборами в стандартной форме; (2) компьютеры с EDI программным обеспечением, как на стороне покупателя, так и на стороне продавца. Одной из задач программного обеспечения этих компьютеров является преобразование сообщений из формата, принятого внутри компаний в стандартные транзакционные наборы EDI.

1.2.4. Сети с добавленной стоимостью (VAN)

Компании партнёры, которые хотят использовать преимущества технологии EDI, могут внедрять эту технологию используя один из двух подходов: (1) организация EDI на основе прямой связи между компаниями и (2) организация EDI на основе непрямой связи между компаниями.

Подход на основе прямой связи предполагает, что каждая из компаний партнёров оперирует своим собственным компьютером с EDI программным обеспечением, как это изображено на рис. 1.5, а компьютеры компаний связаны друг с другом при помощи арендованных/выделенных телекоммуникационных линий связи. Отметим, что компания, использующая EDI на основе прямой связи должна установить множество выделенных линий связи со всеми своими торговыми партнерами. Поскольку выделенные линии связи стоят дорого, то, сегодня, только небольшое количество крупных компаний используют EDI на основе прямой связи. Рис. 1.6 иллюстрирует организацию EDI на основе прямой связи между компаниями.

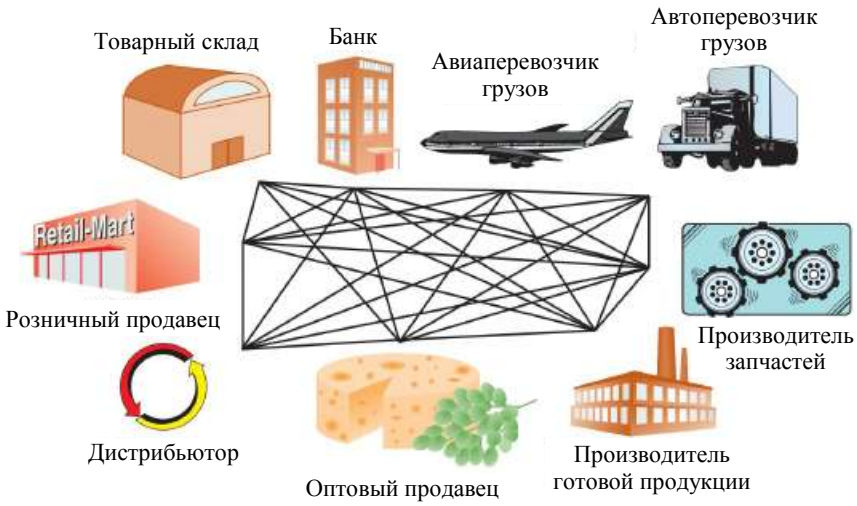

Рис. 1.6. Организация EDI на основе прямой связи между компаниями

Вместо того, чтобы устанавливать прямую связь между своими компьютерами, EDI партнёры могут пользоваться услугами посреднической компании, называемой сетью с добавленной стоимостью (см. подраздел 1.2.1 в конспекте лекций по дисциплине «Электронная коммерция»). *Сеть с добавленной стоимостью* (value-added network – VAN) предоставляет коммуникационное оборудование, программное обеспечение и знания своих специалистов, необходимые для осуществления EDI-транзакций. Для того, чтобы пользоваться услугами VAN, компании партнёры должны инсталлировать специальное программное обеспечение, которое, обычно, предоставляется VAN в рамках договора о предоставлении услуг, а также установить с VAN выделенную телекоммуникационную линию связи.

Для отсылки EDI сообщения своему торговому партнёру, клиент VAN связывается с VAN, используя выделенную линию связи, а, затем, пересылает EDI форматированное сообщение на компьютер VAN. Компьютер VAN регистрирует сообщение и помещает его в почтовый ящик торгового партнёра, которому оно адресовано. Торговый партнёр, которому адресовано сообщение, связывается с VAN и извлекает сообщение из своего почтового ящика. Такой подход организации EDI носит наименование EDI на основе непрямой связи между компаниями, поскольку торговые партнеры осуществляют EDI-транзакции не непосредственно между своими компьютерами, а через почтовые ящики VAN. Рис. 1.7 иллюстрирует EDI на основе непрямой связи.

Наиболее известными компаниями, предоставляющими услуги VAN, являются CovalentWorks, Kleinschmidt Inc. и Promethean Software Services.

Рис. 1.7. Организация EDI на основе непрямой связи между компаниями

Сети VAN обладают следующими достоинствами.

1. Клиенты VAN должны использовать только одну линию связи с VAN, а не множество линий связи с каждым из своих торговых партнёров.
2. VAN может обеспечивает взаимную трансляцию транзакционных наборов, представленных в различных стандартах (например, VAN может осуществлять трансляцию транзакционного набора, представленного в стандарте ASC X12 в транзакционный набор в стандарте UN/EDIFACT).
3. VAN может осуществлять проверку транзакции на соответствие конкретному EDI формату.
4. VAN осуществляет регистрацию всех транзакций в контрольном журнале (audit log). Контрольный журнал является независимым источником информации о транзакциях при разрешении споров между торговыми партнёрами.

Поскольку EDI транзакции представляют собой деловые контракты и, часто, имеют значительное денежное измерение, то наличие независимого контрольного журнала обеспечивает VAN свойство «*неотказуемости*» (non-repudiation) от авторства. Неотказуемость (невозможность отказа) от авторства означает возможность доказать, что конкретная транзакция между партнерами действительно имела место. Невозможность отказа препятствует кому либо из торговых партнеров отрицать выполнение какой либо транзакции.

В прошлом все VAN обладали одним серьезным недостатком, заключающемся в том, что за услуги VAN компаниям приходилось платить высокую стоимость. Компании платили разовый регистрационный взнос и оплачивали каждую транзакцию (в размере от нескольких центов до одного доллара США). Таким образом, единовременные расходы компании на внедрение EDI на основе VAN, включающие стоимость оборудования, программного обеспечения и регистрационный взнос, обычно, превышали 20 тысяч американских долларов.

Сегодня стоимость услуг VAN значительно меньше, поскольку разработана технология позволяющая, для коммуникации клиентов с VAN, использовать Интернет, а не выделенных линий связи. Сегодня единовременные расходы компании на услуги VAN составляют менее 5 тысяч долларов, а ежемесячная оплата трафика транзакций стоит менее 100 долларов. Небольшие компании обнаружили, что они в состоянии использовать EDI на основе VAN и, таким образом, становиться торговыми партнёрами крупных про-

изводственно коммерческих компаний, которые требуют от своих поставщиков использование технологии EDI.

Технология EDI с использованием Интернет, в качестве коммуникационной сети, называется *Интернет EDI* или *Web EDI*. Иногда её также называют *открытый EDI* с учётом того, что сеть Интернет имеет открытую архитектуру (см. раздел 2.3 в конспекте лекций по дисциплине «Электронная коммерция»). Для реализации Интернет EDI чаще всего используется набор протоколов с аббревиатурой EDIINT (Electronic Data Interchange-Internet Integration). Иногда используется аббревиатура EDI-INT.

Для обеспечения безопасности, транзакционные наборы, передаваемые в рамках EDIINT, кодируются с использованием протокола Applicability Statement 2 (AS2) который базируется на протоколе HTTP. Некоторые компании используют протокол Applicability Statement 3 (AS3), обеспечивающий бóльшую безопасность. Достоинством обоих протоколов AS2 и AS3 является то, что они, для каждой транзакции, возвращают отправителю квитанцию, для обеспечения неотказуемости от авторства.

Компания Walmart, являющаяся крупнейшей в мире сетью розничной торговли, требует от всех своих поставщиков использовать EDIINT и протокол AS2.

1.3. Менеджмент цепи поставок с использованием Интернет технологий

Как было отмечено ранее, часть индустриальной ценностной цепи, которая предшествует некоторому стратегическому бизнес-блоку в индустриальной ценностной цепи, называется цепью поставок. Компании используют стратегические альянсы, кооперацию и долгосрочные контракты для установления отношений с фирмами, входящими в цепь поставок. Эти отношения могут быть весьма сложными и означать, что поставщики не только снабжают своих клиентов необходимыми материалами, но и помогают им улучшать характеристики продуктов и создавать новые продукты. Во многих случаях компания может уменьшить стоимость своего продукта путем установления тесных отношений с несколькими поставщиками вместо того, чтобы обсуждать поставки с большим количеством компаний каждый раз, когда необходимо приобретать материалы. Когда компания интегрирует свою деятельность по управлению поставками с деятельностью участников цепи поставок, то управление такой интеграцией называется *менеджмент цепи поставок* (supply chain management). Конечной целью менеджмента цепи поставок является достижение высокого качества и низкой стоимости выпускаемого продукта.

1.3.1. Создание ценности в цепи поставок

В последние годы компании всё более отчётливо понимают, что они могут уменьшить затраты и улучшить качество выпускаемого продукта путём более активного взаимодействия со своими поставщиками. Взаимодействуя с поставщиками, в рамках кооперативных и долгосрочных отношений, компания может обнаружить новый способ обеспечения своих клиентов более дешёвыми и качественными продуктами. Как правило, менеджмент цепи поставок приводит к тому, что между компаниями, вовлечёнными в этот менеджмент, устанавливаются отношения, создающие новую сетевую организационную форму.

Первоначально менеджмент цепи поставок был разработан как средство уменьшения общих расходов. Сегодня, менеджмент цепи поставок используется для создания дополнительной ценности, которую получает, в итоге, конечный потребитель.

Компании, осуществляющие менеджмент цепи поставок, работают над тем, чтобы установить долгосрочные отношения с небольшим количеством очень квалифицированных и дееспособных поставщиков. Эти поставщики, называемые *поставщиками первого уровня* (tier-one suppliers), в свою очередь, формируют долгосрочные отношения с большим количеством поставщиков, которые снабжают их компонентами и исходными материалами. Эти *поставщики второго уровня* (tier-two suppliers) управляют отношениями со следующим уровнем поставщиков, называемым *поставщики третьего уровня* (tier-three suppliers), которые снабжают поставщиков второго уровня необходимыми компонентами

и исходными материалами. Ключевым элементом отношений между поставщиками различных уровней является высокий уровень доверия. Долгосрочные отношения, устанавливаемые между участниками цепи поставок всех уровней, называются *снабженческие альянсы* (supply alliances). Уровень обмена доверительной информацией, который должен иметь место между участниками цепи поставок, может быть главным препятствием для создания снабженческого альянса. Фирмы, как правило, не согласны предавать огласке свою операционную информацию, считая, что огласка этой информации вредит их конкурентоспособности.

Позитивным примером может служить компания Dell Computer, которая смогла уменьшить расходы в цепи поставок путём передачи информации о заказах своим поставщикам. Как только компания Dell получает заказ от клиента, она делает эту информацию доступной для поставщиков первого уровня, которые могут более точно планировать своё производство у учётом текущих производственных трендов компании Dell. Например, поставщики жёстких дисков могут немедленно изменить свои производственные планы, когда они обнаруживают, что клиенты компании Dell имеют тенденцию заказывать компьютеры с жёсткими дисками с бóльшим объёмом хранимых данных. Это предотвращает перепроизводство дисков с меньшим объёмом хранимых данных, что снижает затраты поставщика жёстких дисков за счёт потерь от непроданных дисков. В результате, снижаются затраты всей цепи поставок, поскольку поставщик жёстких дисков не должен увеличивать стоимость дисков, поставляемых компании Dell, для покрытия потерь от непроданных дисков.

В обмен на стабильность тесных и долгосрочных отношений, покупатели ожидают от поставщиков ежегодного уменьшения цен и улучшения качества от каждого звена цепи поставок. Тем не менее, все участники цепи поставок обмениваются информацией и работают друг с другом для того, чтобы создать добавленную стоимость. В идеале, координация деятельностей в цепи поставок должна создавать стоимость, достаточную для того, чтобы каждый уровень поставщиков мог получать выгоду от снижения расходов и более эффективных операций. На протяжении последних десятилетий менеджмент цепи поставок интенсивно развивается. Независимая и некоммерческая организация Supply Chain Council занимается созданием моделей и стандартов в области менеджмента цепи поставок.

Ключевым элементом координации деятельностей в цепи поставок является создание согласованной *производственной стратегии*, которая принимается всеми участниками цепи. Производственная стратегия является способом, позволяющим компании достичь конкурентного преимущества. Существуют две общепринятые производственные стратегии: (1) *стратегия эффективной обработки* (efficient processing) и (2) *стратегия гибкой реакции на рынок* (market-responsive flexibility). Стратегия эффективной обработки предполагает, что компания пытается производить продукты как можно быстрее и с наименьшими затратами, а стратегия гибкой реакции на рынок означает, что компания пытается производить продукты востребованные на изменяющемся рынке. Иными словами, некоторые компании рассматривают себя как эффективного производителя, а другие – как гибкого производителя. К сожалению, средства, которые необходимы для того чтобы компания была эффективным производителем, часто препятствуют ей гибко реагировать на потребности рынка. Например, производитель, придерживающийся стратегии эффективной обработки может инвестировать значительные средства в специализированное оборудование, позволяющее быстро и с небольшими затратами производить большое количество некоторой детали методом прессования. Эти инвестиции снижают затраты на производство конкретной детали, но затрудняют гибко реагировать на необходимость производства других деталей. Если при производстве продукта, которое требует гибкого реагирования на рыночные изменения, хотя бы одна из компаний в цепи поставок придерживается стратегии эффективной обработки, то это оказывает негативный эффект на всех остальных участников цепи поставок. Такая компания создает подобие «бутылочного горлышка» в цепи поставок, которое негативно сказывается на усилиях всех остальных компаний гибко реагировать на изменяющиеся потребности рынка. Чёткое информационное взаимодействие между участниками ценностной цепи позволяет компаниям ясно

представлять требования конечных потребителей и правильно выбирать ту или иную производственную стратегию.

Учёт информации, получаемой от партнёров по цепи поставок, и быстрая реакция на эту информацию является важным элементом успешного менеджмента цепи поставок. Интернет и Web технологии могут быть эффективным «ускорителем» информационного взаимодействия между партнёрами по цепи поставок. Эти технологии позволили компаниям впервые осуществлять детальный мониторинг и управление, как собственными внутренними процессами, так и процессами партнёров, а программное обеспечение, использующее доступ в Интернет, помогает всем участникам цепи поставок анализировать прошлую деятельность, осуществлять мониторинг текущей деятельности и прогнозировать когда и какое количество конкретных продуктов должно быть произведено. В списке, на рис. 1.8, перечислены преимущества использования Интернет технологий в менеджменте цепи поставок.

Поставщики могут:

- Обмениваться информацией об изменениях в требованиях заказчиков
- Быстро получать уведомление о конструктивных изменениях в продукте
- Более эффективно снабжать партнёров спецификациями и чертежами
- Увеличивать скорость и уменьшать стоимость обработки транзакций
- Уменьшать количество ошибок при вводе данных при подготовке транзакций
- Обмениваться информацией о количестве дефектных продуктов и типе дефектов

Рис. 1.8. Преимущества использования Интернет технологий в менеджменте цепи поставок

Единственным недостатком использования Интернет технологий в менеджменте цепи поставок являются дополнительные затраты, связанные с её внедрением и поддержкой. Однако, для большинства компаний преимущества, перечисленные на рис. 1.8, представляют значительно бóльшую ценность, чем стоимость внедрения и поддержки Интернет ориентированного менеджмента цепи поставок.

1.3.2. Увеличение эффективности и кооперации в цепи поставок

Результатом успешного использования Интернет и Web технологий в менеджменте цепи поставок является повышение эффективности функционирования всей цепи поставок, выражающееся в ускорении производственного процесса, уменьшении затрат и увеличении гибкости производства, которое легко реагирует на изменение требований конечного потребителя. Примерами могут служить компании Boeing и Dell.

Компания Boeing, являющаяся одним из крупнейших мировых производителей летательных аппаратов, должна постоянно решать сложную задачу соблюдения графика производства. Каждый самолёт состоит более чем из одного миллиона отдельных компонентов, и индивидуально конфигурируется в соответствии со спецификациями заказчика. Компоненты должны быть произведены и доставлены точно в соответствии с графиком производства, иначе производственный процесс остановится.

Используя EDI, а также Интернет технологии в менеджменте цепи поставок Boeing организовал работу с поставщиками таким образом, что производственный процесс получает необходимые компоненты в сроки заранее определенные графиком производства. Ещё до того, как новый самолёт начинает производиться, компания Boeing передаёт по-

ставщикам его инженерные спецификации и чертежи, используя защищённые каналы связи Интернет. В процессе производства компания продолжает информировать всех участников цепи поставок о завершении очередного производственного этапа и об изменениях в графике производства. Широкое использование EDI и Интернет технологий в менеджменте цепи поставок привело к тому, что компания Boeing сократила время производства одного самолёта с 36 месяцев до 10 месяцев.

Компания Dell Computer известна тем, что она позволяет индивидуальным покупателям, коммерческим компаниям и некоммерческим организациям самостоятельно конфигурировать и заказывать компьютеры, используя Web. Для того, чтобы удовлетворить разнообразные требования своих заказчиков, компания Dell использует Интернет и Web технологии в менеджменте цепи поставок. Поставщики первого уровня компании Dell получают доступ к защищённому Web-сайту, который информирует их о последних прогнозах, а также о планируемых изменениях в производстве, уровне дефектных продуктах и предъявленных гарантийных требованиях. В дополнение к этой информации Web-сайт предоставляет данные о том, кто является заказчиками компании и что они заказывают. Вся эта информация помогает поставщикам первого уровня лучше планировать свои производственные процессы. Обмен информацией осуществляется в обоих направлениях по всей цепи поставок компании Dell. Поставщики первого уровня обязаны снабжать Dell информацией об уровне своих дефектных продуктов и других проблемах. В результате все участники цепи поставок работают совместно над уменьшением складских запасов, улучшением качества и созданием дополнительной ценности для конечного потребителя. Улучшение координации между компанией Dell и её поставщиками привело к существенному сокращению складских запасов, необходимых для непрерывного производства. Компания перешла с трёхнедельного запаса компонентов на двухчасовый. В конечном счёте Dell хочет вообще отказаться от необходимости иметь складские запасы компонентов. Как было отмечено выше, успешный менеджмент цепи поставок требует высокого уровня доверия между партнёрами. Для увеличения уровня доверия и создания ощущения единого сообщества, компания Dell поддерживает открытый дискуссионный форум на котором все участники цепи поставок могут обмениваться своим опытом работы с Dell и с друг другом.

1.3.3. Технологии трекинга материалов

Трекингом материалов (material tracking) называется отслеживание процесса доставки материала заказчику в реальном масштабе времени. Трекинг материалов, в процессе их перемещении от одной компании к другой, и при их перемещении между подразделениями внутри одной и той же компании всегда являлся сложной задачей. В течение многих лет компании использовали оптические сканеры и *штрих-код* (bar code) для отслеживания перемещения материалов. Во многих отраслях широкое распространение получила интеграция EDI и использование штрих-кода. На рис 1.9 изображена типичная *транспортная этикетка* (shipping label) со штрих-кодом, которая используется в автомобильной промышленности США. Каждый отдельный штрих-код на транспортной этикетке, изображённой на рис. 1.9, является репрезентацией элемента EDI транзакционного набора номер 856 «уведомление об отгрузке» в стандарте ASC X12 (см. рис. 1.3). Транзакционный набор 856 включает следующие пять элементов: номер части (PART NO.); поставляемое количество (QUANTITY); номер заказа (PURCHASE ORDER #); серийный номер (SERIAL NO.) и номер упаковочного листа (PACKING LIST #).

Этикетка, снабжённая штрих-кодом, позволяет компании сканировать информацию о полученном материале и отслеживать его перемещение со склада материалов на производство. Компании могут использовать информацию, сканированную с этикетки, совместно с информацией, полученной от EDI системы, для учёта складских запасов и прогнозирования их потребности по всей цепи поставок.

Крупные онлайновые розничные продавцы, такие как Amazon.com и Target поддерживают, так называемые, *фулфилмент-центры* (fulfillment centers) из которых они отправляют продукты, заказанные покупателями в онлайне. В общем случае фулфил-

мент-центром называется аутсорсинговая компания, которая оказывает услуги онлайновым продавцам. Фулфилмент-центр хранит товары, получает заказы от онлайновых магазинов, формирует и упаковывает заказы, а затем передаёт их в службу доставки.

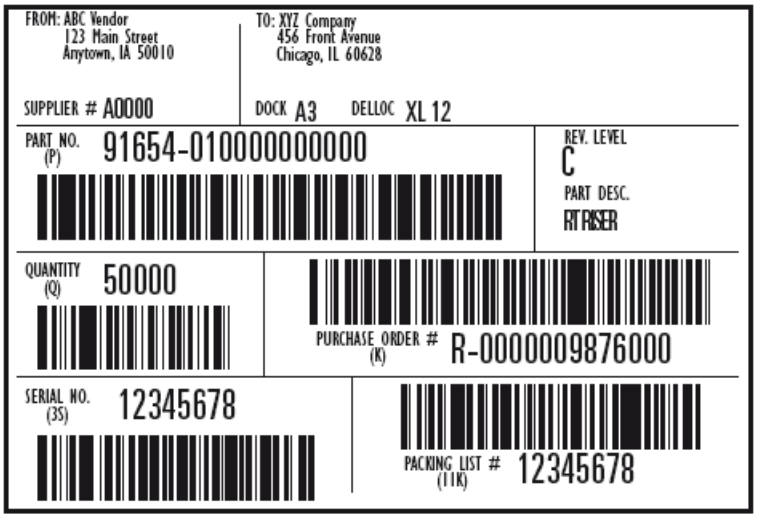

Рис. 1.9. Транспортная этикетка с представлением элементов EDI транзакционного набора 856 «уведомление об отгрузке» при помощи штрих-кода

Фулфилмент-центры компаний Amazon.com и Target эксплуатируют систему трекинга под наименованием *система позиционирования в режиме реального времени* (real-time location systems – RTLS), которая использует штрих-код для мониторинга перемещения материалов и гарантирования того, что они доставляются настолько быстро, насколько это возможно.

В системах электронной коммерции второго поколения компании начали применять новые технологии в своих Интернет системах трекинга материалов. Наиболее перспективной считается технология, основанная на использовании меток с *радиочастотной идентификацией* (radio frequency identification – RFID). Метка с радиочастотной идентификацией представляет собой крошечную интегральную микросхему с антенной, которая использует радиосигнал для передачи информации о продукте. Информация с RFID-метки может быть считана гораздо быстрее и с более высокой степенью точности чем штрих-код. Для того, чтобы сканировать штрих-код, он должен быть видим. RFID-метка может быть помещена где угодно на/в изделии и считывается даже закрытая упаковочным материалом, грязью или пластиковой тесьмой. Сканер, для считывания штрих-кода, должен быть помешен на расстоянии нескольких сантиметров от этикетки. Считыватели RFID-меток могут работать на расстоянии нескольких метров.

Технология учёта материалов на основе RFID-меток существует много лет, но до последнего времени сдерживающим фактором была необходимость снабжения микросхемы RFID индивидуальными источниками энергии. Важным этапом в развитии RFID технологии является разработка пассивных RFID-меток, которые имеют небольшой размер и невысокую стоимость. Пассивная RFID-метка не требует индивидуального источника энергии. Она получает радиосигнал от радиопередатчика считывателя и использует часть энергии этого сигнала для формирования ответного сигнала и передачи его на радиоприёмник считывателя. Ответный сигнал содержит информацию об изделии к которому прикреплена RFID-метка. RFID-метки бывают настолько малы, что их можно встроить в платежную карту или вшить в одежду.

В 2003 году компания Walmart провела проверку возможности использования RFID-меток для трекинга товаров, после чего разработала план, обязывающий своих поставщиков снабжать RFID-метками все товары, поставляемые Walmart. Согласно плану Walmart переход на RFID-метки должен был завершиться в течение трёх лет. Это позво-

лило бы компании улучшить управление поставками и уменьшить случаи *нехватки запасов* (stockouts). Нехваткой запасов называется ситуация, когда розничный продавец несёт убытки из-за того, что на его полках отсутствует товар, который хотел бы купить покупатель. Однако, многие поставщики Walmart посчитали, что стоимость RFID-меткок, считывающих устройств и компьютерных средств, необходимых для трекинга товаров на основе RFID технологии, слишком велика и убеждали Walmart увеличить сроки внедрения системы.

Аналитики, занимающиеся трекингом материалов на основе RFID-меток, отмечают, что полный переход на эту технологию, в большинстве индустрий, займет много лет. Средняя цена пассивных RFID-меток с медной антенной составляет около пяти центов, и всё ещё не позволяет компаниям, поставляющими большое количество товаров низкой стоимости, снабжать эти товары RFID-метками. По мере того, как стоимость RFID-меток будет снижаться, всё большее количество компаний будут использовать RFID технологию для трекинга материалов. Онлайновый журнал RFID Journal содержит большое количество материалов, посвященных RFID технологии. На рис. 1.10 изображена RFID-метка с алюминиевой антенной, выпускаемая предприятием Микрон (г. Зеленоград, Россия).

Рис. 1.10. Внешний вид современной RFID-метки. Для сравнения размеров приведено изображение стандартной SIM-карты

Метка имеет размер 20 на 12 мм. Алюминиевая антенна позволяет снизить её стоимость, по сравнению с медными аналогами, примерно в два раза.

1.3.4. Ориентация на конечного потребителя в менеджменте цепи поставок

Одна из основных целей менеджмента цепи поставок заключается в помощи каждой из компаний цепи поставок сфокусировать усилия на удовлетворении требований потребителя, являющегося последним звеном в цепи поставок. Иногда такой менеджмент называют менеджментом *с ориентацией на конечного потребителя* (ultimate consumer orientation). В прошлом, менеджмент цепи поставок с ориентацией на конечного потребителя, для компаний, работающих в индустриях с длинными цепями поставок, сталкивался с решением трудно решаемых проблем. Поэтому, вместо ориентации на удовлетворение требований конечного потребителя, компании направляли свои усилия на удовлетворение требований ближайшего последующего участника цепи поставок.

Компанией, которая первая использовала Интернет технологии для менеджмента цепи поставок с ориентацией на конечного потребителя, является французская компания Michelin. Компания Michelin обладает известным бренд именем и уважаемой репутацией в индустрии по производству автомобильных шин. В большинстве случаев потребитель, который менял шины на своем автомобиле, выбирал новые шины исходя из рекомендаций местного дилера шин. Компания Michelin тратила значительные средства для того чтобы воздействовать на конечного потребителя при помощи своих рекламных посланий. Целью этих рекламных посланий была поддержка бренд имени компании Michelin и информирование конечного потребителя в достоинствах продукции, производимой компанией. Однако, усилия по рекламированию преимуществ продукции компании и продви-

жению её имени могли быть потрачены напрасно, в том случае когда потребитель получал рекомендации от местного дилера шин.

В 1995 году компания Michelin запустила онлайновый сетевой проект под наименованием BIB NET. Хотя целью проекта была продажа бóльшего количества шин конечным потребителям, сеть BIB NET предназначалась дилерам компании, а не её конечным потребителям. Сеть BIB NET представляла собой сеть типа экстранет, которая позволяла дилерам автомобильных шин получать доступ к спецификациям шин и, информации о состоянии запасов компании Michelin при помощи простого интерфейса Web браузера. До появления сети BIB NET, дилеров, звонивших в компанию для получения информации о продуктах, часто просили подождать и оставаться на линии в течение некоторого времени. Дилер, который в этот момент разговаривал с клиентом, не был в состоянии долго ждать ответа по телефону. После того, как компания Michelin предоставила дилерам возможность получать нужную информацию непосредственно и мгновенно на сайте компании она сэкономила деньги (поддержка Web-сайта гораздо дешевле, чем ответы на тысячи телефонных звонков) и обеспечила своих дилеров лучшим сервисом. Дилеры, которые пользовались BIB NET, гораздо реже рекомендовали своим клиентам шины других компаний – конкурентов Michelin.

Поскольку Интернет технологии представляют собой инструменты, обеспечивающие высококачественную коммуникацию с низкой стоимостью, они являются идеальным средством для создания цепи поставок с высокой степенью координации её участников. Опросы менеджеров и исследования специалистов подтверждают, что большинство менеджеров в области информационных технологий и управления цепью поставок убеждены, что Интернет технологии помогают их компаниям улучшать отношения с поставщиками и менеджмент цепи поставок.

1.3.5. Создание и поддержка доверия в цепи поставок

Одной из важнейших тем, с которой сталкиваются компании, формирующие снабженческие альянсы является тема построения доверительных отношений. Необходимыми условиями построения доверительных отношений должны быть постоянная и непрекращающаяся коммуникация и обмен информацией между участниками цепи поставок. Поскольку Интернет и Web предоставляют отличные возможности для коммуникации и обмена информацией, они могут рассматриваться как новые средства для построения доверительных отношений. Большинство профессионалов в области снабжения годами строили доверительные отношения со своими партнёрами, поддерживая деловые отношения с одним и тем же поставщиком. Во многих индустриях поставщики направляли торговых представителей для регулярного общения с заказчиками, а также активно участвовали в торговых выставках и конференциях. Таким образом, поставщики укрепляли доверительные отношения с заказчиками предоставляя им возможности как можно чаще взаимодействовать со своим представителем.

Поставщики обнаружили, что Web предоставляет им возможность легко и с небольшими затратами находиться в постоянном контакте со своими заказчиками. Хотя многие заказчики регулярно встречаются с торговыми представителями, электронная почта и Web предоставляют им возможность практически мгновенной связи, как с торговым представителем, так и с другим персоналом поставщика. Предоставляя заказчику всеобъемлющую информацию по его первому требованию, поставщик формирует у него доверие к его способности вовремя поставлять необходимые материалы и обеспечивать заказчика теми персонализированными услугами, в которых он нуждается.

Исследователи в области менеджмента цепями поставок работают над новыми способами аккумулирования информации о деятельности поставщиков и передачи этой информации партнерам по цепи поставок. Новые способы мониторинга и обмена информацией могут помочь партнерам устанавливать доверительные отношения в течение короткого времени. Много проблем должны быть решены, прежде чем новые способы мониторинга и обмена информацией станут общепринятыми в сообществе поставщиков. К таким задачам относятся, например, объективность и достоверность измерения и оценки

деятельности поставщика. Отметим, что задача построения сетевых информационных ресурсов, которые снабжают данными партнеров по цепи поставок, была одной из самых трудных задач, которую решали разработчики системы электронной коммерции типа «бизнес-бизнес» второго поколения.

1.4. Электронные рынки и порталы

В конце 1990-х годов появилось большое количество Интернет ориентированных отраслевых центров, предлагающих *электронные рынки* и *аукционы* (auctions) на которых компании, работающие в некоторой индустрии, могли контактировать друг с другом и осуществлять транзакции в рамках электронной коммерции типа «бизнес-бизнес». Идея заключалась в том, что отраслевой центр создаёт и поддерживает Интернет портал, предлагающий услуги компаниям, работающим в конкретной отрасли экономики. Поскольку отраслевые центры были вертикально интегрированы (каждый центр предлагал услуги только в рамках одной индустрии) их стали называть *вертикальными порталами* (vertical portals или vortals). Таким образом, вертикальный портал представляет собой Web-сайт, обеспечивающий информационную поддержку электронной коммерции типа «бизнес-бизнес», для компаний, работающих в конкретной индустрии.

1.4.1. Независимые отраслевые рынки

Первыми вертикальными порталами были *торговые биржи* (trading exchanges), ориентированные на конкретную индустрию. Эти вертикальные порталы известны множеством различных наименований, отражающих различные характеристики их общей природы: (1) *отраслевые рынки* (industry marketplaces), поскольку они ориентированы на одну индустрию; (2) *независимые биржи* (independent exchanges), поскольку они не контролировались компаниями, являющимися общепризнанными лидерами в данной отрасли; (3) *публичные рынки* (public marketplaces), поскольку они были открыты для новых компаний, появившихся в отрасли. Однако, общепринятым наименованием является *независимые отраслевые рынки* (independent industry marketplaces). Один из первых независимых отраслевых рынков, ориентированный на химические продукты массового производства, был создан компанией Chemdex.com (более поздние наименования Ventro Corporation и NexPrise, Inc.) в 1997 году. Компания получила известность в период инвестиционного бума в истории развития электронной коммерции благодаря большой рыночной капитализацией, превышающей 7 миллиардов долларов. Сейчас эта компания не существует.

К середине 2000 годов появилось более 2200 независимых отраслевых рынков в различных индустриях, однако бóльшая их часть не приносила прибыли и, сегодня, продолжают работать не более 100. В каждой из индустрий только один или два отраслевых рынка смогли выжить, однако общее количество отраслей, в которых функционируют независимые рынки, возросло. В 2012 году компания Amazon.com запустила рынок, ориентированный на промышленные товары под наименованием AmazonSupply, который в 2015 году прекратил свое существование и был заменён рынком под наименованием Amazon Business.

Некоторые компании-пионеры, которые первыми создали независимые отраслевые рынки, а затем вынуждены были закрыть их в связи с убыточностью, такие, например, как компания Ventro Corporation, смогли построить успешный бизнес, продавая программное обеспечение и технологию, которые они разработали для оперирования независимым отраслевым рынком. Сегодня, все лидирующие продавцы программного обеспечения, такие как IBM, Microsoft и Oracle предлагают программные продукты для создания онлайновых рынков, ориентированных на электронную коммерцию типа «бизнес-бизнес». К середине 2000-х годов независимые отраслевые рынки, как доминирующие сайты в электронной коммерции типа «бизнес-бизнес», постепенно были заменены *моделями «бизнес-бизнес» рынков* (B2B marketplace models). В последующих подразделах описаны четыре такие модели «бизнес-бизнес» рынков: (1) *частные магазины* (private

stores); (2) *клиентские порталы* (customer portals); (3) *рынки частных компаний* (private company marketplaces) и (4) *отраслевые рынки, спонсируемые консорциумами* (industry consortia-sponsored marketplaces).

1.4.2. Частные магазины и клиентские порталы поставщиков

Крупные компании-поставщики, наблюдая за появлением независимых рынков, начали беспокоиться о том, что эти рынки получат контроль над транзакциями из их собственных цепей поставок, на построение которых компании потратили многие годы и значительные средства. Крупные компании, осуществляющие продажи большому количеству относительно небольших заказчиков, имеют рычаги влияния на заказчиков при обсуждении цены, качества и сроков поставки. Эти компании посчитали, что независимые отраслевые рынки могут ослабить это влияние.

Многие из крупных компаний-поставщиков уже инвестировали значительные средства в собственные Web-сайты, которые, как они были убеждены, удовлетворяют потребности заказчиков лучше, чем любые независимые отраслевые рынки. Например, компании Cisco и Dell, на своих Web-сайтах, предлагают *частные магазины* каждому из своих основных заказчиков. Вход в частный магазин защищён паролем. Частный магазин предлагает обсуждаемое снижение цен на продукты, которые заказчики согласились приобретать в некоторых минимальных количествах.

Web-сайты других компаний-поставщиков, таких, например, как Grainger оказывают дополнительные услуги своим заказчикам. Эти *клиентские порталы* предлагают своим заказчикам частные магазины наряду с дополнительными услугами: перекрёстные ссылки на номера деталей; руководства по использованию продуктов; информацию по безопасности и т.д., которые были бы бесполезно продублированы если бы компания участвовала в работе независимого отраслевого рынка.

1.4.3. Рынки частных компаний-покупателей

В свою очередь крупные компании-покупатели, приобретающие материалы у относительно небольших поставщиков, часто оказывают влияние на поставщиков при обсуждении условий закупки. Отделы снабжения (procurement departments) этих компаний инсталлировали *программное обеспечение электронного снабжения* (e-procurement software), которое позволяло им вести онлайновую снабженческую деятельность. Программное обеспечение электронного снабжения создано для автоматизации выполнения деятельностей, осуществляемых в процессе приобретении материалов или комплектующих (см. рис. 1.1).

Первые версии программного обеспечения электронного снабжения были разработаны для помощи в приобретении материалов, необходимых для технического обслуживания и ремонта (ТОиР). Сегодня это программное обеспечение включает и другие функции, характерные для независимых отраслевых рынков: обработка запросов о котировке, интегрированная поддержка при приобретении прямых материалов и др. Стоимость программное обеспечения электронного снабжения для крупных компаний значительна и составляет несколько миллионов американских долларов.

Компании, использующие программное обеспечение электронного снабжения, обычно требуют, чтобы их поставщики участвовали в тендере за право продавать комплектующие или материалы. Например, все поставщики офисного оборудования и материалов должны создать перечни цен, по которым они готовы продавать свои товары компании-покупателю. Компания-покупатель сравнивает цены всех участников тендера и выбирает поставщика. Выбранный поставщик предоставляет компании-покупателю необходимую информацию о поставляемом оборудовании и материалах, которая вносится в программное обеспечение электронного снабжения. Это позволяет компании-покупателю, в дальнейшем, работать с выбранным поставщиком в онлайне и заказывать офисное оборудование и материалы за оговоренную цену.

Когда появились независимые отраслевые рынки, крупные компании-покупатели материалов были не готовы отказаться от своего программного обеспечения электронного снабжения или адаптировать его к совместной работе с программным обеспечением отраслевых рынков. Эти компании использовали своё влияние на цепь поставок для того

чтобы заставить поставщиков вести бизнес на своих условиях, а не обсуждать условия поставки на независимых отраслевых рынках.

Однако, по мере того как программное обеспечение независимых отраслевых рынков становилось более совершенным, крупные компании-покупатели начали приобретать это программное обеспечение у таких компаний как Ventro Corporation, которые покинули бизнес в области независимых отраслевых рынков и продавали программное обеспечение и услуги тем компаниям, которые хотели использовать его для создания частных рынков. *Рынок частной компании* (private company marketplace) представляет собой электронный рынок, созданный крупной компанией-покупателем материалов и комплектующих, для обслуживания интересов этой компании.

1.4.4. Отраслевые рынки, спонсируемые консорциумами

Некоторые компании-покупатели имели относительно сильные позиции при обсуждении сделок в своей цепи поставок, но не имели достаточного влияния, чтобы заставить поставщиков работать с ними через свои частные рынки. Эти компании начали формировать консорциумы с целью спонсирования отраслевых рынков. *Отраслевой рынок, спонсируемый консорциумом* (industry consortia-sponsored marketplace) представляет собой рынок, сформированный несколькими крупными компаниями-покупателями в некоторой конкретной отрасли промышленности.

Рис. 1.11 обобщает характеристики пяти общих форм рынков, которые сегодня существуют в электронной коммерции типа «бизнес-бизнес».

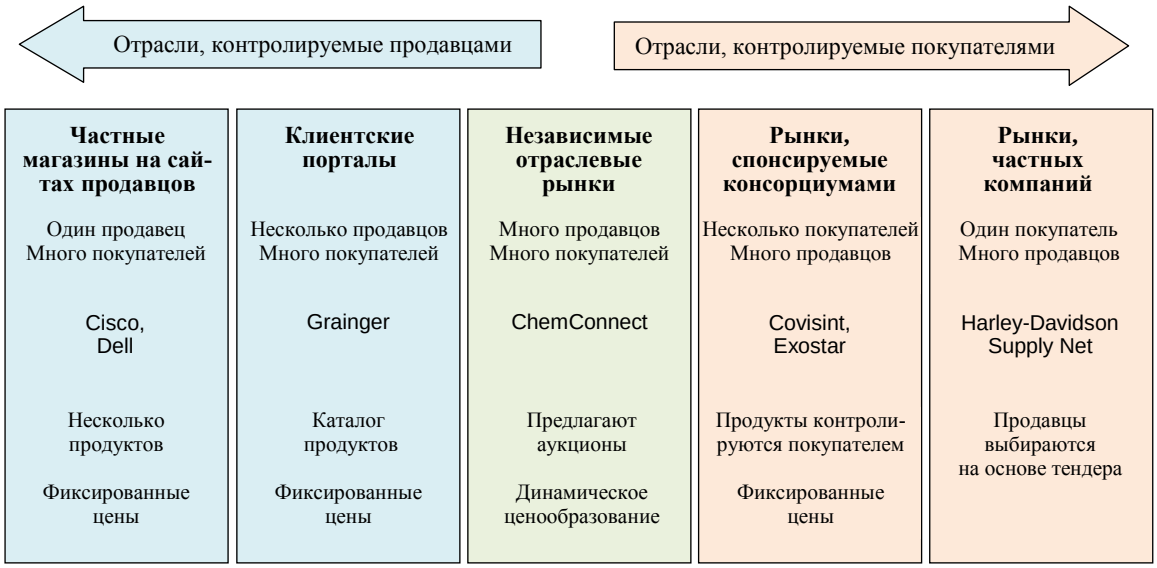

Рис. 1.11. Характеристики рынков электронной коммерции типа «бизнес-бизнес»

Хотя на рис. 1.11 представлены пять различных категорий рынков электронной коммерции типа «бизнес-бизнес», границы между этими категориями не всегда чёткие. Например, компания Dell, время от времени, продаёт на сайте своего частного магазина продукты сторонних компаний, что является признаком клиентского портала, а не частного магазина. По мере развития рынков электронной коммерции типа «бизнес-бизнес» маловероятно, что одна категория из пяти будет доминировать. Большинство экспертов, считают, что в ближайшее время будут существовать все пять категорий рынков.

ЗАДАНИЯ ДЛЯ СЕМИНАРСКИХ ЗАНЯТИЙ

1. Некоторые экономические и политические лидеры считают, что офшоринг опасен, поскольку он перемещает рабочие места из экономически развитых стран в менее развитые страны. Другие считают, что хотя офшоринг и приводит к уменьшению количества рабочих мест, этот эффект имеет краткосрочный характер, а в долгосрочном периоде все будут в выигрыше, поскольку образование в развивающихся странах новых индустрий и рынков, приводит к появлению в развитых странах новых рабочих мест для оказания высокоуровневых услуг и менеджмента. Изучите ресурсы, имеющиеся в Web, посвященные офшорингу и сделайте сообщение о достоинствах и недостатках офшоринга. Приведите два обоснованных аргумента «за» и два аргумента «против».

2. Используя информацию, размещённую в Web, сделайте обзор способов онлайнового приобретения непрямых материалов. Исследуйте достоинства и недостатки использования закупочных карт (p-cards) для расчетов при закупке материалов, необходимых для ТОиР (техническое обслуживание и ремонт). Рассмотрите возможность использования закупочных карт менеджерами крупных транспортных компаний. Отметьте основные причины, по которым крупные транспортные компании могут предпочесть использование закупочных карт при закупке материалов, необходимых для ТОиР.

3. Представьте себе, что Вы работаете стажером в отделе закупок некоторой компании, которая изготавливает электронные системы управления для производителей сборочных линий. Вы не очень много знаете о современном электронном оборудовании, однако получили задание идентифицировать компании, продающие осциллографы, с интерфейсом, позволяющим подключать их к настольному компьютеру. Используя Web-сайт компании ThomasNet, выберите, по крайней мере, три компании, которые предлагают такие осциллографы. Для каждой из выбранных компаний определите, продает ли она свои продукты при помощи Web-сайта, на страницах которого представлена подробная спецификация и стоимость продукта. В своем сообщении сделайте обзор компании ThomasNet и её сайта, и опишите, каким образом каждая из трёх компаний осуществляет онлайновую продажу осциллографов.

4. Возможность доступа в Web при помощи мобильных устройств, таких как смартфоны и планшетные компьютеры существенно улучшила рабочую среду для водителей-дальнобойщиков логистических компаний. Разыщите в Web, по крайней мере, три приложения для мобильных устройств, которые водители-дальнобойщики могут использовать для реализации двух или более функций из следующего списка: (1) получать информацию и маршруте следования; (2) контролировать расход топлива; (3) обнаруживать стояки или места отдыха; (4) учитывать случаи буксировки других транспортных средств; (5) обнаруживать станции взвешивания; (6) вести электронный журнал учёта. Сделайте обзор каждого из обнаруженных приложений. Опишите его функции и возможности, а также стоимость. Для каждого приложения укажите для каких мобильных устройств и операционных систем оно предназначено.

5. Большое количество организаций, занятых установлением стандартов в области снабжения, предлагают коммерческим компаниям стать их членами. Представьте себе, что Вы работаете в небольшой компании, которая производит компоненты, используемые в лабораторных и медицинских электронных приборах. Компания использует технологию EDI для обработки транзакций, как со своими поставщиками (приобретение), так и с покупателями конечной продукции (продажа). Компания исследует целесообразность реализации трекинга материалов на основе RFID-

меток. Вы получили задание собрать информацию о международной организации GS1, занимающейся установлением стандартов, используемых при организации цепей поставок. Изучите материалы, посвящённые этой организации и подготовьте сообщение в котором опишите цели организации и отметьте каким образом она может быть полезна компании в которой Вы работаете. Опишите, по крайней мере, ещё одну организацию, занимающуюся установлением стандартов, которая может быть полезна для реализации инициативы по внедрению трекинга на основе RFID-меток.

6. Компании, входящие в некоторую цепь поставок, могут работать совместно над тем, чтобы сократить затраты в цепи поставок. Во многих случаях эти сэкономленные средства распределяются неравномерно между компаниями, входящими в цепь поставок. Исследуйте этот вопрос. Используя материалы, размещённые в Web, идентифицируйте отрасль в которой средства, сэкономленные в цепи поставок, не распределяются равномерно. Объясните, почему некоторые участники цепи поставок, в выбранной Вами отрасли, получают бóльшую выгоду, чем другие из средств, сэкономленных в цепи поставок.

2. СОЦИАЛЬНЫЕ СЕТИ, МОБИЛЬНАЯ ЭЛЕКТРОННАЯ КОММЕРЦИЯ И ОНЛАЙНОВЫЕ АУКЦИОНЫ

Многие компании используют социальные сети и мобильную электронную коммерцию для взаимодействия со своими клиентами, потенциальными клиентами и другими заинтересованными лицами. Компания Starbucks, один из крупнейших международных розничный продавцов кофе, особенно искусна в использовании этих технологий.

Большинство компаний рассматривают социальные сети и мобильные технологии как ещё один канал для распространения рекламы. Активное участие в работе сайтов социальных сетей, таких как Facebook и Twitter, наряду с покупкой большого количества рекламы на этих сервисах, является подходом, которым пользуются многие компании, достигшие успеха в социальных сетях. Однако, компания Starbucks использует другую стратегию. Вместо того, чтобы наводнять социальные сети своими рекламными сообщениями, Starbucks осуществляет мониторинг взаимодействия между своими клиентами в социальных сетях, а затем использует собранную информацию как для улучшения продуктов и услуг, так и для выработки стратегий, позволяющих удерживать старых клиентов и привлекать новых.

Компания Starbucks рассматривает социальные сети как средство для расширения отношений, образовавшихся между бариста (специалист по приготовлению кофе) и клиентом в магазине, а также отношений между клиентами, которым нравится продукция компании Starbucks и атмосфера в её магазинах. Вместо коммуникации, направленной от компании к клиентам, Starbucks использует социальные сети для предоставления своим клиентам платформы, позволяющей обсуждать свои любимые продукты Starbucks.

Компания Starbucks также интегрирует мобильную технологию с опытом клиентов путём принятия оплаты за свои продукты при помощи мобильных устройств, а также путём предоставления клиентам мобильных приложений, позволяющих следить за доходами, получаемые от участия в программе «лояльный клиент».

2.1. От виртуальных сообществ к социальным сетям

2.1.1. Виртуальные сообщества

Виртуальное сообщество (virtual community), называемое также *Web сообщество* (Web community) или *онлайн сообщество* (online community) это место для общения людей, организаций и компаний, которое не существует в физическом мире. Первые виртуальные сообщества образовались ещё до того как Интернет стал доступен для всеобщего использования. *Электронные доски объявлений* (bulletin board system – BBS) позволяли пользователям компьютеров связываться друг с другом, используя коммутируемые телефонные линии связи, с целью обмена сообщениями на общем дискуссионном форуме, имеющим сходство с электронной версией физической доски объявлений. Электронные доски объявлений были предназначены для дискуссий на темы, специфические для конкретного географического региона. Хотя доступ к большей части электронных досок объявлений был бесплатным, некоторые доски объявлений требовалась оплату в виде ежемесячных членских взносов. Позже, коммерческие компании начали создавать электронные доски объявлений, с целью получения прибыли. Наиболее известной такой компанией является CompuServ. Прибыль формировалась за счёт членских взносов пользователей и средств, получаемых от рекламы.

Группа новостей сети Usenet (Usenet newsgroups) является другим примером ранних форм виртуальных сообществ (см. подраздел 2.1.2 в конспекте лекций по дисциплине «Электронная коммерция»). Сеть Usenet объединяла компьютеры, с целью хранения и обмена информацией, сгруппированной по конкретным темам, а группа новостей Usenet представляла собой виртуальное пространство для размещения сообщений по конкретным темам. Пользователями Usenet были, главным образом, представители академического сообщества, имеющие потребность участвовать в дискуссиях то этим конкретным темам.

В середине 1990-х годов виртуальные сообщества начали формировать, так называемые, *чат-форумы* или *чаты* (chat rooms), предназначенные для обмена информацией по различной тематике. По мере увеличения пропускной способности каналов связи с Интернет, доступных членам виртуальных сообществ, элементами сообщений в чатах стали фотографические и видео изображения.

Социальное взаимодействие представляло собой существенную часть активности членов виртуального сообщества, и многие социологи считают, что коммуникация и деятельность по формированию социальных отношений в онлайне аналогична той, которая имеет место в физическом мире.

2.1.2. Ранние Web сообщества

Одно из первых Web сообществ называлось WELL. Наименование представляет собой акроним словосочетания: «Whole Earth 'Lectronic Link». Web сообщество WELL начало функционировать в 1985 году и осуществляло свою деятельность в виде серии диалогов между авторами и читателями журнала Whole Earth Review. Обмен диалоговыми сообщениями производился при помощи электронной доски объявлений. В этих диалогах принимали участие многие из тех исследователей, кто участвовал в создании Интернет и Web, а также ряд известных писателей и артистов. В 1999 году онлайновый журнал Salon.com купил WELL и продолжил оперировать этим Web сообществом как платным сервисом, доступным при условии ежемесячной оплаты подписки.

После появления Web в середине 1990-х годов, её потенциал начал использоваться для создания виртуальных сообществ. В 1995 году Интернет-провайдеры американского города Беверли-Хиллз (штат Калифорния) создали сайт виртуального сообщества, который использовал две Web-камеры, направленные вдоль улиц Голливуда, содержал ссылки на развлекательные Web сайты и пространство для создания своих собственных страниц членами сообщества. Как оказалось, Web-камеры не очень привлекали внимание членов виртуального сообщество, их в большей степени интересовала возможность бесплатного создания собственных Web-страниц. По мере роста, сайт изменил своё наименование и стал называться GeoCities. Сайт получал прибыль путем продажи пространства для рекламных объявлений, которые размещались на Web-страницах членов сообщества, а также путем размещения «всплывающей» рекламы (pop-up ad), которая появлялась каждый раз, когда посетитель сайта открывал страницы членов сообщества (см. подраздел 4.4.3 в конспекте лекций по дисциплине «Электронная коммерция»). Сайт GeoCities быстро увеличивался в размерах и в 1999 году был куплен компанией Yahoo! за 5 миллиардов американских долларов. Компания Yahoo! продолжала политику получения прибыли путём размещения рекламы, но не заботилась о том, чтобы вовлекать членов сообщества в активное функционирование виртуального сообщества. В итоге сайт GeoCities был закрыт в 2009 году. В период с 1995 по 2001 годы другие компании, как например, Tripod.com и Theglobe.com оперировали похожими сайтами виртуальных сообществ, ориентированными на получение прибыли за счёт рекламной поддержки. Сайты включали бесплатные Web-страницы для своих членов, чат-форумы и дискуссионные площадки.

Ранние Web сообщества эволюционировали и превратились в сайты социальных сетей, появившиеся в конце 1990-х годов, как часть электронной коммерции второго поколения.

2.1.3. Появление социальных сетей

Виртуальные сообщества обеспечивали важный сервис для небольших групп пользователей Интернет в первые годы его существования. По мере развития и Интернет и Web многие виртуальные сообщества обнаружили, что их первоначальная цель, заключающаяся в создании площадки для обмена новыми знаниями и опытом посредством онлайновой коммуникации начала постепенно размываться. Однако, в системах электронной коммерции второго поколения появился новый феномен в онлайновой коммуникации. Люди, использующие Интернет, стали замечать, что часто некие общие интере-

сы/темы (например, садоводство, воспитание детей, медицинские проблемы, и т.п.) необходимо требуют их онлайнового взаимодействия между собой.

Для этих поздних виртуальных сообществ Интернет реализовывал функцию инструмента, который делал возможным коммуникацию *между членами виртуального сообщества*. Внутреннее взаимодействие между членами виртуального сообщества теперь называется взаимодействием при помощи социальной сети. Web сайты, обеспечивающие взаимодействие между членами виртуального сообщества, называются *сайтами социальных сетей*. Большинство сайтов социальных сетей позволяют посетителю, являющегося членом социальной сети (виртуального сообщества), создавать и публиковать свой профиль, создавать список других членов социальной сети, с которыми осуществляется коммуникация, управлять этим списком и осуществлять мониторинг похожих списков, созданных другими членами социальной сети.

Одним из первых сайтов социальной сети является сайт SixDegrees.com, начавший свою деятельность в 1997 году. Работа сайта базировалась на теории, которая в русскоязычных публикациях носит наименование «теория шести рукопожатий», а в англоязычной литературе – «six degrees of separation». Теория утверждает, что если имеется некоторое множество индивидов, то любые два индивида, произвольно выбранные из этого множества, связаны между собой не более чем шестью промежуточными индивидами. Применительно к социальной сети это означает, что любые два члена сети отделены друг от друга не более чем шестью посредниками. Сайт SixDegrees.com был не в состоянии генерировать прибыль, необходимую для его поддержки и был закрыт в 2000 году. Более успешные сайты социальных сетей появились немного позже. В 2002 году заработал сайт Friendster.com, который являлся сайтом, имеющим отличительные черты современных социальных сетей. Сайт быстро увеличивался в размерах, однако, столкнувшись с рядом технологических проблем и ошибками в менеджменте, был вытеснен своими конкурентами, среди которых наиболее известным является сайт MySpace.com. До появления сайта Facebook.com сайт MySpace.com был самым популярным сайтом социальной сети в США.

Сайт Facebook получил своё имя и начал оперировать в 2006 году. Его основателем считается Марк Цукерберг (Mark Zuckerberg). В 2008 году Facebook превзошел MySpace.com и стал одним из наиболее популярных сайтов социальной сети в Северной Америке, Европе и некоторых районах Африки. В 2014 году социальная сеть сайта Facebook включала более одного миллиарда человек, его ежегодный доход превышал 6 миллиардов американских долларов, а рыночная стоимость – более 104 миллиардов долларов.

В 2011 году компания Google представила сайт социальной сети Google+ как конкурента Facebook. Хотя сайт Google+ и получил значительное количество членов в свою социальную сеть, он всё ещё существенно уступает сайту Facebook.

В странах Азии сайты социальных сетей, использующие местные языки, такие как GREE и mixi в Японии, а также Renren в Китае появились примерно в то же время, что и сайт Friendster.com в США и тем самым ослабили популярность последнего в этих странах. В 1999 году китайская инвестиционная компания Tencent Holdings создала сайт QQ для конкуренции с американским сайтом SixDegrees.com, а в 2009 году перезапустила его вместе с двумя дополнительными сайтами на китайском языке (WeChat и Weibo), ориентированными на внутренний рынок КНР. Сегодня сайты социальных сетей, оперирующие на местных языках, занимают ведущие позиции в таких странах как Китай, Россия и Япония. В Иране оперирует сайт на персидском языке под наименованием Cloob, являющийся ведущим сайтом Ирана, восполняющим потребность в создании социальных сетей после блокирования американских сайтов Facebook и Twitter.

Американский сайт социальной сети Orkut (проект кампании Google) никогда не был популярен в США, но стал сайтом ведущей социальной сети в Бразилии и Индии в период с 2008 по 2010 годы.

Сайт LinkedIn был создан в 2003 году и имеет целью содействие в продвижении бизнес контактов. Сайт позволяет членам социальной сети создавать списки проверенных и вызывающих доверие бизнес контактов. Затем члены сети приглашаются участвовать в

нескольких типах отношений, каждый из которых создан с целью либо найти работу, либо найти работника, либо установить деловые связи. Социальная сеть LinkedIn является доминирующей бизнес ориентированной социальной сетью в Северной Америке, Европе и Южной Африке.

Некоторые сайты социальных сетей предлагают членам социальной сети специфические виды взаимодействия. Например, сайт YouTube (владелец компания Google) популяризирует использование видео роликов. Сайт Twitter предлагает членам социальной сети возможность обмена короткими сообщениями, называемых «твитами» (tweets). На рис. 2.1 приведены наиболее популярные сайты социальных сетей и указаны даты из появления.

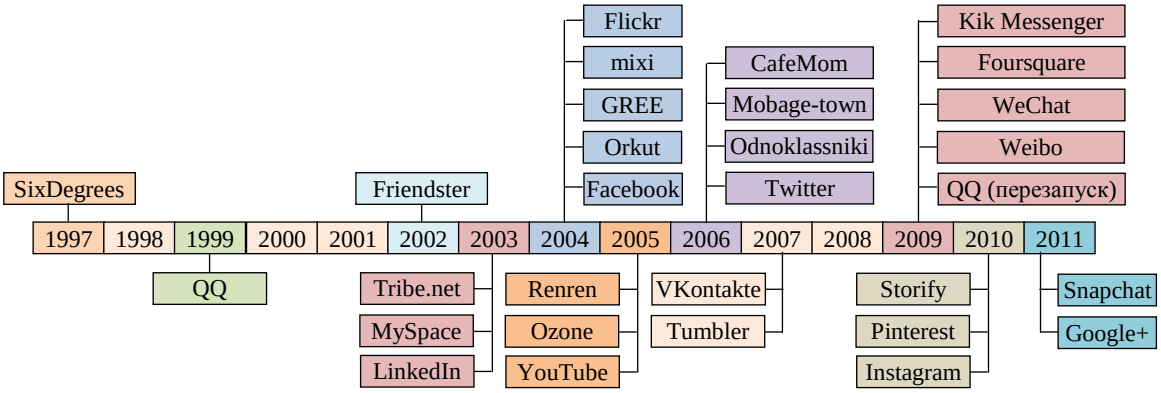

Рис. 2.1. Даты появления популярных Web сайтов социальных сетей

Для большинства сайтов социальных сетей общей является идея, заключающаяся в том, что посетителю сайта предлагается присоединиться к сообществу, исходя из предположения, что новые члены полезны для всего сообщества. Как правило, сайт социальной сети снабжен справочником, в котором содержится информация о членах социальной сети: местонахождение, интересы и характерные особенности. Однако, справочник не раскрывает информацию об имени и контактах членов социальной сети. Член социальной сети может предложить осуществить взаимодействие любому другому члену сети, но связь не будет установлена до тех пор, пока адресат не подтвердит желание осуществить контакт.

В дополнение к возможности поиска и анализа информации о новом члене социальной сети в справочнике, члены социальной сети могут осуществлять взаимодействие с новым членом через друзей, которых они выбрали и установили в сообществе. Путём постепенного построения множества связей, члены социальной сети строят такие взаимоотношения друг с другом, которые могут быть полезны не только в данный момент, но и в будущем.

Некоторые социальные сети фокусируют свою деятельность на специфических интересах или возможностях. Например, спецификой сайтов социальных сетей Flickr, Instagram и Pinterest является использование фотографий и картинок в качестве организующей темы. Сайт CafeMom привлекает посетителей, у которых есть маленькие дети. Сайт Snapchat позволяет членам сообщества обмениваться фотографиями и видео, снабженными текстовыми или графическими аннотациями. Доступ к таким фото и видео ограничен во времени. Сайты Tumbler и Twitter предлагают средства для обмена короткими сообщениями.

Экспансия сайтов социальных сетей по всему миру продолжается по мере развития систем электронной коммерции третьего поколения. В дополнение к, упомянутым ранее, успешным китайским и японским сайтам популярные сайты на местных языках появились в: Германии (Xing), Нидерландах (Hyves), России (VKontakte и Odnoklassniki), Испании (Tuenti) и Тайване (Plurk). Рис. 2.2. иллюстрирует распространение наиболее популярных сайтов социальных сетей в некоторых регионах мира.

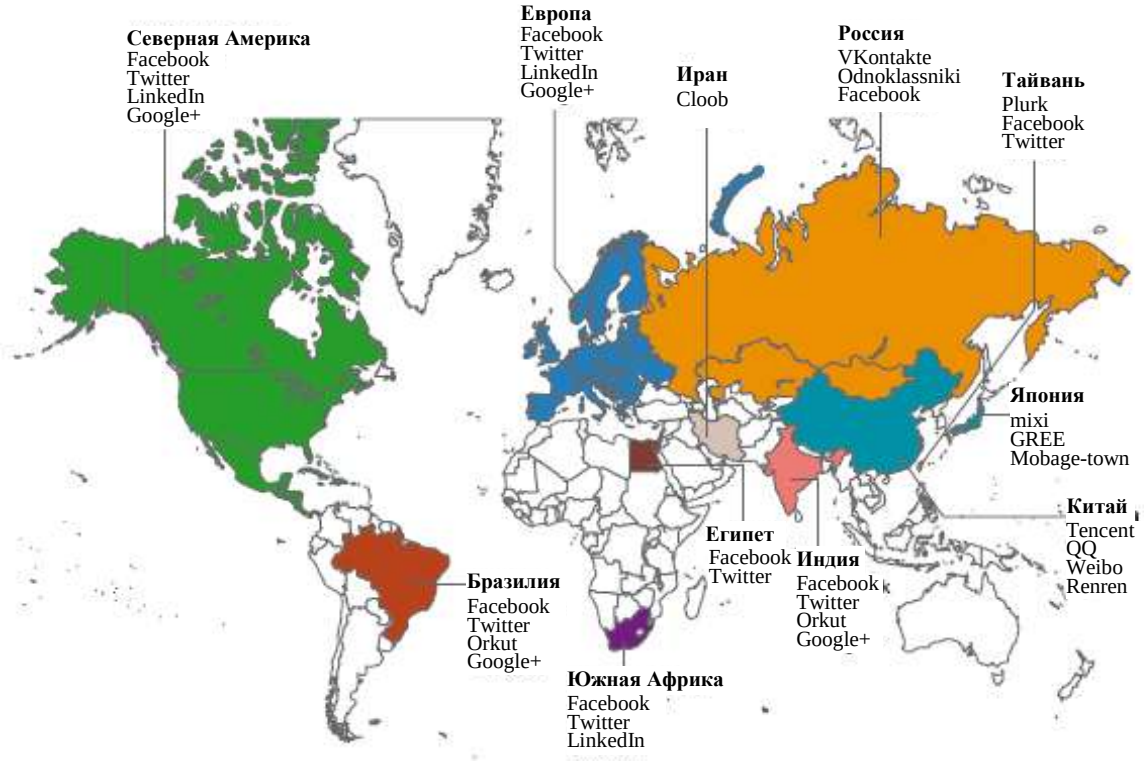

Рис. 2.2. Распределение популярных Web сайтов социальных сетей по странам

Блоги и микроблоги

Ранее, при изучении дисциплины «Электронная коммерция» (см. подраздел 4.2.1. конспекта лекций по дисциплине «Электронная коммерция») мы ввели понятие *Web-лог* или *блог* (*Web log* или *blog*). Блог представляет собой Web сайт, содержащий комментарии, посвящённые некоторому событию или некоторой теме. Многие блоги приглашают посетителей сайта добавлять свои комментарии, которые могут редактироваться либо не редактироваться владельцем блога. В результате деятельности блога формируется продолжающаяся дискуссия по определенной тематике с возможностью участия в ней многих людей, обладающих различной точкой зрения на одну и ту же тему. Поскольку блог-сайты поощряют интерактивное взаимодействие между его посетителями, интересующимися конкретной темой, они могут рассматриваться как одна из форм сайтов социальных сетей. Такие сайты как Twitter могут рассматриваться как *микроблоги* (microblogs), поскольку они функционируют как неформальные блог-сайты с короткими комментариями-твитами, размер которых не превышает 140 символов.

Ранние блоги фокусировали свое внимание на технологических темах, или на темах, относительно которых люди имели устойчивые убеждения (например, политические или религиозные). Сегодня социальные среды часто используются для организации широкомасштабной политической или благотворительной деятельности.

Наблюдая за успешным использованием социальных сред в политической деятельности, многие розничные продавцы начали осваивать этот инструмент для привлечения внимания тех посетителей коммерческих сайтов, кто ещё не готов совершить покупку, но заинтересовался предлагаемыми товарами или услугами. Менеджеры в области маркетинга и управления снабжением также видели выгоду в использовании социальных сетей в улучшении отношений между компаниями, участвующими в электронной коммерции типа «бизнес-бизнес». Многие компании, участвующие в электронной коммерции типа «бизнес-бизнес», используют блоги и микроблоги как часть своего Web присутствия для

предоставления заказчикам площадки, позволяющей обсуждать использование и технические спецификации товаров или услуг, продаваемых компанией.

Американский телевизионный канал CNN был первым средством массовой информации, включившим информацию из блогов и микроблогов в свои новостные программы. Сегодня, многие крупные широковещательные каналы и газеты включают социальные среды в свои Web сайты, передачи и печатные издания. Газеты всех размеров, часто, предпочитают поддерживать микроблог, в котором участвуют читатели, чем платить репортёрам за статьи о событиях, которые интересны только небольшому сегменту читательской аудитории. Тренд на участие читателей в предоставлении новостей средствам массовой информации называется *представительной журналистикой* (participatory journalism) или *гражданской журналистикой* (citizen journalism).

В дополнение к тому, что блог является частью некоторой деятельности (такой, например, как политическая кампания, благотворительность, университетская деятельность, розничная торговля или функционирование средства массовой информации) он может быть бизнесом сам по себе, если генерирует финансовые средства при помощи оплаты услуг или рекламирования. Примером является блог TechCrunch, основанный в 2005 году блогером по имени Майкл Аррингтон (Michael Arrington). Майкл Аррингтон собирал информацию о новых онлайновых компаниях *стартапах* (startups). Вместо того, чтобы публиковать эту информацию в бизнес ориентированных средствах массовой информации, он решил открыть свой собственный бизнес на основе коммерческого использования блога. Основным источником дохода блога TechCrunch являются средства, получаемые от рекламодателей, размещающих рекламные объявления на его страницах.

Территориально-ориентированные мобильные социальные сети

Способность мобильных устройств, имеющих доступ в Интернет, перемещаться по поверхности земного шара открывает для сайтов социальных сред новые возможности основанные на учёте местоположением пользователя. Большинство мобильных устройств могут передавать Web сайтам (с разрешения пользователя) информацию о своём местоположении. Эта информация может использоваться для адаптации сервисов сайта (например, содержания рекламных сообщений) к местоположению пользователя. Такие сервисы называются *территориально-ориентированные сервисы* (location-aware services).

В 2013 году около 30% пользователей социальных сред связывали свои посты с информацией о своём местоположении, а 75% владельцев мобильных устройств получали информацию и своём местоположении. Ведущей территориально-ориентированной социальной сетью является сеть Foursquare, которая спроектирована с учётом того, что взаимодействие между членами социальной сети осуществляется при помощи мобильных устройств и с адаптацией к их местонахождению. Территориально-ориентированные сервисы обеспечивают сайты Facebook и Google+.

2.1.4. Коммерческое использование социальных сетей

Методы коммерческого использования социальных сред всё ещё находятся в процессе развития и существует множество различных точек зрения на то, что компании должны делать для коммерциализации социальных сред. Многие коммерческие компании подвергаются критике за то, что они превратили свою деятельность в социальных средах в плохо замаскированную рекламную кампанию. Хотя социальные среды позволяют компаниям осуществлять традиционную деятельность по рекламированию и продвижению (заниматься брендингом, укреплять уровень доверия между клиентами и компанией, анонсировать новые продукты и т.п.) большинство экспертов считают, что коммерциализация социальных сред должна осуществляться иначе чем традиционная деятельность по продвижению имени компании и её продуктов. Эффективный менеджмент взаимодействия в социальных средах позволяет компаниям получить много полезной информации о покупателях и потенциальных покупателях.

Как было отмечено в начальной части настоящего раздела, компания Starbucks не

использует социальные среды для распространения информации о своих продуктах или брендинга своего имени. Вместо этого Starbucks использует информацию, полученную от клиентов из социальных сред, для вовлечения их в совершенствование своих сервисов. Усилия компании Starbucks в деятельности социальных сред сфокусированы на изучении и анализе дискуссии своих клиентов относительно продуктов и сервисов компании и использовании полученной информации для самообучения.

Компания Brooks Running Shoes, являющаяся производителем обуви для занятий легкой атлетикой, категорически избегает использования социальных сред для непосредственной продажи своей продукции. Поскольку основными покупателями её продукции являются представители сообществ, интересующихся здоровьем и фитнесом, Brooks участвует в работе социальных сред, ориентированных именно на такие сообщества. Участвуя в дискуссиях, посвященных здоровью и фитнесу, компания показывает, что её собственные интересы совпадают с интересами её клиентов и, таким образом, опосредованно, укрепляет своё бренд имя и уровень доверия клиентов.

Компания Campbell's Soup (крупнейший в мире производитель консервированных супов) является ещё одним примером компании, которая крайне успешна в создании эффективного присутствия в социальных сетях. Компания начала свое участие в социальных сетях с фокусировки внимания на своих продуктах, однако, через некоторое время, обнаружила, что дискуссия о том, чем её продукция может быть полезной для семей, привлекает гораздо бóльше участников и, следовательно, бóльший интерес к продукции компании.

Таблица на рис. 2.3 характеризует стратегии, при помощи которых коммерческие компании могут извлекать выгоду от участия в четырёх типах социальных сред. Для каждого типа социальной среды указано: (1) каким образом компания может передавать информацию клиентам (по аналогии с традиционными стратегиям продвижения); (2) получать информацию от клиентов, анализируя содержимое их дискуссии.

	Передача информации клиентам	**Получение информации от клиентов**	**Содействие/мониторинг обмена информацией между клиентами**
Сайты социальных сетей	Размещать рекламные сообщения на платной основе, размещать информацию о товарах или услугах	Выделять информацию из сообщений участников дискуссии, обобщение и анализ этой информации	Выделять знания, общие для участников дискуссии и использовать эти знания для формирования лояльности у клиентов
Блоги	Публиковать новые сведения о будущих продуктах, оказывать информационные услуги по существующим продуктам	Побуждать клиентов высказывать новые идеи, пожелания относительно будущих и текущих покупок	Осуществлять мониторинг и обобщение дискуссий относительно компании и её продуктов
Микроблоги	Отвечать на вопросы о продуктах, откликаться на сообщения клиентов со специфическими ответами	Активно запрашивать у клиентов их мнение о существующих продуктах и пожелания по их улучшению	Осуществлять тщательный анализ содержимого сообщений клиентов и выявлять новые тренды в их восприятии продуктов
Территориально-ориентированные мобильные социальные сети	Размещать информацию о новых территориально-ориентированных продавцах, осуществлять территориально-ориентированное продвижение продуктов	Побуждать клиентов делать комментарии относительно территориально-ориентированного бизнеса	Соединять друг с другом территориально распределенных клиентов и собирать информацию о различиях в восприятии бизнеса клиентами в различных местах

Рис. 2.3. Стратегии коммерческих компаний по отношению к различным социальным средам

Сайты социального шопинга

Практика использования социальных сетей для организации и осуществления сделки между покупателем и розничным продавцом называется *социальным шопингом* (social shopping). Одним из первых сайтов социального шопинга является сайт электронных объявлений craigslist. Сайт был создан в 1995 году членом виртуального сообщества WELL Крейгом Ньюмарком (Craig Newmark) и первоначально был предназначен только для жителей Сан-Франциско. Однако сайт быстро разрастался и набирал популярность. Сегодня он включает информацию для 450 городов по всему миру. Сайт обладает многоязычным интерфейсом, а размещение объявлений на его страницах – бесплатное.

Web сайт под наименованием Etsy является сайтом социального шопинга для людей, участвующих в продаже и покупке изделий ручной работы. Социальная сеть сайта Etsy объединяет покупателей и продавцов, занимающимися различными видами ремёсел. Существует, также, отдельный сайт We Love Etsy где посетители сайта Etsy могут участвовать в обмене информацией о своём опыте работы с сайтом Etsy. Наличие этого отдельного сайта является хорошим примером того, что информационное взаимодействие клиентов между собой не менее важно, чем информационное взаимодействие между продавцом и его покупателями.

Сайт Wanelo комбинирует элементы социальных сред (таких как микроблоги и возможность размещения фотографий) с коммерческой деятельностью. Сайт Poshmark является сайтом социального шопинга, посвященный женской одежде и модным аксессуарам. Члены социальной среды размещают, на страницах этого сайта, фотографии вещей, которыми они владеют и хотят продать. Обсуждение стоимости сделки осуществляется путём частной коммуникации через социальную сеть сайта. Сайт Poshmark спроектирован таким образом, чтобы его использование было максимально комфортным владельцами смартфонов и планшетных компьютеров.

Социальные среды, базирующиеся на концепции

Сайты социальных сетей формируют сообщества, основанные на связях между людьми. Существуют Web сайты, которые создают сообщества, основанные на связях между идеями. Эти, более абстрактные сообщества, называются *социальными средами, базирующимися на концепции* (idea-based social media). Сайт, под наименованием Delicious называет себя «социальный менеджер закладок» (social bookmarks manager). Сайт предоставляет всем зарегистрированным пользователям услугу по хранению и публикации закладок на страницы Web. Все посетители сайта Delicious могут просматривать имеющиеся закладки, упорядочивая их различным способом.

Виртуальные обучающие сети

Одной из форм социальных сетей, с которыми часто сталкиваются студенты, является *виртуальная обучающая среда* (virtual learning media). Сегодня, многие университеты предлагают обучающие среды, подобные Blackboard Learn, предназначенные для заочного общения студентов и преподавателей. Обучающая среда Blackboard Learn включает такие инструменты как доска объявлений, чаты, доска для рисования и др., которые позволяют студентам общаться с преподавателями и друг с другом примерно таким же образом, как они это делают в физической аудитории.

Концепция виртуальных обучающих сред датируется примерно 2008 годом, однако обучающие *курсы, открытые для массового использования* (massive open online courses – MOOCs) стали широко известными в 2012 году после появления в Стэнфордском университете (США) таких проектов, как Coursera и Udacity. Университеты предлагают своим студентам курсы MOOCs бесплатно, и они привлекают внимание сотен и тысяч студентов. В 2013 году Технологический институт штата Джорджия (Georgia Institute of Technology, USA) в партнёрстве с Udacity анонсировал планы подготовки магистров на основе технологии MOOCs, наряду с традиционной технологией обучения.

Хотя многие учебные заведения используют MOOCs, как часть традиционного учебного процесса, специалисты в области образования высказываются критически по поводу ценности такой формы обучения. Большинство MOOCs характеризуются очень низким процентом студентов полностью завершающих программу обучения (в большинстве случаев менее 2% студентов завершают программу обучения). Защитники MOOCs аргументируют тем, что эта технология позволяет предоставлять обучающие услуги практически любому человеку в мире за очень низкую плату. По мере развития и совершенствования MOOCs и учебного процесса, базирующегося на виртуальных обучающих сетях, станут более определёнными перспективы использования этой технологии в будущем.

Программное обеспечение с открытыми исходными кодами

Некоторые компьютерные *программы с открытыми исходными кодами* (open-source software) ориентированы на разработку виртуальных обучающих сред. Примерами являются среды Moodle и uPortal. Программное обеспечение с открытыми исходными кодами создаётся группами программистов, которые распространяют его бесплатно. Программисты, использующие эти программы, могут вносить в них изменения с целью совершенствования их функций. Улучшенные программы становятся доступными всему сообществу на бесплатной основе.

Программы с открытыми исходными кодами являются ранними и успешными примерами виртуальных сообществ, которые сейчас называются социальными сетями. Каждая социальная сеть посвящена созданию, улучшению и поддержке специфического программного приложения. Большое количество программ с открытыми исходными кодами используются для функционирования Интернет, коммерческих Web сайтов и систем электронной коммерции.

2.1.5. Модели получения дохода для сайтов социальных сетей

До конца 1990-х годов виртуальные сообщества использовали, главным образом, модель рекламной поддержки для получения дохода. Машины поиска (Web-порталы) также использовали модель рекламной поддержки и продавали рекламодателям возможность размещать рекламные объявления на своих страницах. В конце 1990-х годов большое количество слияний и поглощений образовали новые сайты. Однако, эти новые сайты обладали теми же отличительными чертами сайтов виртуальных сообществ, Web-порталов и других информационно-ориентированных сайтов распространенных в ранние годы существования Web, и продолжали использовать модель рекламной поддержки для получения дохода.

Сайты социальных сетей с рекламной поддержкой

При изучении дисциплины Электронная коммерция мы отметили, что сайты с большим количеством посетителей могут требовать от рекламодателей более высокую плату за размещение на своих страницах рекламные объявления. Мы, также отметили, что *липучесть сайта* (Web-site stickiness), или его способность удерживать внимание посетителя и вызывать у посетителя желание повторной работы с сайтом является важным элементом привлекательности сайта для рекламодателей (см. подраздел 3.1.3. конспекта лекций по дисциплине «Электронная коммерция»). Одной из простых мер липучести сайта может быть среднее время, которое посетитель тратит на восприятие страниц сайта в течение месяца. В таблице на рис. 2.4, перечислены владельцы некоторых, наиболее популярных сайтов и количество посетителей, имеющих доступ к страницам этих сайтов в течение августа 2013 года. Как видно на рис. 2.4, лидирующие сайты ежемесячно посещают более 200 миллионов уникальных посетителей.

Таблица на рис. 2.4 показывает среднее время, которое каждый посетитель сайта, ежемесячно тратит на восприятие страниц сайта (мера липучести).

Владелец	Миллионы уникальных посетителей	Среднее время работы с сайтом (в часах и минутах) одного уникального посетителя в течение месяца
Google	375	3:19
Microsoft	312	2:59
Facebook	277	7:44
Yahoo!	204	2:36
Wikimedia Foundation	142	0:19
Amazon.com	141	1:34
InteractiveCorp	132	0:12
eBay	132	1:28
Apple Computer	100	1:42
AOL, Inc.	86	2:51

Рис. 2.4. Посещаемость и липучесть лидирующих Web сайтов

Сайты социальных сетей, использующие модель рекламной поддержки совместно с моделью «плата за услугу»

Хотя большинство сайтов социальных сетей используют модель рекламной поддержки в чистом виде, некоторые сайты дополняют её моделью «плата за услугу». Примером может служить Web-портал Yahoo!, который оказывает большинство услуг бесплатно (получая доход за счет рекламной поддержки), однако некоторые премиум-услуги продаёт. Например, Yahoo! продаёт дополнительное пространство для хранения больших сообщений и файлов своего e-mail сервиса.

Некоторые сайты социальных сетей, так же как и Yahoo!, дополняют модель рекламной поддержки моделью «плата за услугу» при помощи стратегии, называемой *монетизация посетителей* (monetizing visitors). Монетизацией посетителей называется стратегия, которая позволяет конвертировать регулярных посетителей сайта, ищущих бесплатную информацию или услугу, либо в подписчиков на платные услуги сайта, либо в разовых покупателей платных услуг. Сайты, использующие стратегию монетизации посетителей, всегда обеспокоены негативной реакцией на эту стратегию со стороны своих посетителей. Трудно предугадать какое количество посетителей будут согласны оплачивать услуги, которые ранее, в той или иной форме, предоставлялись бесплатно. Поэтому многие сайты социальных сетей отказываются от стратегии монетизации посетителей, ограничиваясь моделью рекламной поддержки. Примерами являются сайты Facebook и Twitter.

Другими сайтами социальных сетей, которые использую смешанную модель получения дохода, являются сайты, предоставляющие финансовую информацию. Примерами являются сайты The Motley Fool и TheStreet.com. Эти сайты предлагают советы по инвестированию, осуществляют котировку ценных бумаг и оказывают помощь в планировании финансов. Некоторая часть информации предлагается бесплатно, другая часть информации также предлагается бесплатно тем посетителям, которые требуют персонализированную информацию и являются подписчиками сайта. Однако наибольшее количество персонализированной информации предоставляется платным подписчикам.

Платные социальные сети

Одна из первых попыток монетизации социальных сетей, путём оплаты членами социальных сетей специфических услуг, была осуществлена сайтом Google Answers. Сайт предоставлял своим посетителям возможность размещения вопросов, на которые отвечали эксперты Google Answers. Если посетитель был удовлетворен ответом, он оплачивал услуги эксперта в размере нескольких десятков долларов. Сайт разработал тест, при помощи которого определялись те члены социальной сети, квалификация которых

была достаточна для включения их в состав экспертов. Сайт Google Answers функционировал в период с 2002 по 2006 годы. Похожие услуги предоставляются сайтом Yahoo! Answers. Волонтёры сайта Yahoo! Answers отвечают на вопросы членов социальной сети, но, в отличие от экспертов Google Answers, делают это бесплатно, а доходы сайт получает при помощи модели рекламной поддержки.

После того, как сайт Google Answers прекратил свою деятельность в 2006 году многие его эксперты объединились и создали платный сайт Uclue, который функционировал в период с 2007 года по 2017 год. Сайт отвечал на вопросы своих посетителей и генерировал прибыль, используя модель «плата за услугу». Стоимость ответа зависела от сложности вопроса и колебалась в диапазоне от 10 до 400 долларов.

Приведенные примеры иллюстрируют то, каким образом социальные сети могут получать доход, предоставляя членам сообщества площадку для взаимодействия.

Сайты микро-кредитования

Одно из наиболее интересных направлений в использовании социальных сетей является создание сайтов, которые функционируют как *расчётные палаты* (clearinghouses), осуществляющие *микро-кредитование* (microlending). Микро-кредитованием называется практика предоставления небольших кредитов *с целью запуска или оперирования малыми предприятиями*. Микро-кредитование приобрело особенную популярность в развивающихся странах после того, как автор этой идеи Мухаммед Юнус (Muhammad Yunus) стал лауреатом Нобелевской премии за работы по микро-кредитованию бизнеса в Бангладеш.

Ключевым элементом успешности системы микро-кредитования является её функционирование в среде социальной сети заёмщиков. В этом случае заёмщики оказывают как поддержку друг другу, так и элемент давления друг на друга для гарантирования того, что кредит будет возвращен каждым из членов сети. Сайт Kiva является примером сайта социальной сети, который объединяет большое количество инвесторов, выдающих небольшие беспроцентные займы бизнесменам по всему миру для старта или поддержки функционирования малых предприятий.

Партнёрами сайта Kiva являются микро финансовые организации, обладающие знаниями об условиях для занятия бизнесом в различных частях мира. Эти организации выбирают тех бизнесменов, которые, с их точки зрения, являются надёжными заёмщиками и помогают им разместить запрос о предоставлении займа на сайте Kiva. Кредитор может проанализировать запрос и принять решение о фондировании части (или всей) запрошенной суммы, используя сайт Kiva. Займы, которые обычно находятся в диапазоне от нескольких сотен до нескольких тысяч долларов, должны быть возвращены в течении короткого промежутка времени, колеблющегося от нескольких месяцев до одного года.

На ранних этапах интерес к микро-кредитованию фокусировался на кредиторах из стран с развитой экономикой и заёмщиках из менее развитых стран, потому что сумма, являющаяся незначительной для богатого человека, часто является существенной для того, кто начинает свой бизнес в странах, в которых экономика находится в бедственном положении. Хотя такая модель микро-кредитования продолжает доминировать, страны с преуспевающей экономикой также используют технику микро-кредитования для поддержки малых предприятий на начальной стадии их существования. Примером может служить программа микро-кредитования малых предприятий в штате Мичиган (США), стартовавшая в 2014 году. Эта программа нацелена на выдачу займов в диапазоне от 500 до 50000 долларов для предприятий с количеством наёмных работников не превышающим пять человек.

Сайты краудфандинга

Кроме поиска заёмщика, который может предоставить все средства, необходимые для финансирования бизнес-идеи, предприниматель может получить средства путём продажи большому количеству инвесторов части собственности своего предприятия. Сайты социальных сетей, которые предоставляют такую возможность, называются сайтами *на-*

родного финансирования или сайтами *краудфандинга* (crowdfunding). Примерами таких сайтов являются Kickstarter и IndieGoGo. Эти сайты предоставляют возможность, как малым компаниям, так и отдельным личностям по всему миру продавать долевое участие в своей деятельности.

Краудфандинг предполагает, что инвестирование осуществляет большое количество инвесторов, каждый их которых инвестирует небольшую сумму денег. Таким образом, краудфандинг, с одной стороны, снижает индивидуальный риск отдельного инвестора, а с другой – позволяет собрать значительные средства необходимые для функционирования нового предприятия.

Наиболее часто применяемый тип краудфандинга называется *краудфандинг, базирующийся на вознаграждении* (reward-based crowdfunding). Этот тип краудфандинга предполагает, что инвестор осуществляет предоплату товара или услуги, которые он получает, после того как компания использует инвестируемые средства. В этой версии краудфандинга, инвестор, по сути, является клиентом, который предоплачивает продукт, который он покупает со значительной скидкой.

Краудфандинг используется художниками и благотворительными организациями для финансирования конкретных проектов. Члены сообщества узнают о проекте из их описаний в социальных сетях или на сайтах краудфандинга и предоставляют средства, необходимые для завершения проекта. Обычно речь идёт о небольшой сумме денег, не превышающей 25 долларов, а люди, которые вкладывают свои средства, получают, в качестве награды, благодарность за то, что они поддержали достойный проект.

Внутренние социальные сети

Увеличивается количество компаний и организаций, которые используют внутренние Web сайты социальных сетей, предназначенные для общения между работниками компании. Сайты внутренних социальных сетей функционируют в пределах сети интранет компании или организации (см. подраздел 2.2.4. конспекта лекций по дисциплине «Электронная коммерция»). На сайтах внутренних социальных сетей, также, размещается важная информация, предназначенная для работников компании. Компании экономят значительные средства путем замены печатных информационных листков на информацию, размещенную на сайте внутренней социальной сети в электронной форме.

Сайты внутренних социальных сетей могут быть хорошим средством для укрепления рабочих отношений между сотрудниками компании, рабочие места которых не сосредоточены в одном месте, а территориально распределены по различным географическим областям. Внутренняя социальная сеть часто является площадкой для обсуждения услуг, предоставляемых компанией. Работники, оказывающие услуги клиентам компании, могут размещать в сети различные вопросы, а их более опытные сотрудники (которые могут находиться на значительном расстоянии) отвечать на эти вопросы. Некоторые компании создают личные страницы на таких сайтах как Facebook и используют их как инструменты внутренней социальной сети. Это позволяет компаниям экономить средства на создание собственной внутренней социальной сети.

2.2. Мобильная коммерция

Мобильные телефоны, сегодня, используются гораздо шире, чем устройства, обеспечивающие мобильную голосовую связь. При помощи мобильных телефонов можно отсылать и получать текстовые сообщения, осуществлять коммуникацию в Интернет, получать доступ к спутниковой системе позиционирования и т.д.

Мобильные телефоны, предоставляющие возможность работы с Web сайтами, впервые появились в 1999 году. Однако маленький экран этих телефонов существенно затруднял работу с Web браузерами. Современные смартфоны с большими экранами обеспечивают более приемлемые условия для работы с сайтами. Широкое использование смартфонов для работы с Web сайтами началось в 2008 году. Этому способствовали два технологических достижения: (1) быстрый прогресс в создании высокоскоростных бес-

проволочных телефонных сетей; (2) производство смартфонов с большими экранами с высоким разрешением, которые управляются открытой операционной системой, позволяющей работать не только с Web браузерами, но и различными Интернет ориентированными приложениями.

2.2.1. Интернет ориентированные мобильные телефоны

Интернет ориентированные мобильные телефоны впервые появились в Японии и некоторых странах Юго-восточной Азии, поскольку телекоммуникационные компании в этих странах первые начали внедрять высокоскоростные мобильные телефонные сети. Крупнейшая японская телефонная компания NTT DoCoMo начала заниматься мобильной коммерцией в 2000 году, предоставив своим клиентам возможность доступа к Интернет контенту при помощи технологии, названной i-mode. Технология i-mode предназначена для адаптации интернет контента и услуг для мобильных телефонов. Начав с продажи игр и других программ, предназначенных для мобильных телефонов, компания NTT DoCoMo стала лидером в мировой мобильной коммерции, включая онлайновую покупку и оплату товаров.

В Европе и Северной Америке смартфоны (например, Apple iPhone и смартфоны использующие операционную систему Android), а также высокоскоростные мобильные телефонные сети, необходимые для мобильной коммерции стали доступны в 2008 году.

2.2.2. Планшетные компьютеры

В 2010 году компания Apple выпустила планшетный компьютер iPad (с усечёнными вычислительными возможностями), меньший, по размеру, чем ноутбук, но больший чем смартфон. Планшетный компьютер может подключаться к Интернет либо через мобильную телефонную сеть, либо через беспроводную локальную компьютерную сеть. В течение года много других производителей представили свои планшетные компьютеры, конкурирующие с iPad. К 2012 году некоторые из этих производителей представили устройства, получившие наименование *фаблеты* (phablets, как комбинация слов phone и tablet). Фаблет представляет собой смартфон с большим экраном и может рассматриваться как гибрид смартфона и планшетного компьютера. К 2016 году количество проданных планшетных компьютеров превысило количество проданных настольных компьютеров и ноутбуков вместе взятых. Рис. 2.5 показывает динамику мировых продаж настольных и мобильных компьютеров.

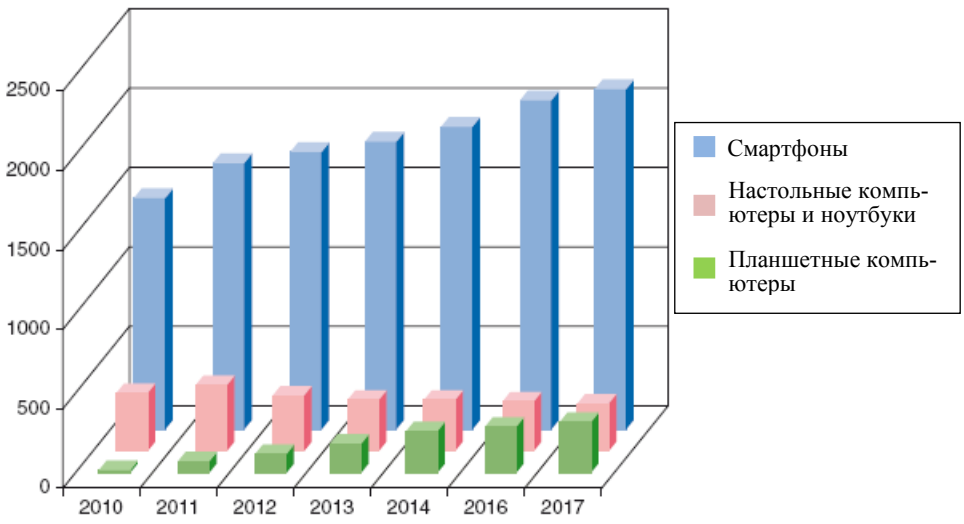

Рис. 2.5. Динамика продаж настольных компьютеров, ноутбуков, планшетных компьютеров и смартфонов (в миллионах штук)

Планшетный компьютер iPad, выпускаемый компанией Apple, управляется операционной системой iOS. Большинство других планшетных компьютеров (выпускаемых, например компаниями Samsung и Motorola) управляются операционной системой Android. Некоторые устройства для чтения электронных книг (например, Kindle, компании Amazon.com) могут использоваться как онлайновые планшетные компьютеры.

Разработку операционной системы Android финансировала компания Google как проект программы с открытым исходным кодом. Компания Google рассматривала эту работу как часть своих усилий по увеличению мобильного Web трафика. Компания Google заинтересована в увеличении Web трафика, поскольку основной моделью получения дохода этой компании является модель рекламной поддержки. Увеличение Web трафика приводит к увеличению стоимости рекламы и количества рекламодателей.

На рис. 2.6 приведены изображения смартфонов, фаблетов и планшетных компьютеров.

Рис. 2.6 Внешний вид смартфонов, фаблетов и планшетных компьютеров

Некоторые смартфоны и Интернет ориентированные мобильные телефоны отображают Web страницы, используя протокол, называемый *Протокол Приложений для Беспроводной Связи* (Wireless Application Protocol – WAP). Этот протокол позволяет отображать HTML отформатированные Web страницы, на устройствах с маленьким экранам. По мере увеличения экранов смартфонов и распространения фаблетов и планшетных компьютеров, использование протокола WAP стало необязательным. Обычные Web страницы могут эффективно отображаться на больших экранах с высоким разрешением, которыми снабжены фаблеты и планшетные компьютеры.

Использование сенсорного экрана для навигации по страницам Web сайта упрощает работу с устройствами, имеющими небольшой экран. Почти все современные модели смартфонов, фаблетов и планшетных компьютеров используют сенсорные экраны. Однако, некоторые модели снабжаются физической клавиатурой.

2.2.3. Операционные системы мобильных устройств

В прошлом, производители мобильных устройств разрабатывали свои собственные операционные системы для управления устройством и приложения, реализующие такие общие функции как календарь, контакты и электронная почта. Сегодня производители мобильных устройств используют стандартные операционные системы, выпускаемые третьей стороной.

Сегодня такими операционными системами являются Android и Windows Phone. Однако, более популярной и быстро развивающейся является операционная система Android, разработанная компанией Google. Как было отмечено ранее, операционная система Android является программой с открытым исходным кодом, что позволяет производителям смартфонов получать её бесплатно.

Одна из первых операционных систем для мобильных Интернет ориентированных устройств, а затем и для смартфонов, была разработана компанией Palm и называлась Palm OS. Смартфоны компании Palm не смогли завоевать популярность, и, после неудачных попыток продать операционную систему Palm OS другим производителям, компания ушла из бизнеса. Операционная система Symbian OS, разработанная в 1998 году консорциумом, состоящим из нескольких компаний во главе с Nokia, начиная с 2008 года, распространялась как программа с открытым исходным кодом. Однако в 2011 году компания Nokia перешла на использование операционной системы Windows Phone, компании Microsoft.

Рис. 2.7 показывает изменения на рынке основных операционных систем для смартфонов в период с 2006 года по 2013 год.

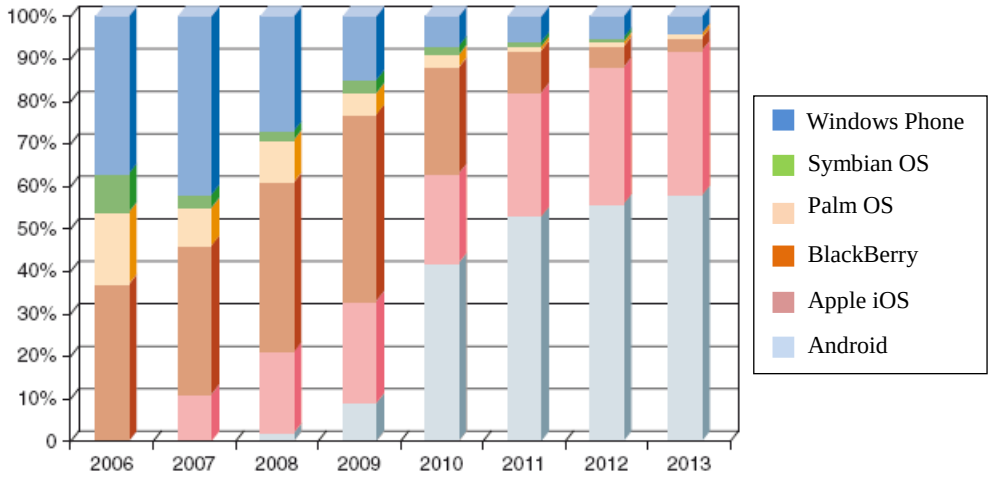

Рис. 2.7. Изменения на рынке операционных систем для смартфонов

После того, как производитель выбрал конкретную операционную систему для своих смартфонов, пользователь не может, по крайней мере, легко переключиться на другую операционную систему. В отличие от настольных компьютеров и ноутбуков операционная система смартфона интегрирована в программы, которые используются смартфоном для функционирования в сети.

Большинство производителей лишают смартфон гарантии, если обнаруживает, что пользователь тем или иным способом модифицировал операционную систему. Однако некоторые пользователи пытаются это сделать.

2.2.4. Мобильные приложения

В прошлом, производители смартфонов разрабатывали свои собственные операционные системы и контролировали использование программных приложений, работающих под управлением этих операционных систем. Сегодня, в большинстве смартфонов используется одна из двух общепринятых операционных систем Android или iOS, а приложения, работающие под управлением этих операционных систем, разрабатываются и продаются независимыми компаниями.

Сайт Apple App Store распространяет бесплатно (либо продаёт) приложения для смартфонов и планшетных компьютеров, производимых компанией Apple и работающих под управлением операционной системы iOS.

Онлайновый магазин Google Play распространяет приложения для смартфонов, фаблетов и планшетных компьютеров, работающих под управлением операционной системы Android.

Как компания Apple, так и компания Google разрешают независимым производителям прикладного программного обеспечения разрабатывать и продавать свои собственные приложения. В ряде случаев независимые производители приложений получают значительный доход от их продажи. Примером является компания Zynga, которая создала игровое приложение для смартфонов, приносящее ей ежегодный доход более чем в 1 миллиард долларов.

Большое количество бесплатных приложений разрабатывается только для того, чтобы обеспечить быстрый доступ к Web сайту компании. Например, онлайновые коммерческие компании бесплатно распространяют приложения, которые обеспечивают пользователю наилучшие условия для работы с сайтом онлайнового магазина на маленьком экране смартфона. В категорию платных приложений попадают игры, головоломки, а также инструментальные приложения, повышающие производительность труда, такие, например, как менеджеры контактов, календари и органайзеры. Стоимость большинства платных приложений невелика и колеблется в диапазоне от 1 до 5 американских долларов (хотя, стоимость отдельных приложений может быть значительно выше).

Продавцы мобильных приложений часто используют рекламирование как элемент своей модели получения дохода. Эти приложения предназначены для отображения сообщения рекламодателя, не являющегося продавцом приложения. Одним из распространённых способов включения рекламного сообщения в приложение является отображение его в виде небольшой полоски в нижней части экрана. Приложения могут отображать рекламное сообщение на части экрана, или на отдельном экране, который вызывается пользователем. Пространство для размещения рекламных сообщений на страницах мобильного приложений продается по той же схеме, что и пространство для размещения баннерной рекламы.

Некоторые онлайновые средства массовой информации предлагают пользователям мобильных компьютеров бесплатный доступ к контенту при помощи специальных приложений; другие – используют приложения для платного доступа к контенту по подписке.

Возрастает количество услуг в банковской и финансовой сферах (таких, например, как услуг биржевых брокеров) оказываемых при помощи мобильных устройств. Возможность выполнения банковских операций или операций фондового рынка мобильно, вне зависимости от географического местоположения, привлекательно для многих клиентов. Специалисты отмечают, что такие приложения легко создать, а финансовые организации заинтересованы в их распространении.

Крупные больницы и клиники распространяют приложения, которые обеспечивают лечащему врачу доступ к детальной информации о пациенте, необходимой для мониторинга состояния организма пациента и его лечения. Кардиологи, при помощи мобильных устройств, могут анализировать кардиограммы своих пациентов, находясь на удалении от клиники и давать немедленные консультации. При помощи мобильных устройств, больные диабетом могут получать сведения об инъекциях инсулина, уровне глюкозы в крови, физической активности и другие данные. Врачи, лечащие пациентов, страдающих диабетом, получают доступ к этой информации и могут оперативно помогать своим больным.

Практически все мобильные компьютеры обладают средствами для точного позиционирования на поверхности земного шара. Поэтому, приложения могут, например, сравнивать местоположение пользователя мобильного устройства с местоположение ближайшего ресторана, кинотеатра, автосервиса или торгового центра и использовать эту информацию в коммерческих целях.

2.2.5. Мобильные приложения для оплаты розничных покупок

В 2004 году, японская телефонная компания NTT DoCoMo начала продажу мобильных телефонов, называемых *мобильными кошельками* (mobile wallets), которые мо-

гут функционировать как кредитные карты при оплате покупок в традиционных магазинах розничной торговли. Хотя эти приложения, часто, имеют ограниченные возможности (например, при помощи одного из приложений можно оплачивать покупки в торговых автоматах на территории Японии) они пользуются популярностью. В странах, где покупатели привыкли расплачиваться за розничные покупки наличными деньгами, приложения для мобильных телефонов, позволяющие оплачивать розничные покупки, получили широкое распространение. Как правило, в таких странах только небольшая часть населения обладает кредитными картами, и владельцев мобильных телефонов привлекает возможность их использования для оплаты покупок.

В экономически развитых странах, где повсеместно используются кредитные карты, использование мобильных приложений для оплаты покупок в традиционных магазинах не столь популярно. Тем не менее, начиная с 2011 года, многие компании в США начали предлагать розничным магазинам технологии, позволяющие использовать смартфоны в качестве средства для оплаты покупок. Компания Starbucks отмечает, что в 2014 году 12% её клиентов оплатили покупки при помощи приложений, установленных на мобильных устройствах.

M1

M2

2.3. Онлайновые аукционы

Во многих случаях онлайновые аукционы обеспечивают коммерческим компаниям возможности, которые хорошо согласуются с организацией и возможностями Web. Сайт аукциона может требовать оплату своих услуг, как от продавца, так и от покупателя, а также продавать пространство на своих страницах для размещения рекламных объявлений. Люди, заинтересованные в торговле специфическими товарами формируют отдельный сегмент рынка, за доступ к которому рекламодатели согласны платить дополнительные деньги. Таким образом, те же самые возможности целевого рекламирования, которые могут предоставлять машины поиска, доступны рекламодателям на сайтах онлайновых аукционов. Возможность комбинации моделей получения дохода (в виде платежей участников торгов за услуги и платежей рекламодателей) позволяет сайтам онлайновых аукционов получать прибыль с первых дней своего существования.

Одна из сильных сторон Интернет заключается в том, что он может соединять между собой людей, географически разделённых большими расстояниями. Онлайновые аукционы могут капитализировать эту возможность либо путём удовлетворения узких потребностей местных рынков, либо путём создания общих сайтов, состоящих из разделов, ориентированных на специфические интересы.

Онлайновые аукционы создают естественную социальную сеть, поскольку продавцы и покупатели, заинтересованные в некоторой категории товаров, «собираются» на сайте аукциона, автоматически образуя критическую массу высоко мотивированных участников. Поэтому, практически все сведения о социальных сетях, приведенные в настоящем разделе, применимы к бизнесу при помощи онлайновых аукционов.

2.3.1. Принципы организации аукционов

Наиболее ранние записи об аукционах сделаны примерно в 500 году до нашей эры в древнем Вавилоне. Известно, что солдаты Римской империи использовали аукционы для продажи трофеев, отобранных у завоёванных племён. Аукционы были общеприняты в английских тавернах в 17 веке, и использовались для торговли предметами искусства и мебелью. Английские колонисты привезли привычку торговли при помощи аукционов в Северную Америку. Здесь, аукционы использовались для торговли сельскохозяйственным инструментом, домашними животными, табаком и чернокожими рабами.

На аукционе продавец предлагает к продаже товар, но не назначает его цену. Потенциальные покупатели получают информацию о товаре, а также возможность ознакомится с товаром, а затем делают *предложение цены* (bid), которую они готовы заплатить за товар. Каждый потенциальный покупатель, или *участник торгов* (bidders) делает индивидуальную оценку товара и назначает свою цену. Процесс торгов управляется *аук-*

ционистом (auctioneer). На некоторых аукционах, люди, нанимаемые продавцом или аукционистом, также могут делать предложения цены. Этих людей называют *подставными участниками торгов* (shill bidders). Подставные участники торгов могут искусственно «раздувать» цену продаваемого товара, и их деятельность, часто, запрещена правилами аукционов.

Английские аукционы

Существуют различные виды аукционов. Большинство людей, которые посещали аукционы, либо наблюдали за их проведением по телевидению, знакомы с *английским аукционом* (English auction), во время которого участники публично и последовательно оглашают всё возрастающие предложения цены до тех пор, пока кто-либо не сделает самое высокое предложение. После этого торги останавливаются. В этот момент аукционист сообщает, что товар продан участнику аукциона, предложившему наивысшую цену. Этот тип аукциона также называется *аукцион по восходящей цене* (ascending-price auction). Английский аукцион иногда называют *открытый аукцион* или *открытый голосовой аукцион* (open auction или open-outcry auction) поскольку предложения цены объявляются публично.

В некоторых английских аукционах товарам назначается минимальное предложение цены или *резервированная цена* (reserve price). Резервированная цена это цена товара, с которой начинается аукцион. Если никто, из участников аукциона не желает платить резервированную цену, то товар снимается с аукциона и не продаётся.

Английский аукцион, на котором торгуется множество однотипных товаров, а участники аукциона указывают количество экземпляров товара, которое они хотят приобрести, называется *Янки аукцион* (Yankee auctions). Когда, во время Янки аукциона, завершается процесс предложения цены и торги останавливаются, то все экземпляры товара, выставленного на торги, распределяются между успешными участниками аукциона, предложившими наибольшую цену. Успешные участники торгов Янки аукциона получают некоторое количество экземпляров товара, однако оплачивают эти экземпляры по цене, предложенной последним из успешных участников торгов (предложившим наименьшую цену).

Рассмотрим пример, поясняющий идею Янки аукциона. Пусть на аукцион выставляется девять экземпляров товара. Пусть, после того как торги завершились определились три успешных участника аукциона, предложившие наивысшую цену. На первом месте находится участник аукциона, предложивший цену в 85 долларов, и заказавший пять экземпляров. На втором месте – участник аукциона, предложивший цену в 83 доллара, и заказавший три экземпляра. На третьем месте – участник аукциона, предложивший цену в 81 доллар, и заказавший четыре экземпляра. Все эти три успешных участника аукциона оплачивают свои покупки по цене 81 доллар за один экземпляр, но получают различное экземпляров. Тот участник, который предложил цену в 85 долларов, и находится на первом месте, получает все заказанные пять экземпляров. Остаётся четыре экземпляра. Тот участник, который предложил цену в 83 доллара, и находится на втором месте, может получить и получает все заказанные им три экземпляра товара. Оставшийся один экземпляр товара достаётся тому участнику, который предложил цену в 81 доллар, и находится на третьем месте, несмотря на то, что он торговался за четыре экземпляра.

Английские аукционы обладают недостатками, как по отношению к продавцу, так и по отношению к участникам аукциона. Поскольку для победы в английском аукционе его участнику достаточно превысить текущее наибольшее предложение цены на незначительную величину, то участник аукциона, как правило, предлагает не полную стоимость товара, в соответствии со своей личной оценкой, а лишь незначительное превышение текущего предложения цены. Это не позволяет продавцу получить максимальную возможную выгоду от продажи товара. Участник торгов рискует быть захвачен перевозбуждением от соперничества в процессе торгов и, в результате, предложить цену, превышающую их личную интуитивную оценку стоимости товара. Этот психологический феномен, спе-

циалисты, изучающие поведение участников аукционов, часто называют *проклятием победителя* (winner's curse).

Голландские аукционы

Голландский аукцион (Dutch auction) представляет собой форму открытого аукциона, на котором торги начинаются с предложения максимальной цены, которая постепенно снижается. Снижение цены происходит до тех пор, пока один из участников торгов не соглашается с текущим предложением цены. Голландский аукцион также называется *аукцион по убывающей цене* (descending-price auction). Фермерские кооперативы в Голландии использовали этот тип аукциона для продажи скоропортящихся продуктов и цветов, что послужило причиной наименования «голландский аукцион». В большинстве голландских аукционов на торги выставляется некоторое количество однотипных товаров. Общепринятая реализация голландского аукциона основана на использовании часов. Цена товара уменьшается на фиксированную величину с каждым «тиканьем» часов. Первый из участников аукциона, который говорит «стоп», останавливает часы, фиксируя, тем самым, цену товара, и становится победителем аукциона. Победитель может забрать либо все экземпляры товара, либо некоторую их часть, за установленную им цену. Если, после этого, часть экземпляров товара остаётся не проданной, то часы запускаются вновь, аукцион продолжается, а на торги выставляются оставшиеся экземпляры товара. Голландский аукцион более предпочтителен для продавца, поскольку участник торгов, как правило, останавливает часы, когда стоимость товара становится равной его личной оценке стоимости товара. Участник торгов не позволяет опуститься цене ниже, поскольку боится, что часы остановит другой участник торгов. Голландские аукционы особенно удобны для быстрой распродажи большого количества *сырьевых товаров* (commodity items). Сырьевой товар – это товар или услуга, которые трудно отличить от товара или услуги, продаваемых различными продавцами, поскольку их свойства стандартизованы. Единственным различием в сырьевых товарах, продаваемых различными продавцами, является их цена.

Аукционы с закрытыми предложениями по первой цене

В *аукционах с закрытыми предложениями* (sealed-bid auctions) участники торгов одновременно и независимо друг от друга предоставляют свои предложения цены. Участники торгов не имеют права обмениваться друг с другом информацией о своих предложениях цены. Для этого, предложения цены могут, например, представляться в запечатанных конвертах. В *аукционах с закрытыми предложениями по первой цене* (first-price sealed-bid auction) побеждает тот участник торгов, который предложил наивысшую цену. Если на торги выставляется несколько однотипных товаров, то оставшиеся товары распределяются среди остальных участников торгов таким же образом.

Аукционы с закрытыми предложениями по второй цене

Аукционы с закрытыми предложениями по второй цене (second-price sealed-bid auction) проводятся таким же образом, как и аукционы с закрытыми предложениями по первой цене, но с одним отличием. Победитель (предложивший наивысшую цену и находящийся на первом месте) покупает товар по той цене, которую предложил участник торгов, находящийся на втором месте. На первый взгляд, кажется, что такой аукцион не имеет смысла, поскольку победитель покупает товар по более низкой цене чем он предложил. Однако, как показывает практика, такой аукцион порождает бóльший доход для продавца, поскольку: (1) поощряет участников аукциона делать предложения цены в соответствии со своими личными оценками стоимости товара; (2) уменьшает вероятность сговора между участниками. Поскольку победитель защищён от ошибочно завышенного предложения цены, то все участники аукциона, как правило, предлагают цену, более высокую, чем в аукционе с закрытыми предложениями по первой цене. Аукцион с закры-

тыми предложениями по второй цене часто называют *аукционом Викри* (Vickrey auction) в честь экономиста Вильяма Викри (William Vickrey), получившего Нобелевскую премию за исследования этого типа аукционов.

Двойные аукционы

В *двойном аукционе* (double auction) и покупатель, и продавец предоставляют аукционисту предложения, состоящие из комбинации количества экземпляров товара и цены за один экземпляр. Аукционист сравнивает предложения и находит совпадения предложений продавцов (двигаясь от самой низкой цены в направлении самой высокой цены) с предложениями покупателей (двигаясь от самой высокой цены в направлении самой низкой цены). Этот процесс продолжается до тех пор, пока все экземпляры всех товаров не будут распроданы. Двойные аукционы могут проводиться либо как аукционы с закрытыми предложениями, либо как открытые голосовые аукционы.

Нью-Йоркская фондовая биржа (New York Stock Exchange), торгующая ценными бумагами, проводит *двойные аукционы с закрытыми предложениями* (sealed-bid double auctions), на которых аукционист, называемый *специалистом* (specialist), управляет торговлей конкретными ценными бумагами. Компания специалиста обязана использовать свои собственные фонды, когда это необходимо, для поддержки стабильности на рынке тех ценных бумаг, торговлей которых занимается специалист. Хотя система торговли ценными бумагами на Нью-Йоркской фондовой бирже, с использованием специалистов-посредников осуществляется более ста лет, критики утверждают, что специалисты, часто, используют свои знания для личного обогащения за счёт инвесторов. В 2007 году Нью-Йоркская фондовая биржа запустила электронную систему торгов, которая автоматически находит совпадение предложений покупателей и продавцов без использования специалистов-посредников. Сегодня электронная система осуществляет бóльшую часть торгов на Нью-Йоркской фондовой бирже.

Чикагская биржа опционов (Chicago Board Options Exchange) проводит *двойные открытые голосовые аукционы* (open-outcry double auctions) для торговли сырьевыми товарами и *фондовыми опционами* (stock options). Фондовым опционом называется договор, по которому покупатель опциона получает право совершить покупку или продажу ценных бумаг по заранее оговорённой цене в определённый момент в будущем или на протяжении определённого отрезка времени.

На Чикагской бирже опционов предложения о покупке или продаже выкрикиваются торговцами, стоящими на небольшой площадке в торговом зале, которая называется *торговая яма* (trading pit). Каждый сырьевой товар или опцион торгуется в отдельной торговой яме. Деятельность в торговой яме может быть весьма шумной, поскольку 20 или 30 торговцев одновременно громко выкрикивают свои предложения.

Двойные аукционы (как открытые голосовые, так и с закрытыми предложениями) успешно работают в том случае, когда продаются товары с хорошо известными стандартными качествами и в больших количествах (например, ценные бумаги или сельскохозяйственные продукты определённого типа). В этом случае торги могут проводиться без предварительной инспекции товара участниками аукциона.

Реверсивные аукционы (аукционы продавца)

В *реверсивном аукционе* (reverse auction), который, также, называется *аукционом продавца* (seller-bid auction) множество продавцов предоставляют предложения цены аукционисту, представляющего интересы одного покупателя. Предложения цены делаются для конкретного количества товара, которое желает приобрести покупатель. Во время торгов продавцы постепенно снижают цену до тех пор, пока снижение цены не прекращается, и торги не останавливаются. В реверсивных аукционах в качестве продавцов и покупателей, чаще всего, выступают не отдельные личности, а производственно-коммерческие компании. В этом случае компания-покупатель действует как аукционист и подбирает продавцов, участвующих в реверсивном аукционе.

Семь типов аукционов, описанные выше, чаще всего используются в бизнесе сегодня. В таблице, на рис. 2.8, приведены ключевые характеристики этих семи аукционов.

Тип аукциона	Ключевые характеристики
Английский аукцион	Начинается с самой низкой цены. Цена увеличиваются до тех пор, пока участники аукциона согласны увеличивать цену
Голландский аукцион	Начинается с самой высокой цены. Цена автоматически уменьшается до тех пор, пока один из участников аукциона не принимает цену.
Аукцион с закрытыми предложениями по первой цене	Процесс с анонимными предложениями цены. Выигрывает участник, предложивший наивысшую цену. Он приобретает товары по первой наивысшей цене.
Аукцион с закрытыми предложениями по второй цене (аукцион Викри)	Процесс с анонимными предложениями цены. Выигрывает участник, предложивший наивысшую цену. Он приобретает товары по второй наивысшей цене.
Двойной аукцион (открытый голосовой)	Покупатели и продавцы объявляют предложения, состоящие из комбинации цены и количества экземпляров товара. Аукционист сравнивает предложения продавца (от низшего к высшему) с предложениями покупателя (от высшего к низшему). Покупатели и продавцы могут изменять свои предложения, основываясь на знаниях, полученных от других предложений.
Двойной аукцион (с закрытыми предложениями)	Покупатели и продавцы объявляют предложения, состоящие из комбинации цены и количества экземпляров товара. Аукционист (специалист) сравнивает предложения продавца (от низшего к высшему) с предложениями покупателя (от высшего к низшему). Покупатели и продавцы не могут изменять свои предложения.
Реверсивный аукцион (аукцион продавца)	Множество продавцов представляют предложения цены аукционеру, который представляет единственного покупателя. Предложения цены делаются для определенного количества товаров, требуемых покупателю. Цена последовательно уменьшается до тех пор, пока ни один из участников аукциона не согласен более снижать цену.

Рис. 2.8. Ключевые характеристики семи типов основных аукционов

2.3.2. Категории онлайновых аукционов

Ежегодно миллионы людей покупают и продают множество разнообразных товаров на сайтах потребительских аукционах. Хотя онлайновый аукционный бизнес быстро меняется, по мере своего роста, сформировались три широкие категории Web сайтов аукционов: *общие потребительские аукционы* (general consumer auctions); *специализированные потребительские аукционы* (specialty consumer auctions) и *аукционы типа бизнес-бизнес* (business-to-business auctions). Большинство участников потребительских аукционов это обычные люди, которые используют сайты этих аукционов для продажи личных вещей. Поэтому, часто, потребительские аукционы относят к электронной коммерции типа потребитель-потребитель. Однако, поскольку участником потребительского аукциона может быть и коммерческая компания, их, также, относят к электронной коммерции типа бизнес-потребитель или потребитель-бизнес (см. подраздел 1.1.3 конспекта лекций по дисциплине Электронная коммерция).

Общие потребительские аукционы

Сегодня, наиболее успешным сайтом потребительских аукционов является сайт eBay. Продавцы и покупатели, торгующие на сайте eBay, должны зарегистрироваться и подтвердить своё согласие с условиями ведения торгов. Продавцы должны оплатить eBay *регистрационный сбор* (listing fee) и процент от окончательной стоимости проданного товара. В дополнение к перечисленным платам, продавец может заказать одну или несколько платных услуг. Например, выделение информации о товарах жирным шрифтом и перечисление товаров в привилегированных аукционах. Для покупателей, участие в аукционе eBay является бесплатным.

Компания eBay оказывает помощь покупателям в определении надежности продавцов. С этой целью она учредила рейтинговую систему. Покупатели, после завершения сделки, могут оценить продавцов и представить их рейтинги. Эти рейтинги преобразуются в графики и появляются рядом с именем продавца в каждом аукционе, где он принимает участие. Хотя такую систему нельзя назвать совершенной, многие участники аукциона eBay считают, что она в состоянии оказать им некоторую защиту от нечестных продавцов. Компания eBay использует рейтинги продавцов для накладывания на них некоторых ограничений (таких, например, как удерживание денежных средств в течение трёх недель), или, если рейтинг достаточно низкий, отстранения их от участия в аукционах eBay. Рейтинговая система работает и в обратном направлении. Продавцы назначают рейтинги покупателям, что обеспечивает их некоторой защитой от нечестных покупателей.

Хотя компания eBay не публикует статистические данные о мошенничестве, как со стороны покупателей, так и со стороны продавцов, большинство аналитиков считают, что потенциальные потери у продавцов выше, чем у покупателей. Наибольшие риски для продавцов исходят от тех покупателей, которые используют номера украденных кредитных карт, или тех, которые выигрывают торги, но не связываются с продавцом для завершения транзакции. Риски для покупателей исходят от тех продавцов, которые не доставляют товар или от тех, которые искажают информацию о своих товарах.

Формат аукциона, который использует eBay, чаще всего представляет собой компьютеризированную версию Английского аукциона. В Английском аукционе eBay продавцам разрешается устанавливать резервированную (начальную) цену, покупатели заносятся в список, но их предложения цены не раскрываются до окончания аукциона. Это несколько отличает Английский аукцион eBay он традиционного Английского аукциона с личным участием покупателей. Однако, поскольку eBay всегда показывает и постоянно обновляет наибольшее предложение цены, участник, наблюдающий за аукционом, видит, каким образом развиваются торги. Наибольшее отличие между «живым» Английским аукционом и аукционом eBay заключается в том, что участники аукциона не видят истории торгов (какой из участников аукциона предложил ту или иную цену и когда) вплоть до окончания аукциона. В Английском аукционе eBay продавцам разрешается специфицировать аукцион как приватный. В *приватном аукционе* eBay (eBay private auction) на сайте никогда не раскрывается информация об участниках аукциона и их предложения цены. По завершению торгов на приватном аукционе, eBay уведомляет только продавца и выигравшего участника аукциона. Другой тип аукциона, предлагаемый eBay, представляет собой аукцион с возрастанием цены для торговли множеством однотипных товаров. eBay называет такой аукцион голландским, однако, по сути, он является Янки аукционом.

В любом типе eBay аукционов, участники аукциона должны внимательно наблюдать за торгами, если они хотят выиграть. Во всех eBay аукционах установлен минимальный инкремент для предложения цены, который должен быть равным примерно 3% от наибольшего предложения. Участники аукциона могут ввести *прокси предложение цены* (proxy bid). Прокси предложение цены непрерывно и автоматически увеличивается до величины, превышающей текущее наибольшее предложения до тех пор, пока не достигнет максимальной цены, установленной участником аукциона.

Для привлечения продавцов, которые часто предлагают товары на аукционе, сайт eBay предлагает платформу онлайновых магазинов eBay stores, в которых продавцы мо-

гут предлагать товары для продажи, а также размещать информацию о товарах, выставляемых на eBay аукционах. Онлайновые магазины позволяют продавцам аукциона eBay получать дополнительную прибыль.

Общие потребительские аукционы: эффект блокировки

Будучи первым основным сайтом среди сайтов потребительских аукционов, и инвестируя значительные средства в рекламные кампании, eBay смогла рано установить и упрочить свою репутацию и бренд имя. Успех eBay инспирировал конкуренцию со стороны крупных и хорошо финансируемых компаний, включая Yahoo! и Amazon.com. Эти компании потратили значительные усилия и средства на то, чтобы сместить eBay с её лидирующих позиций, однако вынуждены были сдаться в 2006 и 2007 годах, соответственно. Экономическая структура онлайновых рынков, часто, предвзята, по отношению к новым участникам. Поскольку рынки становятся более эффективными, по мере того как увеличивается количества продавцов и покупателей, то новые участники аукционов склонны более лояльно относится к существующим рыночным площадкам. Поэтому существующие сайты аукционов, такие как eBay внутренне более ценны для потребителей, чем новые. Этот базовый экономический факт экономисты называют *эффектом блокировки* (lock-in effect). Эффект блокировки делает задачу создания новых успешных сайтов общих потребительских аукционов очень сложной.

Интересен пример влияния эффекта блокировки на Японский рынок общих потребительских аукционов. В Японии, крупной компанией, первой предложившей услуги онлайновых аукционов (в 1999 году), была компания Yahoo!. Первоначально компания Yahoo! не брала плату с продавцов за участие в своих аукционах. Когда, примерно через пять месяцев, компания eBay присоединилась к рынку онлайновых аукционов Японии и начала брать плату за участие в своих аукционах, она обнаружила, что только очень небольшое количество клиентов интересуется её услугами. Позже, когда компания Yahoo! тоже начала брать плату с участников своих аукционов, эффект блокировки всё равно обеспечил ей лидирующую позицию в Японии. Сегодня аукционы компании Yahoo! удерживают более 90% рынка онлайновых аукционов в Японии.

Специализированные потребительские аукционы

Вместо того, чтобы бороться с такими сильными соперниками как eBay, на рынке общих потребительских аукционов, многие компании стали ориентироваться на рынки специализированных товаров и создали сайты специализированных потребительских аукционов для удовлетворения потребностей этого сегмента.

Сайт JustBeads.com является примером сайта аукционов, который удовлетворяет потребности покупателей и продавцов, которые географически рассредоточены, но разделяют общие и очень специальные интересы (торговля бусами и бисером). Сайты Cigarbid.com (торговля сигарами) и Winebid (торговля вином) также являются примерами сайтов специализированных потребительских аукционов. Эти сайты работают с рыночными сегментами с легко идентифицируемыми товарами, которыми интересуются люди с относительно высоким уровнем доходов. Сайты специализированных потребительских аукционов работают с узкими сегментами рынка и являются прибыльными. Это позволяет им успешно сосуществовать вместе с сайтами больших общих потребительских аукционов, такими как eBay.

Реверсивные потребительские аукционы

В прошлом, коммерческие компании создавали сайты, на страницах которых потенциальные покупатели могли размещать запросы, описывающие товары или услуги, которые они желали приобрести. Сайты направляли эти запросы группе продавцов, которые отвечали на запросы при помощи сообщений электронной почты. Сообщения направлялись потенциальным покупателям, и содержали предложения о готовности про-

дать товар по конкретной цене. Такой тип коммерческого предложения часто называют *реверсивным предложением цены* (reverse bid). После получения реверсивных предложений, покупатель мог выбрать то из них, которое удовлетворяли его требованиям. Ни один из таких сайтов не был успешен и, через некоторое время, все они закрылись.

Многие специалисты относят сайт Priceline.com к категории реверсивных потребительских аукционов. Сайт Priceline.com ориентирован на путешественников и позволяет своим посетителям устанавливать цену, которую они готовы заплатить за такие услуги, как покупка авиабилета, аренда автомобиля, бронирование комнаты в отеле и т.п. Если эта цена достаточно высокая, то транзакция совершается. Сайт Priceline.com совершает эти транзакции, ориентируясь на цены, указанные в каталогах авиакомпаний, агенств, сдающих автомобили в аренду и отелей.

Групповой шопинг и сайты групповых купонов

Другой тип онлайнового бизнеса, в области электронной коммерции, реализуется сайтами *группового шопинга* (group shopping). На этих сайтах продавец размещает товар и указывает его предварительную цену. По мере того, как индивидуальные покупатели выражают согласие на приобретение товара (только согласие на приобретение без указания цены), оператор сайта обсуждает с продавцом возможность продажи товара по более низкой цене. Предварительная цена будет снижаться при условии, что увеличивается количество покупателей, желающих приобрести товар. Таким образом, сайты группового шопинга могут увеличить количество покупателей конкретного товара до величины, достаточной для того, чтобы побудить продавца сделать скидку. Чем большую партию товара продаёт продавец, тем большую скидку он готов сделать на единицу товара.

На сайтах группового шопинга хорошо продаются товары имеющие бренд имя, поскольку такие товары дают уверенность покупателю в том, что он совершает хорошую сделку, а не покупает низкокачественный товар по низкой цене.

Две компании, Mercata и LetsBuyIt.com оперировали основными сайтами группового шопинга в течение нескольких лет, однако обе были вынуждены приостановить свою деятельность после неудачных попыток найти постоянные источники продуктов, пригодных для продажи на их сайтах. Они обнаружили несколько продавцов продуктов, пригодных для группового шопинга (таких как компьютеры, бытовая электроника и небольшие электроприборы), которые готовы работать с ними. Однако, эти продавцы не видели особых преимуществ от продажи своих продуктов по сниженным ценам на сайтах группового шопинга, которые отбирали часть продаж у существующих каналов дистрибуции (см. подраздел 3.3.1 в конспекте лекций по дисциплине Электронная коммерция).

В 2008 году была предпринята попытка реформирования технологии группового шопинга. В Чикаго начал функционировать сайт под наименованием Groupon (сокращение от словосочетания «group coupon»). Сайт предлагает жителям Чикаго подписываться на групповые купоны и выставляет на подписку один групповой купон в день. Групповой купон означает, что если на него подписывается определенное количество людей, то он становится доступным для любого подписчика. Например, групповой купон на ужин, стоимостью в 50 долларов и подлежащий погашению в конкретном ресторане, может быть оценен в 30 долларов. Это означает, что подписчик на этот купон может получить 50-долларовый ужин всего за 30 долларов. Компания Groupon удерживает примерно половину стоимости группового купона (около 15 долларов), а остальную сумму получает ресторан. Таким образом, ресторан получал только 15 долларов за ужин стоимостью в 50 долларов. Рестораны согласны на это, поскольку рассматривают групповые купоны как способ продвижения своих услуг. Групповой купон позволяет ресторану произвести хорошее впечатление на нового клиента, продвигая свой бизнес без расходов на рекламу.

Компания Groupon занимается популяризацией своего бизнеса, используя социальные сети как Facebook и Twitter, для контакта со своими клиентами и распространения информации об ежедневных групповых купонах. Сегодня, основными клиентами компании Groupon являются женщины, поэтому групповые купоны, как правило, предлагаются для приобретения косметических и фитнес товаров.

Бизнесом по распространению групповых купонов занимаются, также такие компании как LivingSocial и Gilt Group. Некоторые аналитики считают, что возрастающая активность сайтов групповых купонов может составить конкуренцию таким крупным компаниям как eBay.

Аукционы типа бизнес-бизнес

Онлайновые аукционы типа бизнес-бизнес появились в связи с необходимостью удовлетворения специфических потребностей производственных компаний. Многие производственные компании периодически испытывают потребность в ликвидации излишков (неиспользуемых или избыточных материалов и инвентаря). Несмотря на все усилия менеджеров по снабжению и производству, время от времени производственные компании приобретают больше исходных материалов, чем это необходимо. Кроме того, непредвиденные изменения в требованиях, предъявляемых заказчиками к продуктам, могут приводить к накоплению избыточных готовых продуктах и комплектующих частей.

В зависимости от размера, компании используют один из двух методов дистрибуции излишков. Крупные компании содержат в штате своих сотрудников специалистов по ликвидации, которые занимаются тем, что разыскивают покупателей для неиспользуемых и избыточных материалов и инвентаря. Мелкие компании, часто, пользуются услугами посреднических брокерских компаний, специализирующихся на ликвидации излишков. Онлайновые аукционы являются логическим развитием деятельности компаний по ликвидации излишков с использованием технологии электронной коммерции.

Существуют три модели онлайновых аукционов типа бизнес-бизнес предназначенных для ликвидации излишков. Две из этих трёх моделей являются прямыми потомками двух традиционных методов ликвидации излишков, применяемых крупными и мелкими компаниями. Первая модель, используемая крупными компаниями, предполагает, что компания сама создает сайт аукционов, на котором продаёт свои собственные излишки. Вторая модель, используемая мелкими компаниями, предполагает, что компании пользуются услугами сайта аукционов, созданным брокером, специализирующимся на ликвидации излишков. Продавцы и покупатели, участвующие в торгах на аукционах, как первой, так и второй моделей, как правило, хорошо знакомы друг с другом. Третья модель напоминает потребительские аукционы и предполагает, что на рынке аукционов типа бизнес-бизнес, испытывающем недостаток в эффективности функционирования, появляется сайт новой компании, в торгах которого могут участвовать покупатели и продавцы, которые исторически не работали друг с другом.

Реверсивные аукционы типа бизнес-бизнес

В подразделе 1.4 мы изучали различные типы электронных рынков, предназначенных для осуществления транзакций в системах электронной коммерции типа бизнес-бизнес. Многие из этих электронных рынков работают как реверсивные аукционы.

Компания Owens Corning (крупный производитель стекла и строительных материалов) использует реверсивные аукционы для приобретения широкого спектра материалов в диапазоне от химикатов (прямые материалы) до транспортёров (основные средства производства) и до трубопроводной арматуры (материалы для технического обслуживания и ремонта). Компания Owens Corning участвует в реверсивных аукционах даже для приобретения бутилированной воды. Компания обнаружила, что приобретение материалов на реверсивных аукционах снижает их стоимость в среднем на 10%. Поскольку Owens Corning ежегодно тратит миллиарды долларов на приобретение прямых и непрямых материалов, снижение расходов на десять процентов является существенной экономией. Некоторые другие крупные производственные компании, такие как Boeing и Sony также используют реверсивные аукционы для приобретения прямых и непрямых материалов.

Однако, не все компании являются энтузиастами использования реверсивных аукционов для приобретения прямых и непрямых материалов. Некоторые эксперты в облас-

ти электронного снабжения отмечают, что реверсивные аукционы могут приводить к тому, что поставщики, конкурируя только на основе стоимости поставляемых материалов, экономят на качестве или нарушают графики поставок. Они же отмечают, что реверсивные аукционы могут быть полезны, главным образом, при приобретении товаров с установившимися стандартами качества, например, сырьевых товаров (commodity items). Список крупных компаний, не использующих реверсивные аукционы для приобретения материалов, включает Cisco и IBM.

Сторонники и противники реверсивных аукционов типа бизнес-бизнес приводят веские аргументы «за» и «против» целесообразности их использования, однако целесообразность их использования определяется спецификой производства конкретной компании. Использование реверсивных аукционов не целесообразно в тех случаях, когда доверие и долгосрочные стратегические отношения между участниками цепи поставок определяют эффективность функционирования цепи поставок. Фактически, целью менеджмента цепи поставок как раз и является установление долгосрочных и доверительных отношений между поставщиками. Использование реверсивных аукционов, при приобретении материалов, заменяет доверительные отношения между поставщиками на отношения конкурентов, что, с точки зрения менеджмента цепи поставок, является шагом назад.

В некоторых отраслях, компании-поставщики материалов крупнее и мощнее чем компании-покупатели материалов. В этих отраслях поставщики просто не соглашаются участвовать в реверсивных аукционах, что препятствует их проведению. В тех отраслях, где между поставщиками имеет место высокая степень конкуренции, реверсивные аукционы могут быть эффективным способом снижения цены приобретаемых материалов. На рис. 2.9 перечислены характеристики цепи поставок, которые способствуют или препятствуют использованию реверсивных аукционов типа бизнес-бизнес.

Характеристики цепи поставок, способствующие реверсивным аукционам:

- Поставщики конкурируют и соперничают друг с другом.
- Свойства материалов хорошо специфицированы и стандартизованы.
- Поставщики готовы снизить маржу, которую они получают при продаже.
- Поставщики готовы участвовать в реверсивных аукционах.

Характеристики цепи поставок, препятствующие реверсивным аукционам:

- Поставляемые материалы сложны и требуют регулярной модификации.
- Поставляемые материалы изготавливаются по техническим условиям покупателя.
- Долгосрочные стратегические отношения важны для покупателей и поставщиков.
- Затраты, связанные с заменой поставщика высоки.

Рис. 2.9. Характеристики цепи поставок и реверсивные аукционов

2.3.3. Аукцион ориентированные услуги

Успех сайта eBay и других сайтов аукционов стимулируют предпринимателей создавать онлайновые компании для оказания различных аукцион ориентированных услуг. Аукцион ориентированные услуги включают: эскроу услуги; информационные и справочные услуги и программное обеспечение аукционов.

Эскроу услуги аукционов

Общей озабоченностью покупателей онлайновых аукционов является надежность продавцов. Исследования показывают, что примерно 11% покупателей Web аукционов либо не получают купленные товары, либо получают товары, существенно отличающиеся от тех, которые были представлены на сайте аукциона. Около половины этих покупателей не в состоянии удовлетворительно решить возникшую проблему. При приобрете-

нии дорогостоящего товара покупатели могут воспользоваться *эскроу услугой* (escrow service) для защиты своих интересов.

Эскроу представляет собой соглашение между покупателем и продавцом, согласно которому деньги покупателя хранятся у третьей стороны (личность или организация) до тех пор, пока покупатель не получил товар и не будет удовлетворён его качествами. Некоторые эскроу услуги предполагают инспекцию товара и его доставку от продавца к покупателю. Инспекция товара осуществляется только с согласия и по поручению покупателя. Как правило, эскроу агенты, осуществляющие инспекцию товара, являются квалифицированными оценщиками произведений искусства и антиквариата, квалификация которых позволяет им правильно оценить качество и стоимость товара. Компании или личности, оказывающие эскроу услуги, берут плату в размере от 1 до 10 процентов от стоимости товара. Одной из лидирующих онлайновых компаний, оказывающих эскроу услуги для аукционов, является Escrow.com. Некоторые компании, оказывающие эскроу услуги, предлагают покупателям онлайновых аукционов приобрести страховые полисы, защищающие их от риска получить товар, не соответствующего качества или от риска недоставки товара. Зафиксированы случаи мошенничества со стороны эскроу компаний, особенно при оказании эскроу услуг для дорогостоящих товаров. Поэтому, прежде чем воспользоваться услугой эскроу компании, покупателю рекомендуется проверить её лицензию и обеспеченность и никогда не пользоваться услугами оффшорных эскроу компаний.

В случае приобретения товаров низкой стоимости стоимость эскроу услуг может быть непомерно высокой. Тем не менее, покупатели таких аукционов могут использовать другие способы защитить свои деньги. Один из способов заключается в знакомстве с информацией о продавце и его рейтинге на сайте аукциона. Кроме того, существуют сайты, размещающие на своих страницах списки продавцов, которые в прошлом тем или иным способом обманывали покупателей. Эти сайты представляют собой открытый ресурс и, часто, создаются и поддерживаются покупателями, которые пострадали от участия в аукционах. Поэтому такие сайты могут содержать субъективную и ненадежную информацию.

Информационные и справочные услуги аукционов

Другая аукцион ориентированная услуга, которую некоторые компании предлагают в Web, это доступ к информации, связанной с аукционами. Сайт eCommerceBytes является известным англоязычным информационным сайтом аукционов, который размещает на своих страницах информацию, посвященную индустрии онлайновых аукционов. Сайт публикует руководства для новых участников онлайновых аукционов, полезные рекомендации для продвинутых покупателей и продавцов, а также справочники сайтов онлайновых аукционов.

Сайт Price Watch специализируется на публикации списков актуальных цен на компьютерное оборудование, программное обеспечение компьютеров и потребительскую электронику. Участники Web аукционов могут использовать информацию, размещённую на сайте Price Watch, для выработки стратегии участия в торгах онлайновых аукционов.

Программное обеспечение аукционов

Как продавцы, так и покупатели онлайновых аукционов могут приобретать специализированное программное обеспечение, помогающее управлять продажами/покупками на онлайновых аукционах. Наиболее известными компаниями, продающими подобное программное обеспечение, являются AuctionHawk и Vendio. Продавцы могут участвовать в нескольких аукционах одновременно. Для продавцов эти компании предлагают инструментальные программы, которые могут помочь или автоматизировать решение следующих задач: хостинг изображений, рекламирование, проектирование страницы, трекинг и управление обратной связью, трекинг отчётов и управление электронной почтой и др. Отмеченные инструменты могут использоваться продавцами для создания привлекательного внешнего вида своих страниц и управления сотнями аукционов.

Большое количество компаний продают *программы снайпинга* (sniping software), предназначенные для покупателей аукционов. Программа снайпинга следит за развитием аукциона. За одну или две секунды до его окончания программа размещает предложение цены, необходимое и достаточное для победы (кроме тех случаев, когда эта сумма превышает предел, установленный владельцем программы). Действие по размещению выигрышного предложения цены в последнюю секунду называется *снайп* (snipe). В обыденной речи английское слово «snipe» переводится как снайперский выстрел. Поскольку программа снайпинга синхронизирует свои внутренние часы с часами сайта аукциона и размещает предложение цены с компьютерной точностью, она почти всегда выигрывает у покупателя человека. Некоторые сайты предлагают *услуги снайпинга* (sniping services). Это означает, что программа снайпинга выполняется на сайте компании, а покупатель управляет работой программы, вводя инструкции на сайте компании. Для получения доходов, сайты, предлагающие услуги снайпинга используют либо модель подписки, либо смешанную модель. В случае использования смешанной модели, покупателю аукциона разрешается сделать несколько снайпов бесплатно, при этом он подвергается воздействию рекламных объявлений, а каждый последующий снайп необходимо оплачивать.

ЗАДАНИЯ ДЛЯ СЕМИНАРСКИХ ЗАНЯТИЙ

1. Сделайте краткий обзор истории виртуального сообщества GeoCities. Отметьте, каким образом на работу этого виртуального сообщества повлияло его приобретение кампанией Yahoo!. Отметьте, какую политику, по отношению к GeoCities проводила компания Yahoo! и по каким причинам виртуальное сообщество GeoCities прекратило своё существование. В чём, по Вашему мнению, заключались ошибки компании Yahoo!, приведшие к закрытию GeoCities, и, что она должна была делать для того чтобы сделать сайт GeoCities коммерчески успешным. Отметьте, что, по Вашему мнению, пользователи GeoCities ожидали получить от работы с сайтом и как деятельность Yahoo! конфликтовала с этими ожиданиями. При поиске материала для обзора используйте англоязычные сайты и статьи.

2. Познакомьтесь с Web сайтами Etsy и We Love Etsy. Сделайте краткий обзор этих сайтов. Объясните, каким образом сайт Etsy и бизнес философия его менеджеров сделали его сайтом социальной сети в дополнение к функции коммерческого сайта, занимающегося онлайновой продажей товаров. Опишите те характеристики покупателей и продавцов сайта Etsy, которые делают социальную сеть, как элемента бизнеса, важным условием успешной работы сайта Etsy. Объясните, как сайт We Love Etsy (который не контролируется сайтом Etsy) может способствовать успеху сайта Etsy.

3. Многие компании используют технологии, на основе мобильных компьютеров, для того чтобы сделать решение рутинных задач более лёгким и эффективным. Представьте себе, что Вы работаете помощником менеджера по продажам в компании, которая продаёт оборудование и запасные части для грузовиков. Продавцы компании совершают командировки для встречи с представителями покупателей. Они останавливаются в отелях, арендуют автомобили и ведут деловые беседы в ресторанах. Ежемесячно продавцы должны предоставлять финансовые отчёты о своих тратах с приложением квитанций, подтверждающих расходы. Продавцы жалуются, что подготовка таких отчётов с использованием бумажных документов занимает много времени. Подберите несколько приложений для мобильных устройств (например, на сайтах Apple App Store и Google Play) которые можно использовать для сканирования квитанций. Сделайте обзор этих приложений и предложите то их них, которое, по Вашему мнению, больше всего подходит для решения описанной задачи.
4. Многие университеты в крупных городах хронически испытывают нехватку парковочного пространства на своих территориях. Типичные группы претендентов на

парковочное пространство в университете представлены студентами, преподавателями, администрацией, рабочими и визитёрами. Каждая из перечисленных групп считает, что она должна иметь наивысший приоритет при распределении парковочного пространства. Представьте себе, что Вам поручено решить проблему распределения парковочного пространства для некоторого университета. Вы пришли к выводу, что решением может быть ежегодное проведение онлайнового аукциона парковочного пространства с использованием университетской интранет. Опишите, каким образом должен быть организован этот аукцион. Не забудьте учесть необходимость в парковочном пространстве для инвалидов, а также тот факт, что рабочие места некоторых работников не обеспечивают им регулярного доступа к компьютеру. К таким работникам относятся уборщицы, садовники и некоторые другие категории рабочих.

5. Представьте, что Вы работаете в отделе снабжения компании, которая производит переключающие устройства, используемые для управления обогревательными и вентиляционными системами в крупных зданиях. Комплектующие изделия, которые приобретает компания, должны точно соответствовать спецификациям и не являются взаимозаменяемыми. Поэтому инженеры компании должны работать с поставщиками для разработки конкретных комплектующих изделий для каждого устройства. Ваш руководитель заинтересован в использовании онлайнового реверсивного аукциона для покупки комплектующих изделий и поручил Вам провести анализ такой возможности. Опишите основные характеристики онлайновых реверсивных аукционов и приведите аргументы «за» и «против» использования онлайновых реверсивных аукционов при решении проблемы снабжения в Вашей компании. Дайте рекомендации по проведению таких аукционов.

6. История использования технологии электронной коммерции в частной коммерческой деятельности может выглядеть следующим образом. Мария живёт в приморском городе и владеет небольшим магазином, продающим коллекционные фарфоровые статуэтки. Основная масса покупателей посещает магазин весной и летом, во время туристического сезона. Осенью и зимой покупателей почти нет. Два года тому назад Мария освоила дополнительный бизнес для осеннего и зимнего периода. Она начала продавать свои товары на сайте аукциона eBay. Мария обнаружила, что продажа товаров на аукционе не только поддерживает её бизнес осенью и зимой, но и позволяет продавать те статуэтки, которыми редко кто интересовался в магазине. Мария пришла к выводу, что товары, которые трудно продать в физическом магазине могут быть легко проданы на онлайновом аукционе. Другим положительным эффектом от участия в онлайновом аукционе является то, что Мария познакомилась с большим количеством коллекционеров и предпринимателями, занимающимися аналогичным бизнесом. Мария решила расширить онлайновую часть своего бизнеса. Она узнала, что eBay позволяет людям создавать онлайновые магазины в пределах своего сайта, и, что аналогичные услуги предлагает Amazon.com. Мария хочет создать свой собственный сайт с фотографиями и подробным описанием товаров, ориентированный на коллекционеров, и найти способ направить заинтересованных посетителей этого сайта на аукцион. Представьте, что Мария пригласила Вас, в качестве консультанта, для развития её идей в области онлайнового бизнеса. Ознакомьтесь с информацией о платформах для онлайновых магазинов eBay Stores и Amazon Marketplace и дайте обоснованные рекомендации, какая из них более всего подходит для бизнеса Марии. Опишите элементы стратегии коммерческого использования социальных сетей, которые Мария могла бы использовать в своём бизнесе.

3. ПРОГРАММНОЕ И АППАРАТНОЕ ОБЕСПЕЧЕНИЕ WEB-СЕРВЕРА

3.1. Web-сервер и Web-клиенты

Архитектура типа «клиент-сервер» используется в компьютерных сетях различных типов и предполагает, что компьютер-клиент запрашивает у компьютера-сервера различные виды обслуживания (печать документов, поиск информации, доступ к базе данных и т.п.), а компьютер-сервер своими ресурсами обеспечивает выполнение этих запросов. Компьютеры-серверы, обычно, обладают бóльшими размерами основной и внешней памяти, а также бóльшей производительностью процессора, по сравнению с компьютерами-клиентами.

Web-сервер это один или несколько компьютеров, предназначенных для размещения Web-сайтов. Web-сервер сконструирован таким образом, чтобы обеспечивать публичный доступ к файлам Web-сайта, которые визуализируются в виде Web-страниц на компьютерах-клиентах посетителей сайта. Web-сайты с большим количеством посетителей используют большое количество Web-серверных компьютеров для эффективного обслуживания своих клиентов. Оперирование большим количеством компьютеров требует синхронизации их деятельности и эффективного разделения рабочей нагрузки между компьютерами.

Когда кто-либо использует Web-браузер, для работы с Web, его компьютер приобретают статус Web-клиента мировой клиент-серверной сети. Таким образом, Web-браузер является тем программным обеспечением, которое обеспечивает компьютеру статус Web-клиента.

Интернет связывает компьютеры, и другое оборудование, которые имеют различную архитектуру и управляются различными операционными системами. Способность компьютерной сети коммутировать оборудование, использующее различные операционные системы называется *нейтральностью платформы* (platform neutrality). Нейтральность платформы Web позволяет *разнотипному оборудованию* соединяться друг с другом и обмениваться данными. Нейтральность платформы Web является одним из факторов её быстрого развития. Рис. 3.1 иллюстрирует платформенную нейтральность Web.

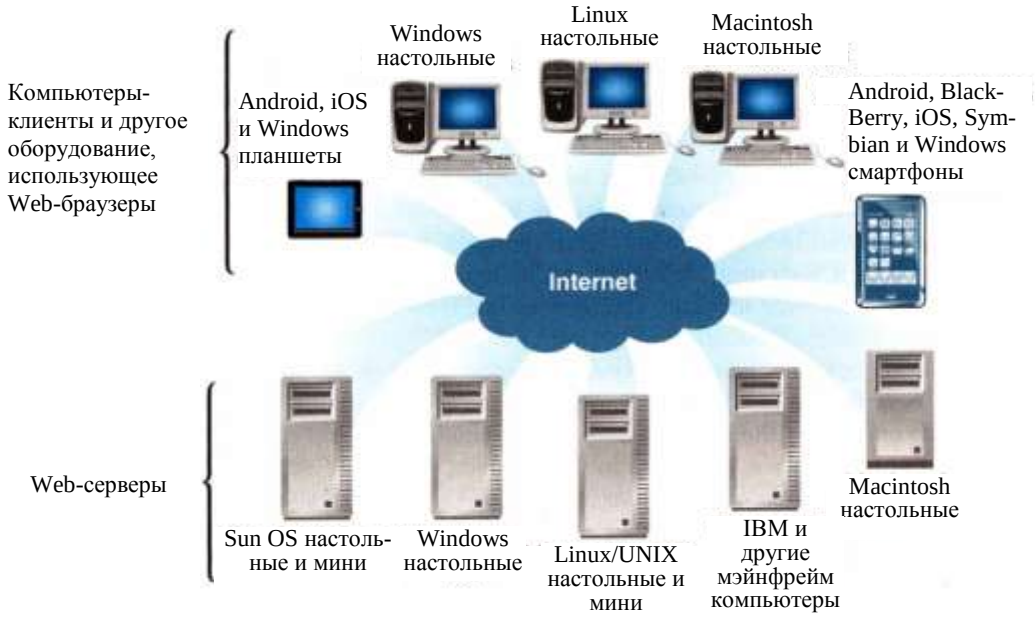

Рис. 3.1. Платформенная нейтральность Web

Основная задача, которую решает архитектура Web-сервера, заключается в обслуживании запросов на передачу страниц Web-сайта, размещенного на Web-сервере, на

клиентский компьютер. Архитектура Web-сервера рассматривается как композиция аппаратного обеспечения, операционной системы и прикладного программного обеспечения Web-сервера. Архитектура Web-сервера проектируется исходя из оценки наибольшего количества посетителей, одновременно работающих с сервером, количества страниц, которые посетитель будет просматривать в течение одного визита и размера страниц с учетом графических и звуковых файлов.

В первые годы существования электронной коммерции, основная часть коммерческого Web-сайта представляла собой фиксированный набор Web-страниц, описывающих продукты, предлагаемые компанией. Сегодня коммерческие сайты формируют персонализированные страницы, соответствующие конкретным потребностям посетителей.

3.1.1. Динамические Web-страницы

Динамической Web-страницей (dynamic Web-page) будем называть Web-страницу, которая не храниться в готовом виде на Web-сервере, а формируется динамически в ответ на интерактивные действия пользователя. В противоположность динамической странице, *статическая Web-страница* (static Web-page) храниться в готовом виде и считывается из одного или нескольких файлов, находящихся на Web-сервере. Динамическая генерация страниц позволяет Web-серверу сформировать персонализированную страницу с содержимым, адаптированным к запросу клиента. Очень часто текст, графика, форма для ввода данных и другие элементы страницы должны формироваться в соответствии с запросами клиента. Например, если клиент запрашивает информацию о текущем статусе своего заказа, то страница, содержащая запрашиваемую информацию, должна адаптироваться к текущей ситуации и формироваться динамически.

Для создания динамических страниц используются два подхода. Первый подход называется «*сценарий на стороне клиента*» (client-side scripting) и предполагает, что браузер изменяет то, что отображается на Web-странице, в ответ на действия пользователя (такие, как «клик» манипулятором «мышь» или ввод данных при помощи клавиатуры). Изменения осуществляются браузером в соответствии со сценарием, написанным на таких языках как JavaScript или Adobe Flash. Браузер получает код сценария от Web-сервера. Код сценария, используя введенные пользователем данные, инструктирует браузер о том какие элементы страницы нужно запросить у Web-сервера и каким образом отобразить их на странице.

Второй подход, называется «*сценарий на стороне сервера*» (server-side scripting) и предполагает, что программа, находящаяся на Web-сервере, динамически формирует страницу, используя информацию, полученную от браузера пользователя. Эта информация может включать: данные введенные пользователем в поля ввода при помощи клавиатуры; тип браузера пользователя; или, просто, выдержку времени. Например, если клиент авторизовался на сайте банковской системы, а затем в течение некоторого времени не предпринял никаких действий, то Web-сервер может прервать связь и переслать браузеру сообщение о том, что сеанс завершен. Во всех случаях использования подхода «сценарий на стороне сервера», комбинируется HTML-тегированный текст и сценарий.

Наиболее популярные инструментальные программы, используемые для создания динамических страниц на стороне сервера, включают: (1) ASP.Net компании Microsoft; (2) Hypertext Preprocessor (PHP) организации Apache Software Foundation; (3) ColdFusion компании Adobe; (4) JavaServerPages (JSP) компания Sun Microsystems.

AJAX (Asynchronous JavaScript And XML) представляет собой инструментальную систему, предназначенную для разработки интерактивных Web-сайтов. Большинство Web-страниц должны полностью перезагружаться при изменении их содержимого в браузере. AJAX позволяет программисту создавать страницы, которые обновляются асинхронно, путём обмена с сервером небольшим количеством данных, в то время как основная часть страницы продолжает отображаться в окне браузера. В классическом варианте работы с Web-станицей выполняется следующая последовательность действий:

- пользователь заходит на страницу и «кликает» какой-либо её элемент;
- браузер формирует запрос и отправляет его серверу;

- сервер формирует совершенно новую Web-страницу и возвращает её обратно браузеру, после чего браузер полностью перезагружает всю страницу.

При использовании AJAX последовательность действий усложняется:

- пользователь заходит на страницу и «кликает» какой-либо её элемент;
- сценарий на стороне браузера (на языке JavaScript) определяет, какая информация нужна для обновления страницы;
- браузер формирует соответствующий запрос и отправляет его серверу;
- сервер формирует и возвращает только ту часть страницы, на которую пришёл запрос;
- сценарий на стороне браузера вносит изменения в страницу с учётом полученной информации без её полной перезагрузки.

Примером динамических Web-страниц, созданных при помощи AJAX, являются страницы, генерируемые приложением Google Maps.

3.1.2. Множественность значений понятия «сервер»

Термин «сервер» не имеет единственного значения, а используется в нескольких различных смыслах. В общем случае сервер это – компьютер, или несколько компьютеров, которые используются для предоставления своих данных или программ другим компьютерам, подключенным к серверу посредством компьютерной сети. Программы, которые использует сервер для реализации своих функций, называют *серверным программным обеспечением* (server software). Серверное программное обеспечение может быть частью операционной системы, управляющей работой сервера.

Некоторые серверы обслуживают не только свою локальную компьютерную сеть, но подключены к Интернет при помощи роутеров. Такие серверы, кроме серверного программного обеспечения, обслуживающего локальную сеть, используют дополнительные *Web-серверное программное обеспечение* (Web-server software), предназначенное для обеспечения публичного доступа к файлам сервера со стороны других компьютеров, подключенных к Интернет. В этом случае сервер приобретает статус Web-сервера.

«Серверная» терминология используется, применительно к компьютерам, которые обеспечивают обработку электронной почты, либо к компьютерам, которые реализуют функции управления базами данных. Сервер, который управляет входными и выходными потоками электронных почтовых сообщений, часто называю *почтовым сервером* (e-mail server), а программное обеспечение, которое реализует функции почтового сервера – *программным обеспечением почтового сервера* (e-mail server software). Сервер, на котором размещено программное обеспечение, управляющее доступом к базам данных, часто называют *сервером базы данных* (database server). Сервер, на котором компания эксплуатирует программное обеспечение, предназначенной для обработки платежа и бухгалтерского учёта часто называют *сервером транзакций* (transaction server).

Таким образом, термин «сервер» используется для обозначения нескольких типов компьютеров и их программного обеспечения, используемых для организации систем электронного бизнеса. Единственным способом определения точного смысла термина «сервер» является анализ контекста, в котором этот термин употребляется.

3.1.3. Модели типа «клиент-сервер» в Web

Когда кто-либо использует браузер для посещения Web-сайта коммерческой компании, то браузер (Web-клиент) запрашивает файлы у Web-сервера компании, которая оперирует этим сайтом. Используя Интернет, как среду для транспортировки данных, браузер, вначале, форматируется запрос в соответствии с протоколом HTTP (Hypertext Transfer Protocol), а затем пересылает его через Интернет на компьютер-сервер. Сервер, получив запрос, разыскивает файл, содержащий Web-страницу, или другую информацию, запрашиваемую клиентом, форматирует её в соответствии с HTTP, и отсылает обратно клиенту через Интернет.

Когда на клиентский компьютер поступает ответ от сервера (файл, состоящий из гипертекстовых элементов и HTML-тегов), то он используется браузером для формирования Web-страницы и отображения её в окне браузера. В некоторых случаях один запрос клиента порождает ответы с десятков и, даже сотен отдельных серверных компьютеров для того, чтобы собрать запрашиваемую информацию. Страница, содержащая большое количество графических и других объектов может медленно появляться в окне браузера, поскольку каждый объект (каждый мультимедийный файл) требует отдельного запроса и ответа.

Базовая модель типа «клиент-сервер» в Web является *двухуровневой* (two-tier) и предполагает обмен сообщениями между одним клиентским компьютером и одним Web-сервером. Конечно, в транспортировке пакетов через Интернет участвует множество промежуточных компьютеров-маршрутизаторов, однако в двухуровневой модели сообщение формируется только одним клиентом и передается только одному серверу. Рис. 3.2 иллюстрирует потоки сообщений в двухуровневой модели «клиент-сервер» в Web.

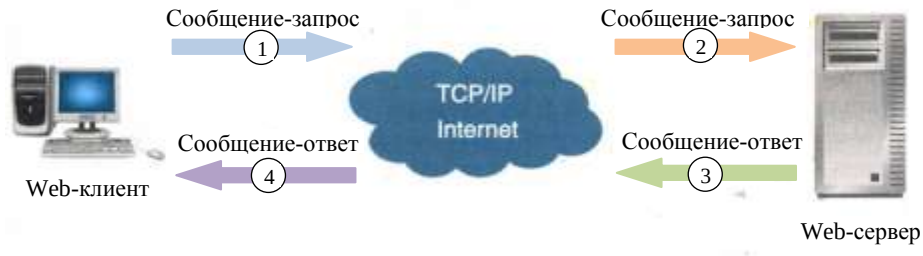

Рис. 3.2. Потоки сообщений в двухуровневой модели «клиент-сервер» в Web

Сообщение, при помощи которого Web-клиент запрашивает файл у Web-сервера, называется *сообщение-запрос* (request message). Сообщение-запрос состоит из трёх частей: (1) стартовая строка запроса; (2) заголовки запроса; (3) тело объекта.

Стартовая строка запроса (request line) является обязательной частью запроса и содержит команду запроса, имя целевого ресурса на сервере (имя файла и описание пути к этому файлу), а также имя и номер версии протокола HTTP. *Заголовки запроса* (request headers) являются необязательной частью запроса и могут содержать информацию о типах файлов, которые клиент должен получить в ответ на запрос. *Тело объекта* (entity body) также является необязательной частью запроса и может использоваться для передачи некоторого количества информации от клиента к серверу.

Когда сервер получает сообщение-запрос, он выполняет команду запроса и, в случае её успешного выполнения, пересылает клиенту файл с запрашиваемой Web-страницей. Сервер разыскивает файл с Web-страницей либо на собственном диске, либо на дисках компьютеров, подключенных к сети. Затем сервер создаёт и форматирует *сообщение-ответ* (response message) для передачи его клиенту. Сообщение-ответ также состоит из трёх частей: (1) строка заголовка ответа; (2) один или несколько полей заголовка ответа; (3) необязательное тело объекта.

Строка заголовка ответа (response header line) содержит версию HTTP, используемую сервером, статус ответа (найден или нет файл, запрашиваемый клиентом) и объяснение информации о статусе ответа. *Поля заголовка ответа* (response header fields) следуют за строкой заголовка и содержат информацию, описывающие атрибуты сервера. *Тело объекта* (entity body) возвращает HTML страницу, запрашиваемую клиентом.

Двухуровневая модель типа «клиент-сервер» хорошо работает в случае транспортировки статических Web-страниц, однако не справляется с транспортировкой динамических страниц, а также обработкой и учетом бухгалтерских транзакций. *Трёхуровневая* (three-tier) модель типа «клиент-сервер» в Web является дальнейшим развитием двухуровневой модели и используется в тех случаях, когда необходимо осуществлять дополнительную работу по формированию ответа сервера перед отправкой его клиенту. Примером такой дополнительной работы может быть обращение к базе данных для получе-

ния информации, необходимой для формирования сообщения-ответа. Поэтому, часто, третий уровень включает сервер базы данных с соответствующим программным обеспечением. Например, Web-сайт онлайнового магазина может строиться на базе Web-каталога с описанием продаваемых товаров. Такой Web-каталог должен подвергаться перманентному редактированию и, поэтому, информацию о товарах удобно хранить в базе данных. В этом случае программное обеспечение сервера базы данных должно обеспечивать функции поиска, обновления и отображения информации, хранящейся в каталоге.

Предположим, что клиент, работающий с сайтом магазина, запрашивает подробную информацию о конкретном товаре. Браузер клиентского компьютера форматирует этот запрос в виде HTTP сообщения-запроса (уровень 1) и пересылает его на Web-сервер через Интернет. Web-сервер (уровень 2) анализирует полученный запрос и определяет, что для формирования ответа необходима помощь сервера базы данных. Поэтому, Web-сервер формирует и посылает запрос серверу базы данных (уровень 3) для поиска информации о конкретном товаре. Полученная информация возвращается Web-серверу, который формирует HTTP сообщение-ответ и пересылает его клиенту через Интернет.

Рис. 3.3 иллюстрирует потоки сообщений в трёхуровневой модели типа «клиент-сервер» в Web.

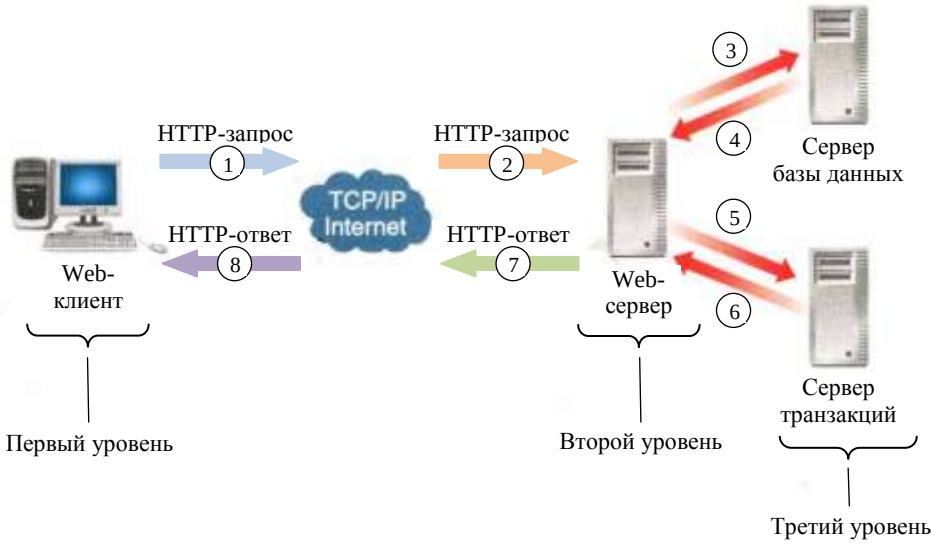

Рис. 3.3. Потоки сообщений в трёхуровневой модели «клиент-сервер» в Web

В Web используются модели «клиент-сервер», которые включают четыре, пять и более уровней. В четырёхуровневой архитектуре, например, на четвёртом уровне могут размещаться прикладные программы, которые генерируют информацию необходимую для работы сервера транзакций (третий уровень), который, в свою очередь, генерирую информацию для Web-сервера (второй уровень). Модели «клиент-сервер», которые включают более трёх уровней, часто называют *n-уровневыми*. Онлайновый магазин, использующий n-уровневую модель, может отслеживать товары, находящиеся в тележке для покупок; разыскивать необходимые уровни налогов на продажу; отслеживать предпочтения покупателя; обновлять базу данных товаров, находящихся на складе и актуализировать каталог онлайнового магазина.

3.2. Программное обеспечение Web-серверов

Некоторое Web-серверное программное обеспечение предназначено для работы на компьютере, который управляется конкретной операционной системой, однако сущест-

вует Web-серверное программное обеспечение, которое может работать на компьютерах, управляемых различными операционными системами.

3.2.1. Операционные системы Web-серверов

Основной задачей операционной системы является *управление* последовательностью выполнения программ и выделение им необходимых компьютерных ресурсов, таких как процессор, основная и внешняя память. Операционные системы также управляют взаимодействием программы с периферийным оборудованием компьютера, таким как клавиатура, обычный монитор, либо сенсорный экран и принтер. В случае многопользовательского режима работы программы, операционная система отслеживает всех пользователей, которые подключены к программе и обеспечивает их независимую работу.

Web-серверные программы работают под управлением таких операционных систем как Microsoft Windows Server, а также Linux, или других UNIX-подобных операционных систем (например, FreeBSD). Некоторые коммерческие компании считают, что их персоналу легче освоить и обслуживать продукты компании Microsoft (операционную систему Microsoft Windows Server и облачную платформу), чем UNIX-подобные операционные системы. Однако эксперты, часто, критикуют слабую безопасность и уязвимость Web-серверов, работающих под управлением операционных систем компании Microsoft. Поэтому Web-сервера, работающие под управлением UNIX-подобных операционных систем, используются чаще, а UNIX считается наиболее безопасной операционной системой для организации Web-сервера.

Linux является быстрой, эффективной и легко инсталлируемой операционной системой, находящейся в свободном доступе. Большое количество компаний, продающих компьютеры для организации Web-серверов, включают операционную систему Linux в базовую конфигурацию компьютеров. Несмотря на то, что операционная система Linux находится в свободном доступе, компании часто покупают её через коммерческих дистрибьюторов. В этом случае компания получает дополнительные продукты и услуги, такие, например, как инсталляционная утилита, а также, контракт на обслуживание. Наиболее известными коммерческими дистрибьюторами операционной системы Linux являются компании Mandriva Linux, Red Hat и SUSE Linux Enterprise.

Компания Oracle продает аппаратное обеспечение для Web-серверов вместе с UNIX-подобной операционной системой Solaris. Дополнительную информацию о программных продуктах, находящихся в свободном доступе можно найти на сайте организации Open Source Initiative.

3.2.2. Web-серверное программное обеспечение

В настоящем подразделе приведены краткие сведения о двух наиболее популярных Web-серверных программ: Apache HTTP Server и Microsoft Internet Information Server (IIS). Кроме отмеченных Web-серверных программ используются также: nginx (произносится «engine-x») и lighttpd (произносится «lighty»). Некоторые крупные онлайновые компании разработали своё собственное Web-серверное программное обеспечение. Например, компания Google разработала программу Google Web Server, работающую под управлением операционной системы Linux, которую она использует на миллионах своих серверных компьютерах. Рис. 3.4 иллюстрирует использование Web-серверного программного обеспечения действующими сайтами по состоянию на начало 2014 года.

В последние годы, после нескольких лет стабильности, рынок Web-серверного программного обеспечения начал меняться. Программа Apache, ранее занимавшая более половины рынка, уменьшила свою долю до 44%. Программа Microsoft IIS, ранее занимавшая от 10% до 20% рынка, увеличила своё присутствие до 24% рынка. Неуклонно растёт использование открытой программы nginx и сегодня эта программа занимает не менее 14% рынка. Программу Google Web Server использует только компания Google, однако, поскольку Google эксплуатирует огромное количество Web-серверных компьютеров по всему миру, эта программа занимает примерно 5% рынка.

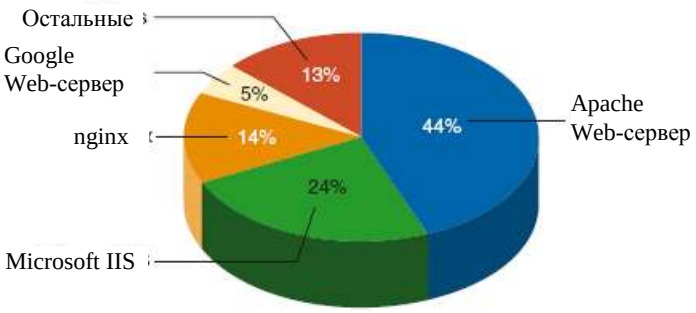

Рис. 3.4. Использование Web-серверного программного обеспечения действующими сайтами

Apache HTTP Server

Apache является продолжающимся проектом, который развивается благодаря усилиям большого количества специалистов. Первую версию программы Apache предложил Роб Маккул (Rob McCool) из университета в штате Иллинойс (США) в 1994 году. Остальные разработчики, работавшие в различных странах, создали свои собственные расширения и сформировали рабочую группу по дальнейшему совершенствованию и развитию Apache. Дополнения, вносимые в Web-серверную программу, известные как «patches» (заплатки) координировались всеми участниками группы при помощи электронной почты. В итоге, структура сервера Apache сформировалась в виде ядра с большим количеством дополнений-заплаток. Поэтому, через некоторое время, сервер стал известен как «a patchy server» или Apache. Программу Apache можно получить бесплатно в Web, как продукт свободного доступа.

Apache HTTP Server начал доминировать в Web начиная с 1996 года, поскольку он бесплатен, эффективно реализует свои функции и поддерживается большим количеством грамотных пользователей, оказывающих консультационные услуги при помощи консультационных форумов, wiki-статей и блогов. Одним из достоинств Apache является возможность работы под управлением большинства современных операционных систем: FreeBSD-UNIX, HP-UX, Linux, Microsoft Windows, SCO-UNIX, и Solaris. Большое количество компаний продают сервисные программы для Apache тем организациям, которые, например, хотят обеспечить дополнительную безопасность. Однако, в большинстве случаев, инсталляция и обслуживание сервера Apache осуществляется техническим персоналом самостоятельно благодаря обширной информационной поддержки, которую можно получить в Web.

Microsoft Internet Information Server

Web-серверная программа Microsoft Internet Information Server (IIS) работает только под управлением операционной системы Microsoft Windows Server и продаётся в одном пакете с этой операционной системой. Программа IIS используется во многих корпоративных интранет сетях, поскольку многие коммерческие компании используют продукты компании Microsoft как стандартные. Программа IIS бесплатна, однако, операционная система Microsoft Windows Server, в пакете с которой поставляется IIS, стоит единицы либо десятки тысяч долларов в зависимости от размера организации и количества Web-серверов. Программа IIS поддерживает технологию ASP (Active Server Pages), позволяющую создавать динамические Web-страницы.

3.3. Электронная почта

Несмотря на то, что Web, и взаимодействие Web-серверов и Web-клиентов является наиболее важной технологией используемой сегодня в электронной коммерции, множе-

ство покупателей и продавцов используют также электронную почту для сбора информации, осуществления транзакций и решения других задач онлайнового бизнеса.

3.3.1. Преимущества электронной почты

Электронная почта была не только первым Интернет приложением, она также послужила одной из причин привлечения внимания большого количества людей к практическому использованию Интернет. Электронная почта доставляет сообщения от отправителя к получателю за несколько секунд. Электронное сообщение может содержать символьный текст, аналогичный тому, которым оперируют текстовые редакторы, а также добавленные файлы документов, графических изображений, аудио, видео, таблиц и других данных. Эти добавленные файлы часто являются наиболее важной части электронного сообщения. Сегодня электронная почта является наиболее популярным средством деловой коммуникации, во много раз более популярным, чем все остальные средства коммуникации вместе взятые.

3.3.2. Недостатки электронной почты

Несмотря на большое количество преимуществ, электронная почта обладает некоторыми недостатками. Одно из неудобств, связанных с электронной почтой, заключается в том, что менеджеры вынуждены ежедневно тратить значительную часть своего времени, отвечая на сообщения электронной почты. Среднее время, которое менеджер тратит на подготовку ответа на одно сообщение, составляет пять минут. Некоторые сообщения, не представляющие интереса, могут быть удалены за несколько секунд, однако для ответа на важные сообщения часто требуется работа с дополнительной информацией, занимающая значительное время. Исследования показывают, что большинство людей находят работу по подготовке ответов на электронные сообщения обременительной в том случае, если им ежедневно приходится отвечать на 20 или 30 сообщений, что отнимает примерно два часа рабочего времени.

Вторым неудобством и опасностью, связанной с электронной почтой являются компьютерные вирусы, представляющие собой небольшие программы, которые могут прикрепляться к другим программам и вызывать повреждение данных и программ, размещенных на компьютере, в том случае если активируется «заражённая» программа. Компьютерные вирусы, обычно, содержатся в файлах, добавленных к электронному сообщению. Необходимость использования антивирусных программ и соблюдение специальных мер безопасности, при работе с электронной почтой, является платой за её удобство.

Изучая вопросы маркетинга на основе электронной почты (см. подраздел 4.5 конспекта лекций по дисциплине Электронная коммерция) мы отмечали негативную роль спама в успешном функционировании этого вида маркетинга. Спам, известный также как *незапрашиваемая коммерческая электронная почта*, представляет собой информационный мусор, рассылаемый в виде электронных сообщений. Сегодня спам является одним из самых неприятных недостатков электронной почты. Борьба со спамом, как правило, требует значительных временных и финансовых ресурсов.

3.3.3. Спам

Рис. 3.5 иллюстрирует долю спама в сообщениях электронной почты, получаемых почтовыми серверами коммерческих компаний в период с 1995 и по 2013 годы. Размер проблемы спама значителен. Согласно имеющимся данным в 2009 году (пик активности спама) отсылалось примерно 220 миллиардов спам-сообщений в сутки.

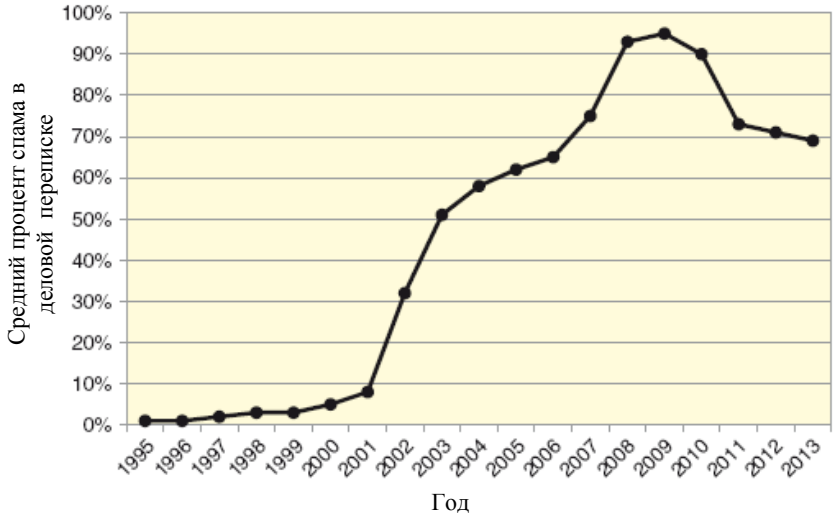

Рис. 3.5. Доля спама в деловой переписке

Исследования показывают, что рост доли спама в деловой переписке постепенно снижается и, что в будущем технические решения этой проблемы резко снизят долю спам-сообщений в общем трафике сообщений электронной почты. Сегодня, большое количество компаний предлагают программное обеспечение, предназначенное для размещения на почтовом сервере и ограничивающее передачу спам-сообщений в почтовые ящики клиентов. Хотя индивидуальные пользователи электронной почты могут инсталлировать программы, фильтрующие спам, и на клиентских компьютерах, (либо устанавливать спам-фильтры в самих клиентских программах), большинство компаний считает более эффективным и дешёвым способом борьбы со спамом, удаление спам-сообщений ещё до того как они попали в почтовый ящик клиента.

3.3.4. Решения проблемы спама

До тех пор, пока стоимость рассылки сообщений электронной почты (и, следовательно, спама) будет оставаться низкой, прибыль, получаемая спамерами, будет делать рассылку спама привлекательным бизнесом. Разработаны несколько различных подходов, используемых для ограничения спама и его влияния на электронную коммерцию. Некоторые из этих подходов требуют принятия законов, а некоторые – технических изменений в системах управления электронной почтой. Существуют подходы, направленные на борьбу со спамом, которые могут быть внедрены в рамках существующих законов и технологий, но при условии кооперации большого количества коммерческих компаний и организаций. Несколько стратегий, позволяющих уменьшить количество спама, предназначены для использования индивидуальными пользователями электронной почты.

Антиспамовские стратегии для индивидуальных пользователей

Один из способов, лимитирующих спам для индивидуальных пользователей, заключается в создании такого адреса электронной почты, который уменьшает вероятность его автоматической генерации. Многие организации создают электронные адреса своих сотрудников путем комбинации элементов имени и фамилии. Например, комбинируются первая буква имени и полная фамилия сотрудника. Крупные компании, с большим количеством сотрудников, обычно, комбинируют полное имя с полной фамилией. Поэтому, спамер, получивший доступ к списку сотрудников, может автоматически сгенерировать список потенциальных адресов электронной почты всех сотрудников. Стоимость рассылки одного электронного сообщения настолько низкая, что спамер может позволить себе разослать тысячи сообщений по случайным образом сгенерированным, адресам в надежде на то, что несколько адресов окажутся правильными. Если пользователь создаёт более

сложный адрес электронной почты, такой например, как xq7yy23@mycompany.com, он, тем самым, уменьшает вероятность автоматической генерации своего адреса. Недостатком этого способа является то, что сложный адрес трудно запомнить и это несколько снижает удобство использования электронной почты как средства коммуникации.

Второй способ борьбы со спамом, который может применять индивидуальный пользователь, заключается в контроле за частотой появления адреса электронной почты в Web. Спамеры используют софтботы (программные роботы) для поиска в Web строк символов, содержащих символ «@», который включён в каждый адрес электронной почты и является его признаком. Софтботы сканируют Web-страницы, блоги, дискуссионные панели, чат-комнаты и другие онлайновые ресурсы, которые включают адреса электронной почты. Как было отмечено выше, спамер может позволить себе разослать тысячи сообщений по адресам, собранным таким образом. Если на эту рассылку откликнутся только один или два человека, спамер будет иметь прибыль, поскольку стоимость рассылки одного сообщения очень мала.

Некоторые индивидуальные пользователи, с целью противодействия спаму, регистрируют множество адресов электронной почты. Один адрес может использоваться для его отображения на страницах собственного сайта, другой при регистрации для получения доступа к страницам других сайтов, ещё один при шопинге, и т.д. Если спамер начинает активно рассылать спам на один из адресов, пользователь прекращает его использовать и переключается на другие. Компании, оказывающие услуги Web-хостинга, часто, предлагают большое количество (от 100 до 200) адресов электронной почты как часть своего сервиса, что может быть полезной антиспамовской стратегией для небольших онлайновых компаний, владеющих собственным сайтом.

Перечисленные стратегии направлены на ограничение доступа спамера к адресу электронной почты. Другие подходы используют одну или несколько технологий фильтрации сообщений в зависимости от их контента.

Базовые контентные фильтры

Контентная фильтрация (content-filtering) спама предполагает использование программного обеспечения способного выделять признаки спама в приходящих электронных сообщениях. Технологии контентной фильтрации спама отличаются тем, какие элементы контента они анализируют и тем насколько строго они применяют правила классификации сообщений. Большинство контентных фильтров разыскивают признаки спама в заголовках электронных сообщений: строки «От», «Кому» и «Тема».

Программное обеспечение, осуществляющее контентную фильтрацию спама, размещается либо на клиентском компьютере (фильтрация на клиентском уровне), либо на компьютере почтового сервера (фильтрация на серверном уровне). *Фильтрацию на серверном уровне* (server-level filtering) может осуществлять либо почтовый сервер Интернет провайдера, либо собственный почтовый сервер коммерческой компании. Часто фильтрация на серверном уровне дополняется *фильтрацией на клиентском уровне* (client-level filtering). Спам, который прошел через один фильтр может быть отфильтрован другим фильтром.

Программы, осуществляющие контентную фильтрацию спама, работают либо на основе «*чёрных списков*» (black lists), либо на основе «*белых списков*» (white lists). Фильтры, работающие на основе чёрных списков, анализируют строку заголовка «От» и проверяют не является ли отправитель одним из спамеров, перечисленных в чёрном списке. Если сообщение отправлено с адреса спамера, то оно либо удаляется, либо помещается в отдельный почтовый ящик для последующей ревизии получателем. Фильтры, работающие на основе чёрных списков, могут использоваться как на серверном, так и на клиентском уровнях. Некоторые организации, например Spam and Open Relay Blocking System, формируют чёрные списки и распространяют их бесплатно среди администраторов Интернет провайдеров. Организация Spamhaus Project выявляет известных спамеров, публикуют списки почтовых серверов, которые они используют и подробную информацию о нарушениях закона, необходимую правоохранительным органам. Главный недостаток

фильтрации на основе чёрных списков заключается в том, что спамеры часто меняют свои почтовые сервера. Это означает, что чёрные списки должны постоянно обновляться, а для их обновления необходима кооперация большого количества организаций.

Фильтры, работающие на основе белых списков, также анализируют строку заголовка «От» и проверяет, находится ли адрес отправителя в белом списком, который содержит адреса, с которых можно получать сообщения (например, адреса, перечисленные в адресной книге). Фильтры, работающие на основе белых списков, обычно, используются на клиентском уровне, однако могут использоваться и на уровне сервера, если администратор почтового сервера имеет доступ к адресным книгам всех сотрудников (некоторые компании, в целях безопасности, требуют обеспечить такой доступ). Главный недостаток фильтрации на основе белых списков заключается в том, что во время фильтрации могут удаляться полезные сообщения от неизвестных адресатов и не являющиеся спамом. Поскольку количество таких полезных сообщений может быть значительно, отфильтрованные сообщения не удаляются, а помещаются в отдельный почтовый ящик для последующей ревизии.

Оба типа фильтров имеют существенные недостатки и для уменьшения влияния этих недостатков на процесс фильтрации, часто оба фильтра используются одновременно или в комбинации с другими подходами борьбы со спамом.

Контентные фильтры с запросом и подтверждением

Техника контентной фильтрации, называемая *контентная фильтрация с запросом и подтверждением* (challenge-response content filtering) использует белые списки. Фильтрация с запросом и подтверждением предполагает, что адреса отправителей всех входящих сообщений сравниваются с адресами в белом списке. Если сообщение пришло от отправителя, адрес которого отсутствует в белом списке, ему автоматически отправляется сообщение-запрос, содержащее небольшую задачу. Отправитель должен решить задачу и правильно ответить на полученный запрос.

Задача сформулирована таким образом, что её может легко решить человек, но не компьютерная программа. Например, запрос может представлять собой картинку, на которой изображены различные фрукты, а в ответе нужно указать точное количество яблок. Пример запроса, использующего изображения искаженных символов (5BM6HW3F) приведен на рис. 3.6.

Рис. 3.6. Пример запроса, использующего изображение искаженных символов

Основной недостаток фильтров с запросом и подтверждением заключается в том, что их работу можно использовать для блокировки электронной почты любого пользователя, выбранного в качестве жертвы. Злоумышленник может отослать тысячи сообщений получателям, использующих фильтры с запросом и подтверждением, и указать в строке «От» заголовка адрес получателя-жертвы. В этом случае получатель-жертва подвергнется бомбардировке огромного количества автоматически сгенерированных сообщений-запросов. Потенциальный вред такой тактики тем больше, чем больше почтовых серверов устанавливают фильтры с запросом и подтверждением.

Поскольку фильтры с запросом и подтверждением требуют от пользователей изменения поведения при работе с электронной почтой, и не обеспечивают немедленного и

существенного эффекта (уменьшение количества получаемых спам-сообщений) они не получили широкого распространения.

Расширенные контентные фильтры

Расширенные контентные фильтры (advanced content filters), анализирующие всё сообщение, а не только его заголовок или IP-адрес отправителя, могут работать более эффективно, чем базовые контентные фильтры. Однако, разработка таких фильтров является сложной задачей. Например, коммерческая компания может решить, что необходимо удалять все сообщения содержащие слово «sex», но, при этом, автоматически будут удаляться сообщения от клиентов из английского графства Essex.

Многие расширенные контентные фильтры работают путём поиска признаков спама во всём сообщении. Когда фильтр обнаруживает признак спама в сообщении, он увеличивает спам-балл этого сообщения. Некоторые признаки увеличивают спам-балл на бóльшую величину, чем другие. Признаками спама могут быть отдельные слова, словосочетания, HTML-коды (такие как код белого цвета, который делает часть сообщения невидимой для большинства почтовых клиентов), а также информация о том, в каком месте сообщения встречается слово. К сожалению, как только разработчики расширенных фильтров, идентифицируют хороший набор признаков спама, спамеры перестают включать эти признаки в свои сообщения.

Один тип расширенных контентных фильтров, базирующийся на разделе прикладной математики, именуемой *Байесовская статистика*, демонстрирует качества, которые не могут обойти спамеры. Так называемый, *Байесовский классификатор* базируется на использовании дополнительные знаний для модификации вероятностных оценок, сделанных ранее. Общеупотребительный контентный фильтр спама на основе Байесовского классификатора, называется *наивный Байесовский фильтр* (naive Bayesian filter). Работа этого фильтра начинается с того, что все сообщения имеют одинаковый статус и не классифицированы. Далее происходит процесс обучения фильтра. Пользователь, ознакомившись с сообщением, информирует фильтр, относится ли это сообщение к категории спам-сообщений или нет. Фильтр постепенно обучается (путем модификации вероятностных оценок того, что элементы сообщения появляются в спам-сообщениях) идентифицировать спам-сообщения.

После просмотра нескольких десятков сообщений, наивный Байесовский фильтр идентифицирует спам в 80% случаев. В процессе работы фильтра пользователь сообщает ему о всех допущенных ошибках. В итоге, после просмотра нескольких сотен сообщений, и, с учётом информации о допущенных ошибках, фильтр идентифицирует спам в 95% случаев. Недостатком наивного Байесовского фильтра можно считать необходимость его обучения в течение некоторого времени. Обучение должно осуществляться индивидуальным пользователем, поскольку то, что для одного пользователя является спамом, для другого может быть важным сообщением. Индивидуальное обучение является ограничением на распространение наивного Байесовского фильтра.

Наивный Байесовский фильтр может быть установлен для защиты клиентского компьютера теми пользователями, которые получают большое количество сообщений и работают в организациях или компаниях, осуществляющих фильтрацию спама на серверном уровне. Программа POPFile является примером программы, находящейся в свободном доступе и работающей как наивный Байесовский фильтр. Программа предназначена для инсталляции на клиентских компьютерах.

Правовые решения

Борьба с распространением спама ведётся на правовом уровне. Рассмотрим, каким образом законодатели пытаются ограничить спам на примере американского закона, известного под наименованием CAN-SPAM (Controlling the Assault of Non-Solicited Pornography And Marketing). Закон вступил в силу в 2004 году. В последующие два месяца после вступления закона в силу наблюдалось уменьшение количества спам-сообщений, од-

нако на третий месяц их количество вернулось на прежний уровень. Вначале спамеры приостановили свою активность, однако, возобновили её в прежнем объеме, обнаружив отсутствие широкомасштабных судебных преследований в соответствии с этим законом.

Закон CAN-SPAM регламентирует сообщения электронной почты, рассылаемые с целью рекламирования и продвижения коммерческих товаров или услуг, и включает следующие основные положения.

- *Вводящий в заблуждение адрес, указанный в заголовке*: Адрес, указанный в заголовке и информация о маршруте, включающая доменное имя и адрес отправителя должны быть точными и идентифицировать личность, отправляющую сообщение.
- *Обманчивая строка «Тема», указанная в заголовке*: Строка «Тема» в заголовке сообщения не должна вводить в заблуждение получателя сообщения относительно его содержания.
- *Ясное и легко заметное уведомление о характере сообщения*: Сообщение должно содержать ясное и легко заметное уведомление о том, что является рекламой или ходатайством и, что получатель может отказаться от дальнейшего получения коммерческих сообщений от отправителя.
- *Физический почтовый адрес*: Сообщение должно содержать действующий физический почтовый адрес отправителя.
- *Обязательное положение о механизме отказа*: Сообщение должно включать адрес электронной почты или другие Интернет ориентированные механизмы, позволяющие получателю отослать запрос с отказом от сообщений. Этот запрос должен уважаться отправителем. Сообщение может включать меню, позволяющее получателю отказаться от некоторых типов сообщений, но один из пунктов меню должен означать отказ от всех типов сообщений.
- *Эффективность механизма отказа*: Запрос с отказом от сообщений должен быть выполнен в течение 10 рабочих дней. Любой предлагаемый механизм отказа должен действовать в течение, по крайней мере, 30 дней после отправки сообщения. После того, как получен запрос на отказ, отправителю запрещается помогать, кому бы то ни было, отправлять сообщения на адрес, с которого получен отказ.
- *Передача адресов электронной почты*: После того как получатель отослал запрос об отказе, отправителю запрещается продавать или передавать адрес электронной почты получателя кому бы то ни было.

Закон, также, запрещает использование вводящего в заблуждение адреса в заголовке сообщений, имеющих отношение к коммерческим транзакциям. Все сообщения, связанные с транзакциями попадают под действие положений этого закона. Каждое нарушение закона наказывается штрафом в размере до 11000 долларов США. Дополнительными штрафами наказывается те, кто нарушает, приведенные ниже положения и осуществляет следующее.

- Использует адреса электронной почты, полученные на Web-сайтах на которых размещено предупреждение о запрете использования электронного адреса с целью рассылки сообщений.
- Отсылает сообщения по адресам, которые были сгенерированы путем комбинации имён, фамилий и цифр в виде набора всевозможных комбинаций и сочетаний.
- Применяет сценарии (scripts) или другие автоматизированные инструменты для регистрации на множестве учётных записей пользователей, которые, затем, использует для рассылки коммерческих сообщений.
- Ретранслирует сообщения электронной почты через компьютеры или компьютерные сети без разрешения их владельцев.

Таким образом, успешное судебное разбирательство может стоить спамеру существенной суммы денег. Закон предусматривает, также, уголовные наказания, включающие тюремное заключение для тех, кто осуществляет (или замышляет осуществить) следующее.

- Использует чужой компьютер для рассылки коммерческих сообщений без разрешения его владельца.
- Использует компьютер для ретрансляции множества коммерческих сообщений с целью обмана получателя или Интернет провайдера об источнике этих сообщений.
- Рассылает множество сообщений, содержащих ложную информацию в заголовках.
- Предоставляет ложную идентификационную информацию при регистрации множества учётных записей электронной почты или доменных имен.
- Ложно представляет себя как владельца множества IP-адресов, которые используются для рассылки коммерческих сообщений.

Имеется множество примеров успешного применения закона CAN-SPAM, включая случаи, когда вред от рассылки спам-сообщений оценивался в сотни миллионов долларов. В результате судебного разбирательства некоторые спамеры подверглись наказанию в виде тюремного заключения. Успешное применение закона CAN-SPAM сдерживает нарастание потока спам-сообщений в США в последние несколько лет. Однако многие спамеры используют почтовые сервера, находящиеся в странах, в которых не действуют антиспамовские законы.

Вопросы юрисдикции, часто, являются неясными в случае онлайновых компаний. Даже если обвинитель успешен в суде, взыскание предписанного судом штрафа, за причинённые убытки, является трудной задачей. Спамер может уклониться от распоряжения о прекращении противоправных действий, поскольку в состоянии, в течение минуты, переключится на другой сервер. Кроме того, многие спамеры рассылают сообщения через сервера, которые они взломали в результате хакерских действий.

Правовые решения проблемы спама имеют ограниченный успех, поскольку преследование спамеров в судебном порядке обходится правительству слишком дорого. Для того чтобы быть эффективным, с точки зрения финансовых затрат, обвинители должны уметь легко идентифицировать спамера и с высокой вероятностью выигрывать судебные разбирательства. Наилучшим способом, позволяющим легко выявить спамеров, являются технические изменения в механизме транспортировки электронной почты через инфраструктуру Интернет.

Технические решения

Интернет не был создан для выполнения многого из того, что он делает сегодня. Он не был спроектирован, чтобы быть безопасным, осуществлять коммерческие транзакции или рассылать миллиарды сообщений электронной почты. Электронная почта появилась в результате проектирования системы передачи больших файлов от одного исследователя к другому. Интернет, как он был изначально спроектирован, и как он функционирует сегодня, не включает никаких механизмов, обеспечивающих гарантию того, что получатель сообщения электронной почты всегда знает, кто его отправил.

По крайней мере, одна техническая стратегия борьбы со спамом основана на эксплуатации «слабых мест» Интернет. Интернет протокол, управляющий коммуникацией между серверами в Интернет (включая почтовые серверы) был спроектирован как «вежливый» набор правил. Когда компьютер-отправитель отсылает сообщение компьютеру-получателю, он ожидает от него подтверждения того, что сообщение получено и только потом отсылает последующие сообщения. Как правило, это подтверждение возвращается очень быстро. Если компьютер-получатель настроен так, что ему требуется много времени на отсылку подтверждения, то компьютер-отправитель вынужден приостановить работу с компьютером-получателем до тех пока не получит подтверждения.

Это свойство протокола, управляющего передачей сообщений в Интернет, может использоваться для борьбы со спамерами. После идентификации компьютера, рассылающего спам, антиспамовская программа почтового сервера может приостановить отсылку ему подтверждения (например, на 24 часа), парализовав, тем самым, работу компьютера, рассылающего спам. Антиспамовская программа может, также, запустить контратаку, отсылая ответные сообщения электронной почты на компьютер спамера. Та-

кая практика носит наименование *тир-граббинг* (teergrubing). Техника тир-габбинга направлена на то, чтобы поймать спамера в ловушку и лишить его компьютер возможности рассылать спам-сообщения. Многие компании используют технику тир-граббинга как часть общей стратегии борьбы со спамом, однако, некоторые компании опасаются, что запуск контратаки может нарушить положения закона CAN-SPAM.

Большинство экспертов, занимающихся вопросами борьбы со спамом, считают, что окончательное решение этой проблемы может быть достигнуто путем разработки новых протоколов электронной почты, осуществляющих полную верификацию источника каждого сообщения электронной почты.

3.4. Программные утилиты Web-сайтов

Кроме Web-серверных программ разработчики Web-сайтов используют большое количество инструментальных программ или *программных утилит* (utility programs). Некоторые из этих программных утилит работают на стороне серверного компьютера, другие – на стороне клиентского.

3.4.1. Программа трассировки маршрута Tracert

Программа Tracert (TRACE RouTe) отсылает пакеты данных каждому промежуточному компьютеру, находящемуся на пути к удалённому компьютеру, и фиксирует время прохождения пакетов в прямом и обратном направлениях. Программа, таким образом, позволяет получить сведения: (1) о времени прохождения сообщения между двумя компьютерами в прямом и обратном направлении; (2) о том, что удалённый компьютер находится в сети и подключён к ней, а также (3) сведения об информационных «заторах» трафика. Программы трассировки маршрута, также вычисляют и отображают количество промежуточных участков между двумя компьютерами и время прохождения сообщения между двумя тестируемыми компьютерами в одном направлении.

Рис. 3.7 иллюстрирует результат работы программы Tracert при трассировке маршрута от домашнего компьютера автора конспекта, через Web-сервер Одесского Интернет провайдера Инфомир к серверу Московского Государственного Университета (IP-адрес 93.180.27.7) на котором размещён один из сайтов Московского Государственного Университета под наименованием Астронет.

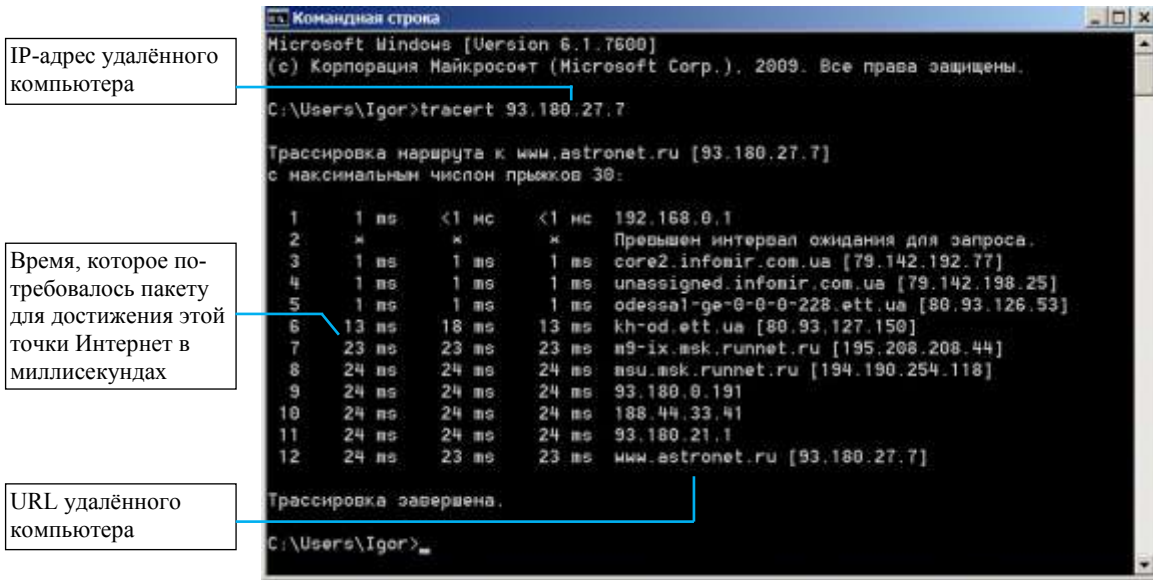

Рис. 3.7. Трассировка маршрута между двумя компьютерами, подключёнными к Интернет

Для запуска программы Tracert в операционной системе Windows необходимо в окне «Командная строка» (путь к этому окну: «Пуск» – «Все программы» – «Стандартные» – «Командная строка») ввести команду

```
tracert <IP-адрес или URL удалённого компьютера>
```

Первая колонка, на рис. 3.7, указывает, что маршрут состоит из 12 транзитных участков, а из второй колонки следует, что пакету понадобилось 24 милисекунды для того, чтобы преодолеть этот маршрут. Программа Tracert, работающая в операционной системе Windows, посылает три тестовых пакета. Времена прохождения промежуточных компьютеров, каждым из пакетов, указаны в миллисекундах во второй, третьей и четвертой колонках на рис. 3.7. В последней колонке указан либо IP-адрес, либо URL каждого промежуточного компьютера, через который проходят пакеты.

3.4.2. Программа Telnet и протокол FTP

Программа Telnet предоставляет возможность пользователю, работающему за компьютером, подключённым к Интернет, получить доступ к файлам, или запустить программу, находящуюся на другом компьютере, также подключённым к Интернет. Возможность удалённой авторизации может быть полезна для запуска старых программ, не имеющих Web интерфейса. Программа Telnet даёт возможность использовать клиентский компьютер для передачи команд программам, выполняющимся на удалённом компьютере, осуществлять удалённый поиск и устранение неисправностей или удалённое системное администрирование. Однако, чем больше компаний и организаций размещают информацию на Web-страницах, доступных при помощи Web браузера, тем реже возникает необходимость в использовании программы Telnet.

Протокол под наименованием *Протокол Передачи Файлов* (File Transfer Protocol – FTP) является частью правил протоколов TCP/IP и определяет форматы, используемые для передачи файлов между компьютерами, обменивающимися данными под управлением протокола TCP/IP. Несмотря на то, что FTP-передача файлов и множество операций по управлению файлами могут быть осуществлены непосредственно через Web-браузер, большинство людей использует для этой цели такие программы как FileZilla или CuteFTP.

3.4.3. Программы анализа посещений Web-сайтов

Web-сервер может сохранять информацию о посещениях Web-сайта, размещённого на сервере. Эта информация включает данные о том, кто посещал сайт (URL посетителя), о том, как долго браузер посетителя просматривал страницы сайта, дату и длительность каждого посещения, а также какие конкретно страницы, которые получал посетитель. Перечисленные данные сохраняются в *журнале регистрации Web* (Web log file). Размер журнала регистрации Web может увеличиваться очень быстро, особенно для популярных сайтов, с которыми ежедневно работают тысячи посетителей, поэтому неавтоматизированный анализ этих данных, как правило, невозможен. Анализ данных, хранящихся в журнале регистрации Web, является крайне желательным, поскольку позволяет делать выводы, как о статистике посещений сайта (количество посещений в течение дня, часа или минуты; время пиковой нагрузки на сайт и т.д.), так и о предпочтениях посетителей сайта.

Для анализа данных, находящихся в журнале регистрации, используются внешние *программы-аналитики журнала регистрации* (Web log file analytics). Наиболее известными программами-аналитиками журнала регистрации являются Adobe Analytics, Google Analytics и Weberends Analytics.

3.4.4. Программы контроля гиперссылок

Важной функцией администратора Web-сайта является контроль работоспособности и корректности гиперссылок, связывающих страницы сайта со сторонними сайтами.

Ссылки на сторонние сайты, размещенные на некоторой странице, со временем могут стать неактуальными, поскольку сайты могут изменить свои URL или вовсе исчезнуть. Когда пользователь коммерческого Web-сайта пытается выполнить переход по ссылке на отсутствующую страницу, то вместо страницы он получает сообщение об ошибке. Такие сообщения раздражают пользователей и побуждают их к прекращению работы с сайтом.

Программные утилиты контроля гиперссылок (link checker utility programs) проверяют каждую страницу сайта и сообщают о некорректных ссылках. Они могут, также, обнаруживать «зависшие» файлы Web-сайта, или файлы, размещенные на сервере, которые не связаны ни с одной из Web-страниц.

Некоторые инструментальные программы, предназначенные для разработки сайтов, например, Adobe Dreamweaver включают функции контроля гиперссылок. Однако, большинство программ контроля гиперссылок являются самостоятельными утилитами. В свободном доступе находятся такие программы контроля гиперссылок, как Elsop LinkScan и LinxCop.

3.4.5. Удалённое администрирование сервером

Программы удалённого администрирования сервером (remote server administration software) позволяют администратору Web-сайта осуществлять мониторинг и управление сайтом с любого компьютера, подключенного к Интернет. Компании LabTech Software и NetMechanic продают программы, реализующие функции удалённого администрирования, контроля гиперссылок, поиска и устранения HTML ошибок, и другие программные утилиты необходимые администратору для управления Web-сайтом и его сопровождением.

3.5. Аппаратное обеспечение Web-серверов

Коммерческие компании и некоммерческие организации используют широкий спектр компьютеров, отличающихся производителем, типом и размерами для ведения своей онлайновой деятельности. Web-сервера маленьких компании могут функционировать на настольных компьютерах, однако большинство сайтов, используемых в электронном бизнесе, работают на компьютерах, сконструированных специально для реализации функций Web-сервера.

3.5.1. Web-серверные компьютеры

Компьютеры, которые используются в качестве Web-серверов, в общем случае, обладают бóльшим объёмом быстродействующей основной и внешней памяти и более производительным процессором, чем типичные настольные компьютеры. Многие Web-серверные компьютеры являются мультипроцессорными. Отмеченные свойства Web-серверных компьютеров резко повышают их стоимость по сравнению с настольными компьютерами, используемыми в качестве рабочих станций. Сегодня стоимость высококачественного настольного компьютера колеблется в диапазоне от 500 до 1200 долларов США. Большинство компаний тратят от 2000 до 50000 долларов на приобретение индивидуального Web-серверного компьютера. Крупные компании, использующие тысячи Web-серверных компьютеров, могут расходовать миллионы долларов на аппаратное обеспечение своих Web-серверов. Компании, специализирующиеся на продаже аппаратного обеспечения Web-серверов, такие как Dell, Gateway, Hewlett Packard и Oracle, предлагают на своих сайтах инструменты, позволяющие посетителям сайта самостоятельно конфигурировать аппаратное обеспечение Web-сервера.

Оборудование Web-серверного компьютера может размещаться в индивидуальном корпусе, однако, обычно, оно размещается в специальных *шкафах* (equipment racks). Эти шкафы имеют стандартные размеры, и в каждом их них может быть размещена аппаратура нескольких серверов. Популярна конфигурация размещения аппаратуры Web-сервера на основе блэйд-серверов. *Блэйд-сервер* (blade server) представляет собой вычислитель-

ную часть сервера, состоящую из процессора/процессоров и основной памяти, размещённые в отдельном модуле. Модули с блэйд-серверами устанавливаются в шкаф. К ним подключаются компоненты, реализующие общие, для всех блэйд-серверов, не вычислительные функции периферийной части, а также питания и охлаждения. В одном шкафу могут разместиться более 100 блэйд-серверов. На рис. 3.8 приведена фотография двухпроцессорного блэйд-сервера компании Supermicro, а на рис. 3.9 – шкафы с блэйд-серверами.

Рис. 3.8 Блэйд-сервер компании Supermicro

Рис. 3.9 Шкафы с блэйд-серверами

3.5.2. Web-сервера и «зелёные вычисления»

Работа большого количества компактно расположенных компьютеров, особенно, таких мощных компьютеров как Web-сервера, потребляет значительное количество электрической энергии. Бóльшая часть этой энергии расходуется непосредственно для работы серверов, однако существенная её часть используется для охлаждения помещений, в которых расположены сервера. Большие компьютеры генерируют огромное количество тепла. Меры, направленные на уменьшение влияния мощных компьютеров на окружаю-

щую среду называются «*зелёными вычислениями*» (green computing). Компании, эксплуатирующие большое количество Web-серверных компьютеров находят интересные способы минимизации их влияния на окружающую среду.

В 2009 году компания Google начала эксплуатацию серверного оборудования в Финляндии, в здании, в котором ранее размещалось предприятие по изготовлению бумаги. Здание располагалось на побережье, а под ним, в гранитном массиве, проходили тунели, выходившие в море. Google начала использовать морскую воду, вместо электрических кондиционеров, для рассеивания тепла, выделяемого серверами. Низкая среднегодовая температура воздуха в Финляндии, также, снижала потребность в искусственном охлаждении серверов.

Компания Facebook эксплуатирует серверное оборудование в городе Лулеа в северной Швеции (находится примерно на 100 км южнее северного полярного круга) и использует наружный воздух для охлаждения серверов. На близлежащей реке установлен гидроэлектрический генератор, который поставляет дешевую электроэнергию, необходимую для работы серверов.

Компания Hewlett-Packard разместила серверное оборудование в городе Форт-Коллинс (штат Колорадо, США), находящегося у подножья Скалистых гор, и использует холодный горный воздух для охлаждения серверов. Многие другие крупные компании в США, такие, например, как FedEx также используют естественное охлаждение своего серверного оборудования.

Зелёные вычисления уменьшают негативное влияние электронного бизнеса на расходование ограниченных запасов энергетических ресурсов планеты. Они, также, обеспечивают значительную экономию средств, для тех компаний, которые следуют идее зелёных вычислений.

3.5.3. Оценка эффективности Web-сервера

Проведение оценочных испытаний аппаратного и программного обеспечения Web-сервера может помочь принять информированное решение о его эффективности. Оценочное испытание, в этом контексте, представляет собой тестирование, проводимое с целью сравнения эффективности совместной работы аппаратного и программного обеспечения.

Компоненты, влияющие на общую эффективность Web-сервера, включают: аппаратное обеспечение; операционную систему; Web-серверное программное обеспечение; пропускную способность канала связи с Интернет; пользовательский потенциал и тип доставляемых Web-страниц. Важным является количество пользователей, которые могут быть обслужены сервером. Это количество трудно измерить, поскольку на него влияют и пропускная способность канала связи с Интернет и размер доставляемых Web-страниц. Два фактора должны быть оценены для измерения способности сервера доставлять Web-страницы: *производительность* (throughput) сервера и *время отклика* (response time). Производительностью сервера называется количество HTTP-запросов, которые, конкретная комбинация аппаратного и программного обеспечения, позволяет обработать в единицу времени. Время отклика это время, которое требуется серверу, для обработки одного запроса.

Одним из способов выбора наилучшей конфигурации аппаратного обеспечения Web-сервера является тестирование различных возможных вариантов этой конфигурации, однако такое тестирование трудно осуществить для оборудования, которое ещё не приобретено. Существуют независимые лаборатории, тестирующие различные варианты комбинации аппаратного и программного обеспечения Web-серверов и публикующие отчеты с результатами этого тестирования. Некоммерческая организация Standard Performance Evaluation Corporation (SPEC) разрабатывает и распространяет тесты для оценочных испытаний серверов. Тестовые пакеты SPEC являются стандартами для оценки производительности современных компьютерных систем.

Компании, которые оперируют множеством серверов, должны решать, каким образом нужно конфигурировать эти сервера для обеспечения наиболее высокой эффективно-

сти его функционирования. Объединение серверов друг с другом и с сетевым оборудованием, таким как роутеры и свитчи, называют *серверной архитектурой* (server architecture)

3.5.4. Архитектура аппаратного обеспечения Web-сервера

Коммерческие Web-сайты используют двухуровневую, трехуровневую или n-уровневую модель типа «клиент-сервер» для того, чтобы разделить работу по обслуживанию Web-страниц, администрированию баз данных и обработке транзакций. Трафик Web-сайтов некоторых онлайновых компаний настолько велик, что для аппаратного обеспечения серверов каждого уровня требуется множество компьютеров.

Большие компании используют сотни и даже тысячи Web-серверных компьютеров. Совокупность большого количества серверных компьютеров часто называется *серверной фермой* (server farm), поскольку, при размещении шкафов с серверным оборудованием в помещении, их, обычно располагают рядами, как растения на сельскохозяйственной ферме. Существует два подхода к проектированию аппаратного обеспечения Web-серверов больших компаний. Первый из подходов базируется на *централизованной архитектуре* (centralized architecture), которая предполагает использование нескольких мощных и быстродействующих компьютеров.

Второй подход предполагает использование большого количества менее мощных компьютеров и оптимальное распределением их загрузки. Такая архитектура называется *децентрализованной архитектурой* (decentralized architecture). Рис. 3.10 иллюстрирует централизованную и децентрализованную архитектуры аппаратного обеспечения Web-сервера.

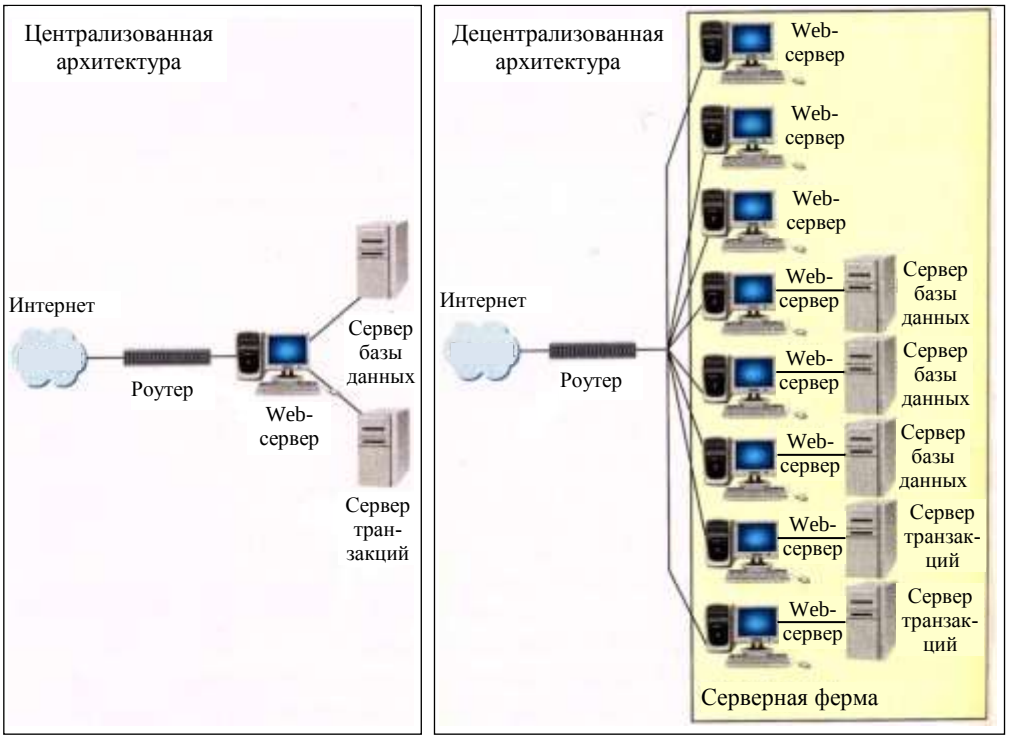

Рис. 3.10 Централизованная и децентрализованная архитектура Web-сервера

Централизованная архитектура требует использования дорогих компьютеров и более чувствительна к техническим отказам оборудования. Если один из нескольких компьютеров выходит из строя, то теряется значительная часть функциональных возможностей сайта, размещенного на сервере. Децентрализованная архитектура распределяет риски, связанные с отказом оборудования, между большим количеством серверных компьютеров. Если один из большого количества серверных компьютеров выходит из строя,

сайт продолжает работать, теряя незначительную часть своих возможностей. Компьютеры, используемые в децентрализованной архитектуре дешевле, чем мощные компьютеры, используемые в централизованной архитектуре. Например, общая стоимость 100 серверных компьютеров, используемых в децентрализованной архитектуре, меньше чем стоимость компьютера эквивалентной мощности, используемого в централизованной архитектуре. Однако, децентрализованная архитектура предполагает использование дополнительного сетевого оборудования для связи серверов друг с другом. В большинстве вариантов децентрализованной архитектуры используется *система балансировки нагрузки* (load-balancing system) серверов, которая может иметь значительную стоимость.

Система балансировки нагрузки серверов

Очень часто система балансировки нагрузки серверов, строится на базе устройства, называемого коммутатор с балансировкой нагрузки или свитч-балансировщик нагрузки. *Свитч-балансировщик нагрузки* (load-balancing switch) представляет собой устройство, предназначенное для мониторинга рабочей нагрузки, подключенных к нему серверов, и направления входного трафика на тот сервер, который, в данный момент времени, располагает наиболее подходящими ресурсами для его обработки. В простой системе балансировки нагрузки серверов, Web трафик, приходящий на Web-сайт через входной роутер, попадает на вход свитч-балансировщика нагрузки, который направляет его на тот сервер, который может обработать этот трафик наиболее эффективно. На рис. 3.11 изображена архитектура системы балансировки нагрузки серверов на базе коммутатора с балансировкой нагрузки.

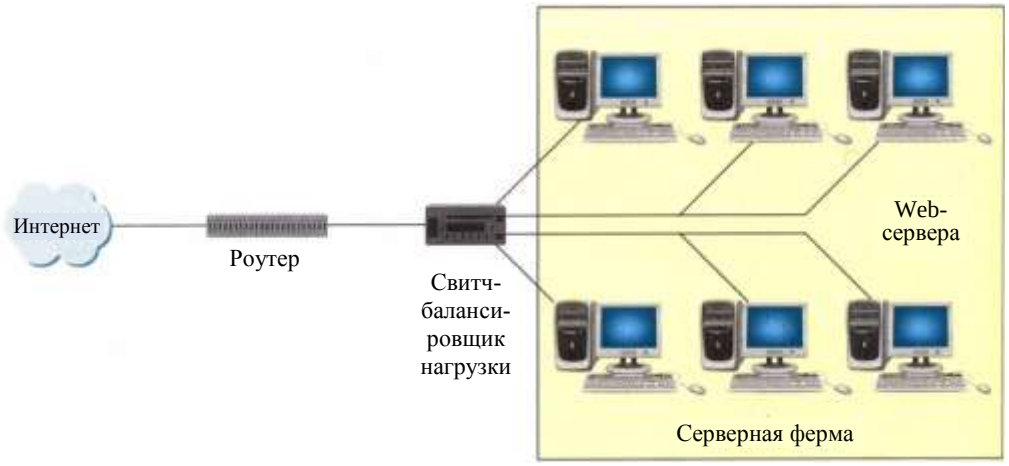

Рис. 3.11. Система балансировки нагрузки серверов с использованием свитч-балансировщика

В более сложных системах балансировки нагрузки серверов, входной трафик, который может поступать на Web-сайт от двух и более роутеров, направляется к различным группам серверов, специализированных на обработку специфических запросов. В сложной системе балансировки нагрузки серверов, изображенной на рис. 3.12, серверы объединены в группы, каждая из которых специализирована на реализацию отдельных функций: поиск и доставку статических HTML страниц; обработку запросов к базе данных, создание и доставку динамических Web-страниц; обработку транзакций.

Стоимость свитч-балансировщика нагрузки и программного обеспечения, необходимого для его работы, для простых систем балансировки нагрузки серверов, составляет около 2000 долларов США. Стоимость свитч-балансировщика нагрузки, вместе с соответствующим программным обеспечением, для сложных систем колеблется в диапазоне от 15000 до 40000 долларов.

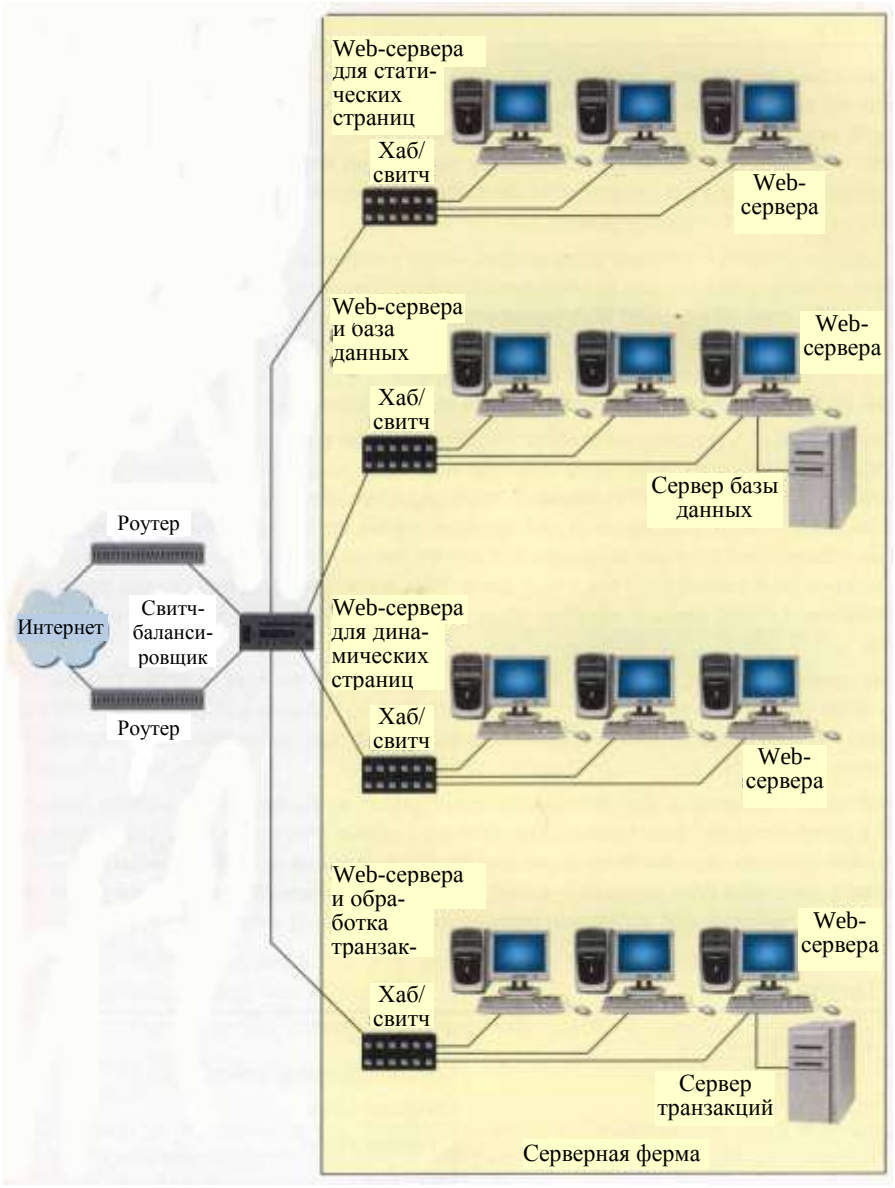

Рис. 3.12. Сложная система балансировки нагрузки серверов

3.6. Сети доставки контента

Одна из наиболее важных целей коммерческого сайта заключается в обеспечении постоянной и надёжной связи с клиентами в реальном масштабе времени. В период систем электронной коммерции первого поколения, когда Web-сайты состояли, главным образом, из текстовых страниц, Интернет легко обеспечивал необходимую пропускную способность для обмена информацией между Web-сервером компании и браузером клиента. По мере того, как страницы коммерческих сайтов стали насыщаться графическими изображениями и файлами документов, начали возрастать требования к пропускной способности каналов связи, однако технологии, используемые для построения сетей Интернет, позволяли справляться с возросшим трафиком.

Начиная с 2008 года, трафик Интернет включает существенное количество аудио- и видео-файлов. Обычная Web-страница, состоящая из смеси текста и графики имеет размер менее 1 Мб, но песня, записанная в формате MP3, имеет размер от 3 до 5 Мб, а размер компрессированного видео-файла колеблется в диапазоне от нескольких мегабайт до

нескольких гигабайт. Например, размер видео-файла, содержащего качественный фильм, находится в диапазоне 4 – 8 Гб. По оценкам специалистов от 40% до 55% всего современного мирового трафика Интернет состоит из видео-файлов сайтов YouTube и Netflix. Поскольку размер видео-файла примерно в 8000 раз больше размера средней Web-страницы, мировой Интернет трафик растет очень быстрыми темпами. Рост мирового Интернет трафика в период с 2006 по 2019 годы показан на рис. 3.13.

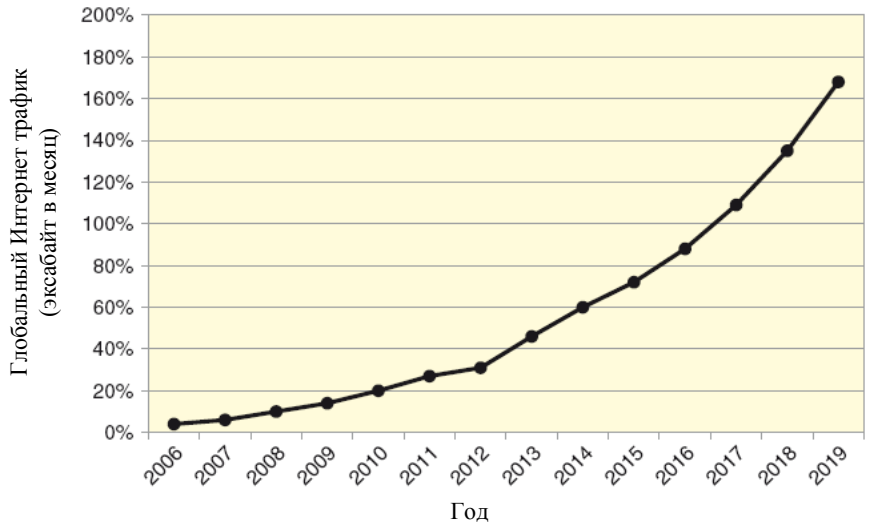

Рис. 3.13 Рост мирового Интернет трафика.
1 эксабайт равен миллиону терабайт или 10^{18} байт

Хотя пропускная способность магистральных сетей Интернет достаточна для обработки такого трафика, нельзя быть уверенным, что все данные, запрошенные любым браузером, будут переданы эффективно. Интернет является сетью с коммутацией пакетов (см. подраздел 2.2 конспекта лекций по дисциплине Электронная коммерция). Это означает, что перед передачей данных через Интернет, большие файлы разбиваются на множество небольших пакетов, которые передаются получателю через промежуточные узловые компьютеры. Этот процесс разбивки и последующего восстановления файлов требует дополнительных коммуникаций в сети, количество которых возрастает с ростом среднего размера файла. Часто, при просмотре видео-файлов, возникают паузы, связанные с неспособностью сети транслировать весь трафик в реальном масштабе времени. Эта задержка, или *латентность* (latency) трафика может быть проблемой для тех компаний, бизнес которых основан на передаче по Интернет потокового видео.

Для защиты своих клиентов от латентности трафика, онлайновые компании, транслирующие потоковое видео, пользуются услугами посреднических компаний, называемых *сети доставки контента* (content delivery networks – CDNs). Эти компании хранят копии больших файлов на множестве территориально распределённых серверов. Когда браузер клиента запрашивает большой файл, CDN направляет этот запрос серверу, находящемуся на наименьшем расстоянии от клиента. Основные CDN, такие как Akamai Technologies, Level 3 Communications, Limelight Networks и Tata Communications, размещают свои сервера в дата центрах больших компаний, у провайдеров услуг Интернет, в университетах и в других крупных организациях таким образом, чтобы файлы располагались как можно ближе к потенциальным клиентам.

Крупные компании, продающие контент в больших файлах, оплачивают услуги CDN непосредственно. Небольшие компании могут получать услуги CDN опосредованно через своих провайдеров услуг Интернет. В этом случае, стоимость услуг CDN составляет около 10 центов за гигабайт. Компании, которые снабжают своих клиентов большим количеством аудио- и видео-файлов, такие, например, как Apple, создали свои собственные CDNs.

ЗАДАНИЯ ДЛЯ СЕМИНАРСКИХ ЗАНЯТИЙ

1. Найдите и посетите Web-сайты, по крайней мере, двух коммерческие компании, которые оказывают платные услуги по технической поддержке Web-северного программного обеспечения Apache. Изучите перечень и стоимость каждой из услуг, оказываемых этими компаниями. Изучите найденные сайты и сделайте обзоры деятельностей найденных компаний, а также обзоры структуры сайтов.

2. Представьте, что Вы осуществляете поддержку Web-сайта некоторой онлайновой коммерческой компании. Менеджер компании поручил Вам периодически проверять валидность гиперссылок, этого сайта. Вместо того чтобы покупать и инсталлировать платные утилиты контроля гиперссылок Вы решили исследовать применимость онлайновых средств контроля гиперссылок. Используйте W3C Link Checker и проверьте гиперссылки любого выбранного Вами сайта. Будьте терпеливы, поскольку работа этой программы может занять некоторое время. Представьте результаты Ваших исследований и сделайте заключение о применимости использованного Вами онлайнового средства контроля гиперссылок, и результаты его работы.

3. Многие компании, продающие компьютеры, предназначенные для организации Web-серверов, предлагают конфигурацию управления дисковым пространством сервера под наименованием RAID массив (Redundant Array of Independent Disks). Ознакомьтесь с идеей, лежащей в основе RAID массива, используя статью в Википедия и другие источники. Опишите возможные варианты конфигурации RAID массива, а также достоинства и недостатки каждого из вариантов. Какой или какие из этих вариантов более всего подходят для Web-сервера, на котором размещается сайт коммерческой компании.

4. Представьте, что Вы работаете в новом онлайновом отделении компании, производящей светодиодные осветительные лампы. Владелец компании поручил Вам сделать предложение по использованию наиболее подходящей модели типа «клиент-сервер», которая необходима для онлайновой продажи продукции компании. Компания уже эксплуатирует сервер, на котором размещён каталог её продукции и сервер транзакций, который отслеживает каждую продажу. В докладе расскажите об особенностях различных моделей типа «клиент-сервер» в Web, а также обоснуйте какая из моделей (2-х уровневая, 3-х уровневая или n-уровневая) будет наиболее подходящей для компании. Отметьте, какие дополнительные сервера понадобятся компании.

5. Китайская Народная Республика (КНР) является вторым по зна́чимости рынком для компании Microsoft, которая получает примерно 300 миллиардов долларов, продавая лицензии на свои продукты в КНР. Однако более 90% продуктов компании Microsoft используются в КНР нелегально. В Microsoft считают, что конвертирование нелегальных пользователей в легальных, путём продажи им лицензий по сниженной цене может существенно увеличить прибыль компании. Стратегия, которой придерживается Microsoft в КНР, заключается в продаже лицензий крупным компаниям и правительственным учреждениям по полной цене и малым компаниям по дисконтной цене. Тем не менее, официальные лица КНР критикуют Microsoft за высокую цену её программ, а также сомневаются в их безопасности. Компания Microsoft не публикует коды своих программ, считая их производственным секретом. В КНР допускают, что Microsoft может включать в свои программы секретные модули, позволяющие получать доступ к правительственным серверам КНР. Программы с открытым кодом и находящиеся в свободном доступе являются привлекательной альтернативой, поскольку они бесплатны и не содержат секретных модулей. Однако, Microsoft утверждает, что использование программ с открытым кодом: (1) доро-

же, поскольку требуются дополнительные затраты на их инсталляцию, поддержку и обновление; (2) опасно, поскольку открытый код позволяет злоумышленникам разрабатывать средства для взлома. Опишите трудности, с которыми сталкивается компания Microsoft, продавая свои продукты в КНР. Вначале, представьте, что Вы работаете в законодательном органе КНР. Сформулируйте и обоснуйте аргументы, которые Вы могли бы использовать, в поддержку закона требующего, чтобы все правительственные организации КНР использовали только программы с открытым кодом для своих Web-серверов. Теперь, представьте, что Вы работаете в отделе Microsoft, который занимается продажами в КНР. Сформулируйте и обоснуйте аргументы, которые могут убедить руководителей крупных компаний КНР использовать программное обеспечение Microsoft на своих Web-серверах. И, наконец, представьте, что Вы работаете в консалтинговой компании, которая предлагает услуги по инсталляции и обслуживанию как Windows, так и Linux операционных систем. Перечислите аргументы «за» и «против», которые могут помочь Вашим клиентом сделать выбор операционной системы для Web-сервера.

6. Татьяна является владельцем магазина, продающего кроссовки, украшенные вручную. Большинство людей, покупающих такие кроссовки, хотят иметь возможность выбрать специфическую комбинацию кроссовок и украшения или заказать дизайн украшения специально для себя. Татьяна решила, что она может удовлетворить потребности своих клиентов, продавая обувь в онлайновом магазине. Кроме того, онлайновый магазин должен привлечь гораздо больше клиентов, чем физический магазин. Используя цифровую фотокамеру, Татьяна сделала несколько сотен фотографий комбинаций кроссовок и их дизайна, а затем пригласила специалиста для создания прототипа своего будущего сайта. Когда была завершена работа над прототипом, Татьяна, вместе со специалистом, определила, что средний размер Web-страницы, равен 100 Кб, а среднее количество страниц, которые может посетить потенциальный клиент равно 23. Затем были произведены оценки требуемого дискового пространства и трафика. Оценки дали следующие цифры. Для размещения базы данных Web-страниц (включая фотографии) потребуется 1 терабайт. Для размещения СУБД потребуется 500 Мб. Программное обеспечение тележки для покупок потребует 300 Мб. В первый месяц сайт посетит примерно 8000 потенциальных клиентов, а затем, в течение двух лет трафик будет ежемесячно возрастать на 20%. Наибольшее количество посетителей, одновременно работающих с сайтом равно 1000. Исходя из приведенных оценок, определите и обоснуйте основные характеристики Web-сервера, который понадобится Татьяне, для размещения своего сайта. (1) Размер основной и внешней памяти, а также производительность процессора (можете сослаться на информацию таких продавцов как Dell, Hewlett Packard или Oracle). (2) Наиболее приемлемая операционная система для управления Web-сервером, а также её преимущества и недостатки. (3) Наиболее приемлемое Web-серверное программное обеспечение, а также его преимущества и недостатки.

4. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ

4.1. Web-хостинг и его альтернативы

Web-хостингом (Web hosting) называется услуга по предоставлению компьютерных ресурсов для размещения Web-сайта на Web-сервере, постоянно находящимся в сети Интернет. Компании, предоставляющие услуги по Web-хостингу, обычно, предоставляют и услуги по хостингу электронной почты, файлового хранилища и др.

Коммерческая компания, занимающаяся онлайновым бизнесом, может эксплуатировать свой собственный Web-сервер и всё необходимое программное обеспечение. Такой подход называется *собственным Web-хостингом* (self-hosting) и используется, как правило, крупными онлайновыми компаниями. Небольшие и средние компании, чаще, прибегают к услугам посредников, специализирующихся на Web-хостинге.

В дисциплине Электронная коммерция было введено понятие *провайдера услуг Интернет* (см. подраздел 2.1.4 конспекта лекций по дисциплине Электронная коммерция) продающего услуги по доступу в Интернет отдельным личностям и компаниям. Фактически все провайдеры услуг Интернет предлагают, также, услуги Web-хостинга и, иногда, называют себя *провайдерами услуг электронной коммерции* (commerce service providers – CSPs). Отмеченные провайдеры часто предлагают дополнительные услуги по администрированию Web-сервером, аренду прикладного программного обеспечения (такого как базы данных, тележка для покупок и др.) и опосредованный доступ к сетям доставки контента.

Провайдеры Web-хостинга могут предлагать своим клиентам три вида хостинга: виртуальный хостинг, выделенный хостинг и услуга по размещению сервера.

Виртуальный хостинг (shared hosting) означает, что на Web-сервере провайдера размещаются Web-сайты нескольких клиентов, которые одновременно обслуживаются.

Выделенный хостинг (dedicated hosting) означает, что на Web-сервере размещается Web-сайт только одного клиента. Как при виртуальном, так и при выделенном хостинге владельцем сервера является провайдер, который передает его в лизинг клиенту. Провайдер несет ответственность за работоспособность аппаратного и программного обеспечения и обеспечивает связь с Интернет через свои роутеры и другое сетевое оборудование.

Услуга по размещению сервера (co-location) означает, что провайдер предоставляет клиенту в аренду свои помещения, электроснабжение и связь с Интернет. В этих арендуемых помещениях клиент размещает свою аппаратуру и устанавливает необходимое программное обеспечение. Клиент полностью обслуживает свою аппаратуру, Web-сервер и сайт. Провайдер несёт ответственность только за надёжное электроснабжение и связь с Интернет.

Список компаний-провайдеров Web-хостинга можно получить, сделав поиск в Web по ключевым словам: «услуги Web-хостинга», или «Web hosting services».

Размеры коммерческого сайта и его трафик имеют тенденцию увеличиваться со временем. Поэтому, когда коммерческая компания принимает решение о выборе одной из возможных альтернатив Web-хостинга, она должна учитывать возможность масштабируемости/расширяемости Web-сервера. Под масштабируемостью Web-сервера понимается его способность наращивать аппаратные и программные ресурсы для удовлетворения растущих потребностей коммерческого сайта.

4.2. Базовые и расширенные функции программного обеспечения электронной коммерции

Поскольку сайты электронной коммерции существенно отличаются друг от друга в терминах размеров, целей, посетителей и т.д., существует широкий спектр доступного аппаратного и программного обеспечения, необходимого и достаточного для построения коммерческого сайта. На одном полюсе этого спектра находится сайт с минимальными потребностями, размещенный на Web-сервере провайдера и полностью им обслуживаемый. На другом полюсе – сайт, использующий изощренное аппаратное и программное

обеспечение, который в состоянии обслуживать большие потоки транзакций и включающий широкий ассортимент инструментов технологии электронной коммерции интегрированных со средствами управления деятельностью предприятия. Все виды программного обеспечения электронной коммерции должны обеспечивать следующие базовые функции:

- отображение Web-каталога;
- возможности тележки для покупок;
- обработка транзакций.

Большие и сложные сайты электронной коммерции используют дополнительное программное обеспечение, расширяющее базовые функции. Эти дополнительные компоненты программного обеспечения могут включать:

- связующее программное обеспечение, интегрирующее систему электронной коммерции с существующими программами, используемыми для управления запасами, обработки заказов и бухгалтерского учёта;
- интеграцию программных приложений предприятия:
- интеграцию с программой планирования ресурсов предприятия;
- Web-сервисы;
- программу менеджмента цепью поставок;
- программу менеджмента отношений с клиентом;
- программу управления контентом;
- программу управления знаниями.

4.2.1. Программы работы с Web-каталогом

Web-каталог является составной частью большинства коммерческих сайтов, представляет собой перечень товаров или услуг, продаваемых онлайновой компанией, и служит для их упорядочения. Для удобства работы, товары, представленные в Web-каталоге, группируются в логические разделы, примерно так же как товароведы обычных магазинов распределяют товары между разными отделами магазина. Однако, в обычном магазине один физический товар располагается только в одном месте. В Web-сайте на один и тот же товар могут указывать ссылки из различных мест. Например, на одну и ту же обувь для бега могут быть ссылки как из раздела, продающего обувь, так и из раздела, продающего спортивное снаряжение.

Коммерческие сайты, продающие небольшое количество неизменных товаров могут строиться на основе простого статического каталога. *Статический каталог* (static catalog) это HTML документ, описывающий список товаров, который отображается на одной или нескольких Web-страницах в окне браузера. Для того, чтобы добавить, удалить или изменить информацию о товаре в статическом каталоге, компания должна отредактировать соответствующее место в HTML документе. Коммерческие компании, продающие большое количество часто меняющихся товаров, обычно, строятся на основе динамического каталога. *Динамический каталог* (dynamic catalog) хранит информацию о товарах в базе данных. База данных размещается на отдельном компьютере, который доступен Web-серверному компьютеру. Динамический каталог может включать множество фотографий каждого товара, его детальное описание и средства поиска, позволяющие посетителю сайта осуществлять поиск нужного товара в каталоге. Программы, реализующие динамические каталоги, обычно, включаются в пакеты программного обеспечения электронной коммерции, однако некоторые компании разрабатывают собственные программы, связывающие Web-сайт с ранее созданными базами данных с информацией о товарах. Оба типа каталогов (статический и динамический) размещаются на сервере базы данных на третьем уровне модели «клиент-сервер» в Web (см. рис. 3.3).

Коммерческие сайты, продающие небольшое количество товаров (менее 100) могут обходиться простым списком товаров, группировка которых в логические разделы не обязательна. Такие сайты могут предоставлять каждый товар его фотографией и ссылкой на информацию о товаре. Поэтому статический каталог достаточен для их построения.

Однако, большинство онлайновых продавцов хотят встраивать в свои сайты средства поиска и навигации и другие инструменты, облегчающие работу с каталогом, что является прерогативой динамического каталога.

4.2.2. Программы виртуальной тележки для покупок

В ранних системах электронной коммерции первого поколения покупатель, выбрав товары, оформлял заказ путем заполнения электронной формы заказа. В форму заказа покупатель должен был вручную вносить шифр товара, наименование товара и количество приобретаемых экземпляров товара. Такой способ оформления заказа порождал ошибки при заполнении формы заказа, особенно в тех случаях, когда покупатель, при помощи одной формы, оформлял заказ на приобретение нескольких товаров. Сегодня, стандартным способом оформления онлайнового заказа является использование программы, называемой *тележка для покупок* (shopping cart) или *корзина для покупок* (shopping basket). Виртуальная тележка для покупок хранит информацию о товарах, которые отобрал покупатель, позволяет ему видеть и редактировать эту информацию. Для того чтобы заказать товар (поместить его в тележку для покупок) покупатель должен кликнуть кнопку, находящуюся рядом с описанием товара и имеющую надпись «добавить в тележку». Вся, информация о товаре, необходимая для оформления заказа (цена, наименование и идентификационный номер товара) автоматически сохраняется в тележке для покупок. Хорошая тележка для покупок позволяет покупателю в любой момент видеть содержимое тележки и удалять из неё ненужные товары. Когда покупатель готов завершить сеанс покупки, он должен кликнуть на кнопку «оформить заказ». На рис. 4.1, в качестве примера, приведена Web-страница виртуальной тележки для покупок Харьковского магазина Rt.co.ua, продающего инструменты.

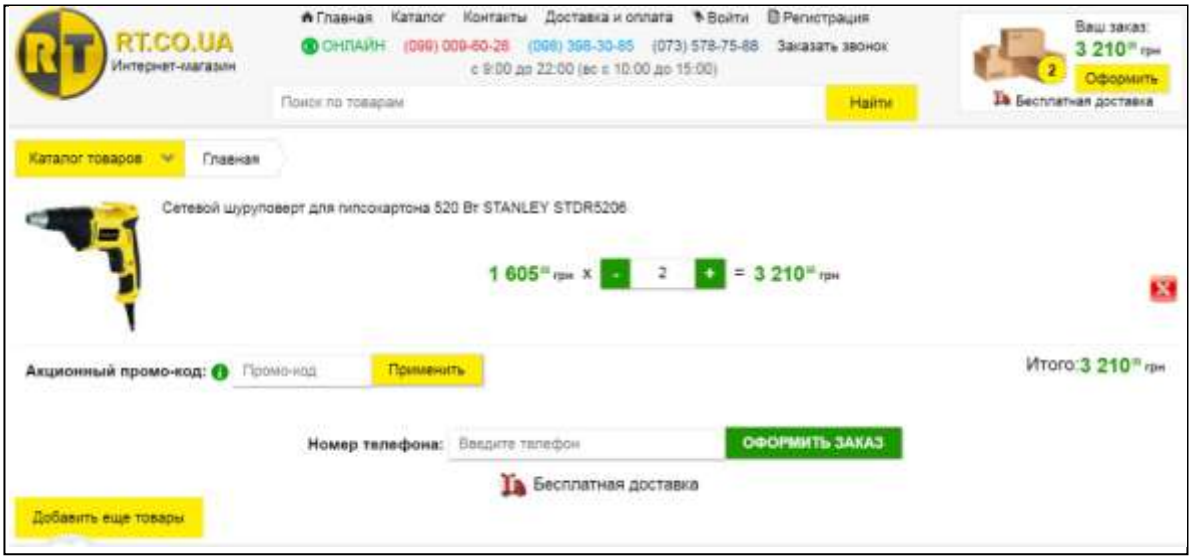

Рис. 4.1. Пример Web-страницы виртуальной тележки для покупок

Нажатие на кнопку «оформить заказ» перемещает покупателя на страницу, где ему предлагается указать способ оплаты, адрес и способ доставки. На этом оформление заказа завершается. Как это видно на рис. 4.1, программа подсчитывает общую стоимость заказа с учётом количества приобретаемых товаров. Перед завершением оформления заказа программа, также, подсчитывает и отображает его общую стоимость, учитывая стоимости доставки и, возможные скидки.

Некоторые программы позволяют покупателю поместить заполненную тележку для покупок в виртуальное хранилище и завершить оформление заказа через несколько дней. Программное обеспечение тележки для покупок разрабатывают и продают многие ком-

пании. Наиболее известными являются BigCommerce, SalesCart и Volusion. Компании, продающие тележки для покупок, требуют ежемесячную оплату за эксплуатацию программы в диапазоне от 20 до 300 американских долларов. В некоторых случаях, для эксплуатации тележки для покупок, необходимо приобрести лицензию, стоимость которой колеблется в диапазоне от нескольких сотен до нескольких тысяч долларов.

Протокол HTTP не предусматривает хранения информации о сеансе связи, поэтому тележки для покупок сохраняют информацию о покупателях и их покупках. Одним из способов, при помощи которого тележка для покупок идентифицирует покупателей и запоминает информацию о его покупках, является использование данных, называемых куки-файлами. *Куки-файлы* (cookies) это небольшие файлы, предназначенные для хранения в браузере клиентского компьютера. Они формируются и пересылаются браузеру покупателя во время его работы с сайтом. Когда покупатель повторно посещает сайт, браузер возвращает куки-файлы Web-сайту, информируя его, таким образом, о предыдущей активности пользователя.

Использование куки-файлов является наиболее простым и надёжным способом информирования тележки для покупок о предыдущей активности покупателя. В том случае, когда браузер покупателя настроен таким образом, чтобы он не запоминал куки-файлы, используются другие, однако менее эффективные, способы сохранения в тележке для покупок информации о покупателе и его покупках.

4.2.3. Программа обработки транзакций

Обработка транзакции начинается в тот момент, когда покупатель нажимает кнопку «оформить заказ». Программа обработки транзакции выполняет все необходимые вычисления, такие, например, как вычисление скидки на все товары, находящиеся в тележке, вычисление налога со стоимости заказа и вычисление общей стоимости заказа, включая стоимость доставки. После нажатия кнопки «оформить заказ», Web браузер покупателя и Web сервер продавца переключаются в *безопасное состояние коммуникации* (secure state of communication). Вопросы безопасного состояния коммуникации будут рассмотрены в следующем разделе.

Хотя базовое программное обеспечение электронной коммерции онлайнового магазина может генерировать отчёты, которые резюмируют продажи и отправленные заказы, большинство средних и крупных компаний используют отдельные пакеты программ бухгалтерского и складского учёта. Поэтому программное обеспечение электронной коммерции должно быть связано с программой бухгалтерского учёта и передавать ей данные о каждой транзакции. Программное обеспечение бухгалтерского учёта, обычно, размещается на отдельном компьютере или локальной компьютерной сети коммерческой компании.

Начисление налога и вычисление стоимости доставки является важной частью обработки транзакции. Ставки налогов на продажи и услуги транспортных компаний изменяются весьма часто, поэтому менеджер Web-сайта должен либо постоянно отслеживать эти изменения и вручную обновлять их значения, либо использовать программное обеспечение, которое автоматически актуализирует значение ставок. Крупные международные транспортные компании, такие как FedEx и UPS (United Parcel Service) предлагают своим клиентам программы, которые интегрируются в программное обеспечение электронной коммерции и автоматически актуализирует налоговые ставки транспортных услуг этих компаний. Программа обработки транзакций должна учитывать другие возможные вычислительные сложности, возникающие при обработке транзакции. Например, учёт купонов, или предложение о скидке, привязанное к конкретному временному промежутку, такое как: «купите билет туда-и-обратно до конца текущего месяца и получите скидку в 50%».

В крупных компаниях интеграция процесса обработки онлайновой транзакции с программой бухгалтерского и складского учета и другими программами управления предприятием может быть очень сложной задачей.

4.3. Взаимодействие программного обеспечения электронной коммерции с другими программами коммерческой компании

Большинство крупных компаний, занимающихся электронной коммерцией, осуществляют, также, множество деятельностей, не относящейся к электронной коммерции. Поэтому важными являются вопросы интеграция электронной коммерции с другими видами деятельности компании. Основой информационной системы любой крупной компании является её база данных.

4.3.1. Базы данных

База данных представляет собой набор данных, хранящихся в компьютере в высоко структурированном виде. Правила, которые детерминируют структуру базы данных, основаны на правилах, в соответствии с которым компания осуществляет свою деятельность и которые называются *бизнес-правилами* (business rules) или *бизнес-логикой* (business logic) компании. Поэтому базу данных можно рассматривать как информационную модель компании.

Система управления базой данных (СУБД) облегчает процесс ввода, редактирования, обновления и поиска информации в базе данных. СУБД Microsoft Access является относительно простой и наиболее частотной. Более сложные СУБД, позволяющие оперировать большими базами данных и выполнять операции с высокой скоростью, включают: IBM DB2, Microsoft SQL Server и Oracle. Крупные компании, работающие во многих различных регионах, должны обеспечивать доступ к своей базе данных пользователям любого из регионов. Большая информационная система, которая хранит одни и те же данные во многих физически распределённых местах называется распределённой информационной системой, а база данных, на основе которой строится такая система, называется *распределённой базой данных* (distributed database).

Большинство компаний используют, упомянутые выше, коммерческие СУБД, однако всё возрастающее количество коммерческих компаний и некоммерческих организаций используют программу MySQL, поддерживаемую сообществом программистов в Web. Так же как и операционная система Linux программа MySQL является программной с открытым кодом и находится в свободном доступе, хотя первоначально и была разработана шведской компанией MySQL AB (теперь принадлежащей Oracle). Компания Oracle продает годовую подписку на услуги по эксплуатации и поддержке MySQL.

Онлайновые магазины, продающие множество различных товаров, используют базы данных для хранения информации о товарах (размер, цвет, тип, цена и т.д.). Компании, которые продают товары и в онлайновых и в физических магазинах, используют в своей деятельности одну и ту же базу данных.

4.3.2. Связующее программное обеспечение

Средние и крупные коммерческие компании интегрируют программное обеспечение электронной коммерции (программы Web-каталога, тележки для покупок и обработки транзакций) с программами управления запасами, обработки заказов и бухгалтерского учёта при помощи связующих программ. *Связующее программное обеспечение* (middleware) получает информацию о транзакции от программного обеспечения электронной коммерции и передает её программе бухгалтерского и складского учёта в той форме, которая принята в этой программе. Связующее программное обеспечение выделяет информацию о продажах из тележки для покупок и вводит её непосредственно в модуль продаж программы бухгалтерского учёта без участия человека. Модуль продаж программы бухгалтерского учета может быть сконструирован таким образом, чтобы получать информацию от продавца, когда он принимает заказ по телефону. В этом случае продавец вводит всю информацию, необходимую для оформления заказа, в модуль продаж при помощи клавиатуры во время телефонного разговора с покупателем.

Большие компании, располагающие квалифицированными специалистами в облас-

ти информационных технологий, разрабатывают своё собственное связующее программное обеспечение. Однако большинство коммерческих компаний приобретают готовые связующие программы и адаптируют их к условиям своего бизнеса. Часто работу по адаптации выполняют либо продавцы связующих программ, либо *консалтинговые компании* (consulting firms). Услуги консалтинговых компаний, обычно, стоят больше, чем стоимость самой связующей программы. Общая стоимость адаптации связующих программ к условиям конкретной компании колеблется в диапазоне от 30 тысяч до нескольких миллионов долларов. Наиболее известными продавцами связующего программного обеспечения являются BroadVision, IBM Tivoli Software и Informatica.

4.3.3. Интеграция программных приложений предприятия

Программы, предназначенные для реализации специальных функций, таких, например, как создание *счёта-фактуры* (invoice), формирование *платёжной ведомости* (payroll) или обработка платежа, полученного от покупателя, называются *программными приложениями предприятия* (enterprise application software). *Сервером приложений* (application server) называется компьютер, который получает запросы, полученные Web-сервером, и передаёт управление тем программным приложениям, которые могут выполнить действия в соответствии с содержимым запросов. Действия, реализуемые программными приложениями предприятия, определяются бизнес-правилами или бизнес-логикой. Примером простого бизнес-правила может быть следующее: «Когда клиент авторизовался в системе, сравни введенный пароль с паролем, хранящемся в базе данных».

Действия, реализуемые программными приложениями предприятия, определяются правилами, используемые в бизнесе. Эти правила называют *бизнес-логикой* (business logic). Бизнес-логика распределена между многими приложениями, которые используются в различных частях предприятия. В последние годы компании тратят значительные ресурсы на создание связей между этими распределенными приложениями таким образом, чтобы сформировать взаимосвязанную бизнес-логику предприятия. Создание таких связей и управление ими называется *интеграцией программных приложений предприятия* (enterprise application integration). Интеграция осуществляется при помощи программ, которые передают информацию от одного приложения к другому. Например, программа может передавать информацию, поступающую от систем ввода заказов, различных подразделений предприятия, в единую систему учёта заказов и продаж. Как правило, форматы данных в различных приложениях отличаются друг от друга и, поэтому, передающая программа должна уметь переформатировать данные.

Серверы приложений, обычно, подразделяют на два типа: *система, базирующаяся на страницах* (page-based system) и *система, базирующаяся на компонентах* (component-based system). Система, базирующаяся на страницах, возвращает страницы, описанные при помощи сценария, который совмещает правила презентации данных на Web-странице и бизнес-логику. Поскольку, генерируемые страницы являются динамически, то для создания системы, базирующейся на страницах, используются те же инструментальные средства, что и при создании динамических страниц на стороне сервера: (1) ASP.Net компании Microsoft; (2) Hypertext Preprocessor (PHP) организации Apache Software Foundation; (3) ColdFusion компании Adobe; (4) JavaServerPages (JSP) компания Sun Microsystems (см. подраздел 3.1.1 «Динамические Web-страницы»). Поскольку система, базирующиеся на страницах, сочетает презентацию данных и бизнес-логику, то её трудно изменять.

Для того, чтобы устранить этот недостаток, многие компании используют систему, базирующуюся на компонентах, в которой разделены бизнес-логика и логика презентации. Отдельный программный компонент, в такой системе, соответствует одному бизнес правилу. Системы, базирующиеся на компонентах, создаются при помощи инструментальных средств и сред компонентного программирования: Enterprise JavaBeans (EJBs), Microsoft COM и Common Object Request Broker Architecture (CORBA), предложенной организацией Object Management Group (OMG).

4.3.4. Интеграция с программой планирования ресурсов предприятия

Многие сайты систем электронной коммерции типа «бизнес-бизнес» должны быть в состоянии работать совместно с такими сложными информационными системами как программа планирования ресурсов предприятия. Пакет программ *планирования ресурсов предприятия* (enterprise resource planning – ERP) интегрирует все аспекты деятельности предприятия, включая бухгалтерский учёт, логистику, производство, маркетинг, планирование, управление проектами и казначейские функции.

Двумя основными продавцами пакетов программ ERP являются компании Oracle и SAP. Стоимость типичной инсталляции программы ERP находится в диапазоне от 1 до 10 миллионов долларов (для крупных компаний стоимость может превышать 100 миллионов долларов). Поэтому, компании, эксплуатирующие программы ERP, уже сделали существенные инвестиции в автоматизированное управление бизнесом и хотят, чтобы их онлайновые операции были интегрированы с работой программ ERP. Рис. 4.2 иллюстрирует архитектуру системы электронной коммерции типа «бизнес-бизнес» в компании, которая эксплуатирует программы ERP и использует EDI (см. подраздел 1.2 «электронный обмен данными с удалёнными компьютерами») для связи со своими торговыми партнёрами.

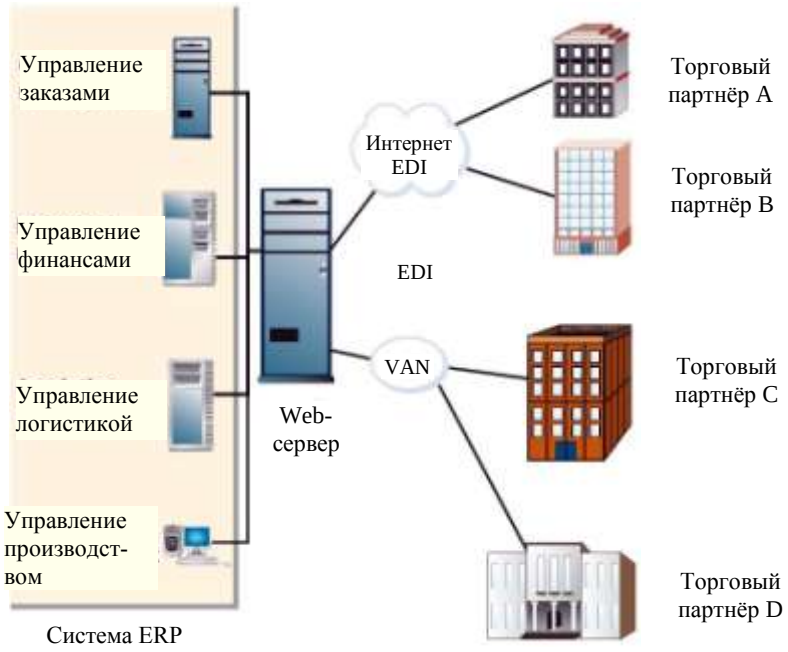

Рис. 4.2. Интеграция Web-сервера с программами ERP и технологией EDI

4.3.5. Web-сервисы

Компании могут использовать Интернет для непосредственной связи программных приложений одной компании с программными приложениями другой компании. Организация *Консорциум всемирной паутины* (World Wide Web Consortium – W3C) определяет *Web-сервисы* (Web services) как программные системы, которые обеспечивают операционной межмашинное взаимодействие при помощи Web. Другими словами, Web-сервисы представляют собой набор программ и технологий, которые позволяют программным приложениям различных компаний использовать Web для непосредственного взаимодействия друг с другом без участия человека оператора.

Программный интерфейс приложения (application program interface – API) является общим наименованием средств взаимосвязи прикладных программ. Когда взаимодействие между прикладными программами осуществляется через Web, то используемые технологии называются Web APIs. Web-сервисы используют различные виды Web APIs.

Возможности Web-сервисов

Коммерческие компании используют Web-сервисы для улучшения обслуживания клиентов и уменьшения расходов. В некоторых компаниях Web-сервисы используются для передачи XML-тегированных данных от одного приложения к другому при интеграции программных приложений предприятия. В других случаях Web-сервисы используются для обмена данными между программными системами двух различных компаний. Многие компании считают, что использование Web-сервисов дешевле и проще чем инсталляция множества связующих программ. Рассмотрим несколько конкретных примеров внедрения Web-сервисов.

- Известный американский инвестиционный банк J.P. Morgan Chase, использует Web-сервисы на своем сайте для сбора информации (такой, как общеэкономические прогнозы, анализы финансовой деятельности конкретных компаний, индустриальные прогнозы и итоги работы финансовых рынков) с целью формирования отчётов, доступных посетителям сайта.
- Британская ипотечная компания Nationwide Building Society, использует Web-сервисы для автоматической коммуникации с ипотечными сервисными компаниями. Эти ипотечные сервисные компании получают информацию от клиентов, желающих получить ипотеку, и передают её в Nationwide в XML формате, где Web-сервисная программа переформатирует полученную информацию и вводит её в компьютерную систему Nationwide. Когда Nationwide принимает решение относительно выдачи ипотечного займа, Web-сервисная программа отсылает это решение на компьютер ипотечной сервисной компании. Благодаря использованию описанной технологии компания Nationwide Building Society сократила время обслуживая клиентов и собственные расходы.
- Американская компания CUNA Mutual Group продаёт финансовые услуги кредитным союзам, кооперативам и другим клиентам. Многие из этих услуг, такие как чековый клиринг (чековые взаимозачеты между банками), остаются неизменными на протяжении многих лет, поэтому CUNA многие годы использует для их реализации старые компьютерные системы. Вместо того, чтобы заменить эти компьютерные системы и создать новое программное обеспечение, CUNA разработала «оболочку» из Web-сервисов, которые получают информацию от старой компьютерной системы и генерирую Web-страницы для своих клиентов, получающих услуги онлайн.

Как работают Web-сервисы

Ключевым элементом технологии Web-сервисов является то, что программист может разрабатывать программы, получающие доступ к программным блокам, реализующим бизнес-логику, без знания деталей того, как она воплощена в этих блоках. Одни Web-сервисы могут комбинироваться с другими Web-сервисами для решения сложных бизнес задач и позволяют связываться программам, написанным на разных языках и для разных платформ.

Первоначально общеупотребительным форматом для межмашинной коммуникации являлся HTML, однако, сегодня, большинство Web-серверных программ используют XML. Многие компании и организации договорились следовать общим стандартам при определении XML тегов и, поэтому, могут использовать XML для описания совместно используемых данных (см. подраздел 2.5.2 «Расширяемый язык разметки XML» конспекта лекций по дисциплине «Электронная коммерция»).

Первые Web-сервисные программы представляли собой источники данных, которыми снабжались программные приложения. Например, компания, которая хотела интегрировать информацию о своем финансовом менеджменте в одной электронной таблице (spreadsheet), могла использовать Web-сервисы для сбора данных о банковском счёте, остатке займа, портфеле акций и текущих процентных ставках из множества различных

источников. Программа электронной таблицы использовала данные, поставляемые Web-сервисами для автоматического обновления таблицы.

Рассмотрим более сложный случай, когда компания использует Web-сервисные программы при автоматизации работы отдела закупок. После того, как агент по закупкам проверил цену и информацию о доставке и санкционировал транзакцию, Web-сервисная программа может передать заказ непосредственно на компьютер продавца и отслеживать доставку (путём связи с компьютерной системой транспортной компании) вплоть до получения товара. По мере того, как Web-сервисные программы становятся всё более сложными, они могут брать на себя функции принятия решений.

Спецификации Web-сервисов

Первым, широко используемым, средством описания Web-сервисов был *Простой Протокол Доступа к Объектам* (Simple Object Access Protocol – SOAP), представляющий собой протокол передачи сообщений, который определяет каким образом пересылать размеченные данные через компьютерную сеть, от одного программного приложения другому. Имплементация SOAP предполагает использование трёх наборов правил, которые позволяют программам работать с XML или HTML форматированными потоками данных. Правила коммуникации также включены в спецификацию SOAP.

Две другие спецификации носят наименования: *Язык Описания Web-сервисов* (Web Services Description Language – WSDL) и *Спецификация Универсального Описания, Поиска и Интеграции* (Universal Description, Discovery, and Integration Specification – UDDI). Язык WSDL используется для описания логического блока Web-сервиса, а спецификация UDDI работает как своего рода «адресная книга» для идентификации местоположения Web-сервисов и ассоциированных с ними WSDL описаний. После использования UDDI «адресной книги» для поиска WSDL описания конкретного Web-сервиса, программист может использовать информацию, содержащуюся в WSDL описании, для связи прикладных программ с Web-сервисом (некоторые программы могут, даже, реконфигурировать себя, используя информацию WSDL описания).

REST подход и RESTful проектирование

Хотя протокол SOAP продолжает широко использоваться при разработке Web-сервисов, другой подход, использующий более простые структуры, становится популярным и общеупотребительным при разработке Web-сервисов. В 2000 году, один из создателей протокола HTTP, Рой Филдинг (Roy Fielding), анонсировал подход, названный *Репрезентативная Передача Состояния* (Representational State Transfer – REST). Подход, предложенный Филдингом, представляет собой архитектурный стиль проектирования распределённого приложения, при котором каждый запрос (REST-запрос) клиента к серверу содержит в себе исчерпывающую информацию о желаемом ответе сервера (желаемом репрезентативном состоянии), и сервер не обязан сохранять информацию о состоянии клиента. Некоторые разработчики Web-сервисов, считающие протокол SOAP чрезмерно усложненным, начали использовать подход REST в своей работе.

Проектирование Web-сервисов, в соответствии с моделью REST, называют *RESTful проектирование*, а сами Web-сервисы *RESTful приложениями*. RESTful приложение передает структурированную информацию из одной точки Web в другую. Эта структурированная информация, чаще всего, представляет собой XML- или XHTML-тегированный набор данных. Web-сервис доступен по своему адресу (примерно так, как Web-страница доступна по своему URL) и к нему может обратиться любой компьютер, реализующий функции Web браузера. Более половины всех Web-сервисов сегодня являются RESTful приложениями.

Примеры RESTful приложений, можно найти на сайте ProgrammableWeb, который является лидирующим источником новостей и информации о Web APIs.

4.4. Программное обеспечение электронной коммерции для компаний, имеющих небольшие размеры

В большинстве случаев компании, имеющие небольшие размеры, создают Web-сайт, который реализует часть деятельностей компании (главным образом продвижение и продажа) независимо, и не координирует их с другими деятельностями компании.

4.4.1. Базовая услуга провайдеров услуг электронной коммерции

Вместо того, чтобы эксплуатировать свой собственный Web-сервер и всё необходимое программное обеспечение, либо покупать услугу по размещению собственного сервера в помещении провайдера, небольшие компании, как правило, используют виртуальный или выделенный хостинг. В этом случае, провайдер услуг электронной коммерции берёт на себя решение проблем, связанных с кадровым обеспечением Web-сервера, а также гарантирует круглосуточную работу Web-сервера, в том числе, и при отключении сетевого электроснабжения.

Провайдеры услуг электронной коммерции предлагают бесплатное или недорогое программное обеспечение электронной коммерции для создания коммерческого сайта на сервере провайдера. Такого рода базовая услуга часто стоит менее 30 долларов в месяц и позволяет компании быстро создать сайт и обеспечить своё присутствие в Web. Базовая услуга предназначена для онлайновых компаний, продающих не более 100 различных продуктов и осуществляющих менее 100 продаж ежедневно. Примерами провайдеров услуг электронной коммерции, специализирующихся на обслуживании небольших компаний являются Gate.com и 1&1 Internet.

4.4.2. Провайдеры услуг электронной коммерции в стиле супермаркета

Провайдеры услуг электронной коммерции в стиле супермаркета (Mall-style CSPs) обеспечивают небольшие компании базовой услугой, а также программой «тележка для покупок» и программой обработки платежей при помощи кредитных карт. Эти провайдеры взимают низкую ежемесячную оплату и могут, также, взимать одноразовую плату за оказание базовых услуг по размещению сайта. Некоторые из этих провайдеров взимают оплату (фиксированную или в виде процента от суммы продаж) за каждую транзакцию с клиентом онлайнового магазина.

В ранние дни электронной коммерции существовало много различных провайдеров услуг электронной коммерции в стиле супермаркета. Некоторые из этих провайдеров предлагали бесплатный хостинг Web-сайта в обмен на размещение на страницах сайта рекламных объявлений. Сегодня в бизнесе остались только два основных провайдера услуг электронной коммерции в стиле супермаркета: Amazon Services (программы «Professional Sellers» и «Individual Sellers») и eBay Stores. Эти провайдеры дают возможность отдельным личностям и небольшим компаниям быстро запустить онлайновый бизнес без долгосрочных обязательств и существенных инвестиций.

4.4.3. Стоимость внедрения онлайнового бизнеса для небольшой онлайновой компании

Для владельца небольшого физического магазина (продаёт не более 100 наименований товаров), который хочет начать онлайновую деятельность, важно знать стоимость создания и поддержки онлайнового магазина в том случае если он воспользуется услугами провайдера (базовыми, либо в стиле супермаркета). Как показывают, приведенные ниже, оценки, сегодня, эта стоимость колеблется в пределах 400 – 8200 долларов в течение первого года эксплуатации сайта. Оценки, приведенные в настоящем подразделе, относятся к США, однако могут быть использованы для любой другой страны путём введения поправочного коэффициента. В таблице, на рис. 4.3, приведены оценки операцион-

ных затрат в долларах США, для владельца небольшой компании, в течение первого года онлайновой деятельности.

Операционные затраты	**Оценки затрат**	
	Нижняя	Высшая
Первоначальная настройка сайта	0	200
Ежегодное обслуживание провайдером (от 20 до 300 долларов в месяц)	240	3600
Регистрация доменного имени	0	300
Сканер или цифровая фотокамера	60	2000
Программное обеспечение для редактирования фотографий	0	800
Непериодическая помощь с проектированием сайта и HTML	100	1100
Настройка кредитной карты	0	200
Общие затраты первого года	**400**	**8200**

Рис. 4.3. Примерные затраты небольшой компании на внедрение онлайнового бизнеса

Затраты, приведенные на рис. 4.3, указаны в виде нижних и высших оценок для каждого вида затрат. В зависимости от выбора провайдера и опций программного обеспечения электронной коммерции, реальные затраты могут быть немного меньше или существенно выше. Например, некоторые провайдеры предлагают бесплатную регистрацию нескольких доменных имён, если компания подписывает контракт на долгосрочное (не менее одного года) обслуживание. Провайдер может взимать плату за обработку платежей при помощи кредитных карт, которая не учитывается в оценках, на рис. 4.3. Эта плата, обычно, колеблется в диапазоне 3% – 5% от стоимости проданного товара.

Оценим, теперь, затраты небольшой компании, которая решила осуществлять собственный хостинг онлайнового магазина. Расходы на создание и поддержку Web-сайта включают расходы на: (1) оборудование, (2) связь с Интернет, (3) физическое размещение и (4) персонал. Расходы на оборудование (серверный компьютер и роутер) являются разовыми и находятся в диапазоне от 2000 до 10000 долларов. Связь с Интернет, необходимая для функционирования небольшого онлайнового магазина, стоит от 480 до 1800 долларов в год. Сервер должен размещаться в безопасном помещении, удобном для коммуникации с Интернет. Расходы на обеспечение безопасности помещения средних размеров, снабжение его средствами кондиционирования воздуха и пожаротушения могут легко достигать 5000 долларов в год. Для поддержки и эксплуатации собственного сайта компания должна располагать специалистами, в области информационных технологий, которые знакомыми с языками написания программ и сценариев для Web, пакетами программ электронной коммерции и системами управления базами данных, а также техническими специалистами, обеспечивающими работоспособность оборудования. Ежегодные расходы на персонал могут колебаться в диапазоне от 50000 до 100000 долларов. Таким образом, *средние операционные расходы небольшой компании, на собственный хостинг могут находиться в пределах от 60000 до 100000 долларов в год*. Это, примерно в 10 раз больше операционных расходов в случае использования провайдера услуг электронной коммерции.

4.5. Программное обеспечение электронной коммерции для компаний, имеющих средние размеры

Компании, имеющие средние размеры, часто самостоятельно создают коммерческие сайты, используя для этой цели специальные программные инструменты. Эти компании, также приобретают готовые программные продукты электронной коммерции, обеспечивающие функционирование коммерческих сайтов средних размеров.

4.5.1. Инструментальные программы для создания Web-сайтов

Инструментальные программы, предназначенные для создания HTML документов и Web-сайтов, такие, например, как Adobe Dreamweaver, упомянутые при изучении HTML и XML редакторов (см. подраздел 2.5.2 «HTML и XML редакторы» конспекта лекций по дисциплине «Электронная коммерция») могут применяться компаниями, имеющими средние размеры, для создания собственного программного обеспечения электронной коммерции. После создания Web-сайта при помощи инструментальной программы, разработчик сайта должен подключить к нему компоненты, реализующие коммерческие функции, такие, например, как «тележка для покупок» и программу обработки транзакций. Заключительным этапом является разработка связующего программного обеспечения для связи сайта с существующими программами бухгалтерского и складского учёта.

4.5.2. Программные продукты, обеспечивающие функционирование коммерческих сайтов средних размеров

Стоимость готовых программных продуктов, обеспечивающих работу коммерческих сайтов средних размеров, колеблется в диапазоне от 5000 до 300000 долларов и ежегодными операционными платежами в диапазоне от 1000 до 30000 долларов. Почти все программы из этой категории обеспечивают возможность подключения к базе данных или программе планирования ресурсов предприятия (ERP). Поскольку большинство отмеченных программных продуктов должны конфигурироваться с учётом специфики компании, они продаются либо в виде набора компонентов, из которых собирается конкретная конфигурация, либо в виде набора готовых версий, спроектированных для специфических видов бизнеса.

Компания Intershop продаёт пакеты программ для обеспечения функционирования систем электронной коммерции типа «бизнес-потребитель», «бизнес-бизнес» и мобильной электронной коммерции, а также услуги по их обслуживанию. Каждый пакет обеспечивает возможность работы с Web-каталогом (включая средства поиска информации в каталоге), виртуальной тележкой для покупок, программой обработки платежей при помощи платежных карт и возможность связи с существующим программным обеспечением базы данных. Пакеты, ориентированные на электронную коммерцию типа «бизнес-потребитель» и мобильную электронную коммерцию, включают много встроенных шаблонов оформления витрины магазина. Пользователи этих пакетов могут редактировать оформление витрины при помощи своего браузера. В пакетах, ориентированных на электронную коммерцию типа «бизнес-потребитель» и «бизнес-бизнес» пользователи могут отслеживать информацию о запасах на различных уровнях, видеть количество товара, создавать списки проданных товаров и пополнять запасы новыми товарами. В пакеты компании Intershop включены системы управления базами данных (СУБД), однако они могут работать с устаревшими СУБД DB2 (реляционная база данных компании IBM) или с СУБД компании Oracle.

Компания IBM производит и продаёт пакеты программ электронной коммерции IBM WebSphere Commerce для систем типа «бизнес-потребитель» и «бизнес-бизнес». Компоненты пакета IBM WebSphere включают образцы каталога, программу «мастер установки» и инструменты для работы с каталогом. Эти компоненты могут связываться с уже существующими базами данных запасов и системами снабжения. Компоненты IBM WebSphere могут, также, связываться с устаревшими базами данных через СУБД DB2 или Oracle. Для адаптации программ IBM WebSphere к специфике конкретной компании, требуется работа программистов, имеющих опыт программирования на языках JavaScript, Java или C++. Большое количество сайтов электронной коммерции средних размеров используют программы IBM WebSphere. Сайты, построенные средствами IBM WebSphere, обеспечивают такие возможности, как: виртуальная тележка для покупок; уведомление покупателя при помощи электронной почты; поддержка безопасности транзакций; продвижение и назначение скидки; отслеживание доставки; связь с системой

бухгалтерского учёта; а также локальное и удалённое администрирование при помощи браузера. Стоимость инсталляции программы WebSphere Commerce Professional Edition находится в диапазоне от 50000 до 300000 долларов в зависимости от количества опций, предоставляемых программой и количества серверных компьютеров на которых будет развернута система.

4.6. Программное обеспечение электронной коммерции для компаний, имеющих большие размеры

Программное обеспечение электронной коммерции больших компаний реализует те же возможности, что и программное обеспечение средних компаний, но должно обслуживать более высокий трафик запросов. В дополнение к этому, программное обеспечение больших компаний должно быть в состоянии реализовывать: управление контентом, управление знаниями, менеджмент цепи поставок и менеджмент отношений с клиентами.

Программное обеспечение электронной коммерции больших компаний иногда называют *программным обеспечением корпоративного класса* (enterprise-class software). Термин «корпоративный» означает, что система обслуживает множество, территориально-распределенных отделений компании и охватывает все аспекты её бизнеса. Программное обеспечение электронной коммерции корпоративного класса предлагает инструменты для систем электронной коммерции типа «бизнес-потребитель» и «бизнес-бизнес» и взаимодействует с большим количеством уже существующих систем, включая базы данных, системы бухгалтерского учёта и программы планирования ресурсов предприятия (ERP). По мере эволюции технологии электронной коммерции, большие компании, предъявляют новые требования к функциональным возможностям программного обеспечения электронной коммерции. Стоимость программного обеспечения электронной коммерции для компаний, имеющих большие размеры, колеблется в диапазоне от 200000 (базовый комплект) до 10 миллионов американских долларов.

4.6.1. Программное обеспечение электронной коммерции корпоративного класса

Программное обеспечение корпоративного класса, эксплуатируемое крупными онлайновыми компаниями, требует, для своего развёртывания, нескольких выделенных компьютеров, в дополнении к Web-серверной системе и брандмауэрам. Примерами пакетов программ корпоративного класса, которые могут использоваться крупными онлайновыми компаниями с высоким трафиком запросов могут быть: WebSphere Commerce Enterprise и Oracle E-Business Suite.

Программное обеспечение корпоративного класса, обычно, содержит инструменты для автоматической поддержки снабженческой деятельности. Существенной частью работы системы электронной коммерции типа «бизнес-бизнес» является поддержка снабженческой деятельности компании, сопровождающаяся созданием соответствующих документов, таких как заказы на приобретение требуемых материалов/инвентаря или EDI транзакционные наборы. Программное обеспечение корпоративного класса должно взаимодействовать с системой инвентаризации для *автоматического создания заказов на приобретение необходимых материалов*, а также автоматически генерировать входные данные для программы бухгалтерского учёта и программы управления ресурсами предприятия. Отметим, что программное обеспечение электронной коммерции небольших и средних компаний, обычно, предусматривает, что администратор вручную просматривает наличные материалы и размещает заказы на те материалы, которые должны быть приобретены.

В случае продажи оцифрованной информации (программное обеспечение, электронные книги, видео, музыка и т.п.) программное обеспечение корпоративного класса позволяет клиентом скачивать продукты непосредственно из сайта продавца.

Базы данных, связанные с программным обеспечением корпоративного класса, могут содержать миллионы строк информации о продуктах, ценах, профилях клиентов и

истории взаимодействия клиента с сайтом. Эта информация позволяет давать рекомендации клиентам, в случае их повторного визита. Рис. 4.4 иллюстрирует типовую архитектуру программного обеспечения корпоративного класса.

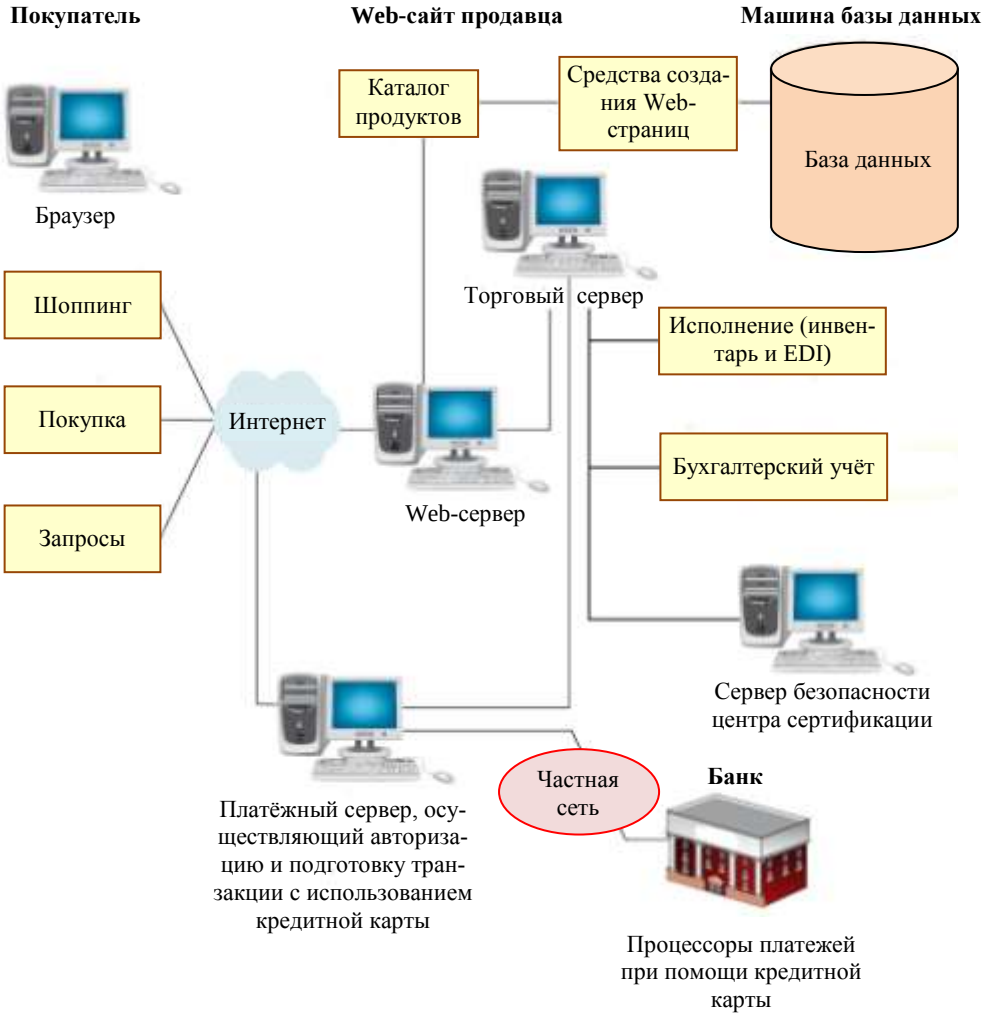

Рис. 4.4. Типовая архитектура программного обеспечения электронной коммерции корпоративного класса

Крупные компании используют Web для интеграции своих цепей поставок и управления ими (см. подраздел 1.1.2). Поэтому программное обеспечение электронной коммерции корпоративного класса должно содержать компонент, обеспечивающий управление поставками.

Компании встраивают в свои сайты элементы общения при помощи социальных сетей для привлечения покупателей и поставщиков (см. подраздел 2.1.4). Частью такой стратегии является обеспечение полезного и обновлённого контента, привлекающего внимание посетителей. Эта потребность послужила стимулом для разработки программ, обеспечивающих автоматическую ротацию контента Web-сайта.

Компании сохраняют данные об истории взаимодействия посетителей с сайтом в виде клик-потока в больших базах данных для их последующего анализа и улучшения отношений с клиентами (см. подраздел 4.6 в конспекте лекций по дисциплине «Электронная коммерция»). Клик-поток отслеживает траекторию перемещения посетителя по страницам сайта и включает информацию о том, какие страницы и в какой последовательности были просмотрены, а также, сколько времени было затрачено на изучение каждой страницы. Поэтому программное обеспечение электронной коммерции корпора-

тивного класса должно включать компонент, обеспечивающий менеджмент отношений с клиентом.

4.6.2. Программное обеспечение управления контентом

Программное обеспечение управления контентом (content management software) помогает компаниям контролировать большое количество текста, графики и медиафайлов, которые стали критически важными для ведения бизнеса. Большинство программ управления контентом включают инструменты, помогающие компании управлять информацией, сохраненной на бумажных носителях (отчёты, расписания, служебные записки и т.п.). В дополнение к символьным данным, хранящимся в традиционных базах данных, программное обеспечение управления контентом облегчает хранение и доступ ко всем типам не символьной информации: изображения, технические чертежи, географическая информация, видео- и аудио-файлы и т.д. Использование социальных сетей, как части онлайновой деятельности коммерческих компаний, сделало управление контентом ещё более важным, поскольку, сегодня, все типы Web-сайтов стали размещать на страницах своих сайтов контентную информацию. Программа управления контентом помогает компании организовать и контролировать контентную информацию, размещаемую на страницах сайта. Компании, которые используют различные способы доступа к такой корпоративной информации, как спецификации продуктов, чертежи, фотографии и результаты лабораторных тестов, часто, для управления этой информацией и доступа к ней, выбирают программы управления контентом.

Ведущими разработчиками программного обеспечения управления контентом являются компании IBM и Oracle, которые включают это программное обеспечение в свои пакеты программного обеспечения электронной коммерции корпоративного класса в виде одного из компонентов. Существует, также, несколько компаний меньшего размера, которые разрабатывают и продают отдельные пакеты программ для управления контентом. Стоимость программного обеспечения управления контентом колеблется в диапазоне от 50000 до 500000 долларов, однако стоимость их конфигурации и адаптации к специфическим условиям компании может быть в три или четыре раза больше.

4.6.3. Программное обеспечение управления знаниями

Многие компании, больших размеров, используют программное обеспечения управления контентом для упорядочивания разнообразной бизнес информации, но всё бóльшее количество таких компаний начинают понимать, что истинной ценностью являются знания, содержащиеся в этой информации которые используются коллективно. Такие компании хотят использовать программные системы, которые помогают управлять знаниями, как таковыми, а не электронным представлением файлов, содержащих эти знания. Программное обеспечение, разработанное для достижения этой цели, носит наименование *программное обеспечение управления знаниями* (knowledge management (KM) software).

Программное обеспечение управления знаниями помогает компаниям реализовать четыре основные функции: (1) накапливать и упорядочивать знания; (2) распространять знания среди пользователей; (3) расширять возможности кооперации между пользователями; (4) сохранять накопленные знания таким образом, чтобы они были полезны будущим пользователям. Программное обеспечение управления знаниями включает инструменты, которые читают электронные документы (в форматах Microsoft Word или Adobe PDF), сканы бумажных документов, сообщения электронной почты или Web-страницы. Программное обеспечение управления знаниями, часто, включает мощные средства поиска, использующие патентованные семантические и статистические алгоритмы и помогающие пользователю находить контент, человека эксперта и другие ресурсы, необходимые ему для исследования и принятия решения. Современные системы управления знаниями накапливают элементы знаний путем выделения их из взаимодействия пользователя с различной информацией.

Программа управления знаниями включена в пакет Microsoft SharePoint. Продавцом программного обеспечения управления знаниями является, также, компания IBM. Общая стоимость внедрения программного обеспечения управления знаниями, включая аппаратное обеспечение, лицензионные программы и оплату консультационных услуг колеблется в диапазоне от 10000 до 1 миллиона долларов.

4.6.4. Программное обеспечение менеджмента цепи поставок

Программное обеспечение менеджмента цепи поставок (supply chain management (SCM) software) помогает компании координировать свою деятельность с партнёрами по цепи поставок, участником которой она является. Программное обеспечение менеджмента цепи поставок реализует *две главные функции: планирование и выполнение*. Большинство компаний, продающих программы менеджмента цепью поставок, предлагают продукты, которые реализуют обе функции. Функция планирования, помогает компании строить скоординированный прогноз спроса, используя информацию от каждого участника цепи поставок. Функция выполнения, помогает решать такие задачи, как управление складом и транспортировкой. Основными продавцами программного обеспечения менеджмента цепи поставок являются JDA и Logility.

Общими компонентами программного обеспечения менеджмента цепи поставок являются компоненты, которые осуществляют: (1) планирование спроса; (2) планирование снабжения и (3) реализацию снабжения. Компонент, осуществляющий планирование спроса, анализирует шаблоны покупки и генерирует постоянно обновляющийся прогноз. Компонент, осуществляющий планирование снабжения, координирует логистику дистрибуции, прогнозирует уровень запасов, координирует совместные закупки и распределение поставок. Компонент, осуществляющий реализацию снабжения, управляет такими деятельностями, как менеджмент заказов, верификация клиентов, контроль задержек и выполнения заказа.

Стоимость инсталляции, программного обеспечения менеджмента цепи поставок, варьируется в широком диапазоне и зависит от того, как много элементов (розничные магазины, оптовые склады, дистрибьюторские центры и производственные предприятия) включены в цепь поставок. Например, розничный продавец, владеющий 500 магазинами, может заплатить от 1 до 5 миллионов долларов за пакет программ менеджмента цепи поставок, реализующий как функцию планирования, так и функцию выполнения. Владелец оптового склада с тремя или четырьмя дистрибьюторскими центрами сможет инсталлировать программу менеджмента цепи поставок стоимостью в 300000 долларов.

4.6.5. Программное обеспечение менеджмента отношений с клиентом

В дисциплине «Электронная коммерция» были рассмотрены философия и техника менеджмента отношений с клиентом (см. подраздел 4.6 конспекта лекций по дисциплине «Электронная коммерция»). Цель *менеджмента отношений с клиентом* (customer relationship management – CRM) заключается в том, чтобы понять конкретные потребности каждого клиента, а затем персонализировать продукт таким образом, чтобы удовлетворить эти потребности. Идея заключается в том, что клиенты, потребности которого были полностью удовлетворены, готовы платить больше за приобретаемые товары или услуги. Хотя, компании всех размеров могут практиковать технику менеджмента отношений с клиентом, большие компании в состоянии купить и внедрить программные продукты, автоматизирующие многие функции этого вида менеджмента.

Программа менеджмента отношений с клиентом должна получать данные от программ, которые обслуживают такие деятельности, как автоматизация продаж, операции сервисного центра и маркетинговую деятельность. Программа должна, также, собирать данные о работе клиентов с Web-сайтом компании и данные о любых других контактах компании с существующими и потенциальными клиентами. Программа менеджмента отношений с клиентом использует эти данные для помощи менеджерам в проведении такой деятельности как сбор бизнес-аналитики, планирование маркетинговых стратегий,

моделирование поведения клиентов и адаптация продуктов для удовлетворения потребностей конкретных клиентов или категорий клиентов.

В своей наиболее общей форме менеджмент отношений с клиентом использует информацию о клиентах для того чтобы продавать им больше (или с большей прибылью) товаров или услуг. Наиболее продвинутый менеджмент отношений с клиентом должен обеспечивать клиентам исключительно привлекательный и позитивный опыт на регулярной основе. Менеджмент отношений с клиентом может быть очень важным в поддерживании лояльности клиента в том бизнесе, где процесс покупки продукта является длительным и сложным. Компании, которые разрабатывают и инсталлируют заказное оборудование, прикладное программное обеспечение или офисные системы документооборота, являются примерами бизнеса с длительным и сложным процессом приобретения продукта. В этом случае программное обеспечение менеджмента отношений с клиентом может помочь поддерживать позитивные и устойчивые контакты с множеством работников компании покупателя.

Во времена систем электронной коммерции первого поколения некоторые компании тратили миллионы долларов на приобретение CRM-систем, которые предполагали полную реструктуризацию их стратегии взаимодействия с клиентами. После осознания того, что одна всеобъемлющая CRM-система не может одним махом решить все проблемы, компании перестали думать о такой системе, как об инструменте, меняющем всю стратегию отношений с клиентами, и начали применять программы, предназначенные для решения небольших и конкретных проблем. Например, компания, оказывающая услуги кабельного телевидения, может использовать CRM-систему для отслеживания, в реальном масштабе времени, перебоев в обслуживании и ремонте, но не будет требовать от такой системы рассчёта прибыльности сервиса «видео на заказ».

Одной, из наиболее популярных, сфер применимости для таких сфокусированных CRM-систем является деятельность колл-центров. Путём анализа проблем, которые выявляются при работе колл-центров, многие компании идентифицировали конкретные приложения, где программы менеджмента отношений с клиентом, могут сократить время отклика, улучшить точность и эффективность. Сегодня, большинство компаний используют небольшие, точно сфокусированные CRM-системы, направленные на решение конкретных проблем в области менеджмента отношений с клиентом. Например, мониторинг таких метрик как, частота покидания тележки для покупок, частота возврата товаров, частота просмотра страниц с описанием продуктов и другие характеристики визита клиента на Web-сайт, позволяет компании выявлять специфические элементы поведения клиентов и вносить такие изменения в сайт, которые повышают его эффективность и прибыльность.

Внедрение CRM-систем требует интеграции множества источников данных, агрегированных с аналитическими процессорами, которые могут извлекать знания из этих данных, используя постоянно обновляемые модели. На основании полученных знаний генерируются стратегии для персонализированного ценообразования, маркетинговых кампаний, специальных предложений на Web-сайте и, даже, рассылки каталогов, синхронизированной с онлайновой маркетинговой кампанией. На рис. 4.5 приведена общая структура CRM-системы.

Некоторые компании разрабатывают своё собственное программное обеспечение менеджмента отношений с клиентом, используя услуги внешних консультантов и собственный штат специалистов в области информационных технологий. Однако, бóльшая часть компаний, сегодня, приобретает готовые пакеты программ менеджмента отношений с клиентом, вместо того, чтобы создавать их самостоятельно. Компания Siebel Systems была первой компанией, специализирующейся на разработке программного обеспечения менеджмента отношений с клиентом. В 2006 году компания Oracle приобрела Siebel Systems и объединила её деятельность с уже существующим подразделением компании Oracle CRM On Demand. Другие производители прикладного программного обеспечения также предложили программное обеспечение менеджмента отношений с клиентом. Наиболее известным является SAP CRM.

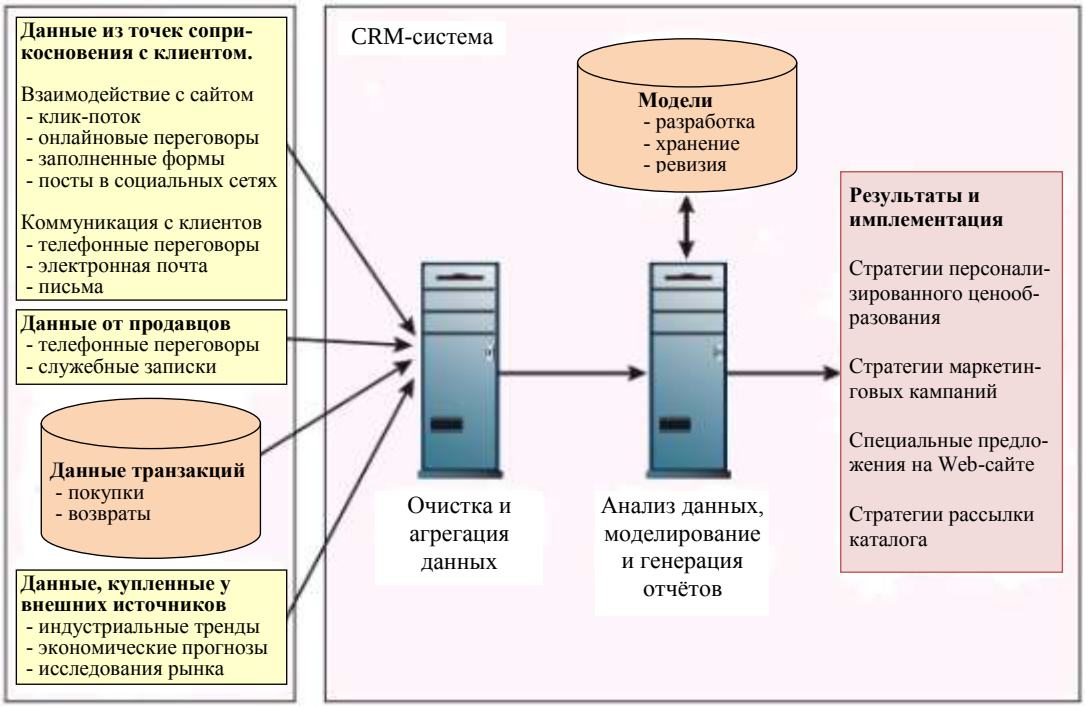

Рис. 4.5. Общая структура CRM-системы

Стоимость покупного программного обеспечения менеджмента отношений с клиентом колеблется в диапазоне от 20000 до нескольких миллионов долларов. Одним из наиболее известных продавцов программного обеспечения менеджмента отношений с клиентом, ориентированного на облачные вычисления является компания Salesforce.com.

4.7. Облачные вычисления

Установка и эксплуатация программного обеспечения электронной коммерции является сложной и дорогостоящей деятельностью, даже в том случае, когда часть этой деятельности выполняет провайдер услуг электронной коммерции. Для того, чтобы избежать затрат и усилий по планированию, инсталляции и обслуживанию аппаратного и программного обеспечения как Web-сервера, так и программного обеспечения электронной коммерции, многие компании (и малые и крупные) *передают полностью на аутсорсинг все свои вычислительные сети*, используя для этого, так называемые, облачные вычисления. *Облачные вычисления* (cloud computing) это услуга, которая позволяет множеству организаций совместно использовать сеть серверных компьютеров и их программное обеспечение, принадлежащие облачному провайдеру. Облачные вычисления обеспечивают компаниям доступ к большому массиву компьютеров с соответствующей памятью и средствами резервного копирования за меньшую цену, чем цена, которую бы они платили, если бы приобретали это оборудование самостоятельно. Облачные вычисления иногда называют *инфраструктура как услуга* (infrastructure as a service – IaaS) или *платформа как услуга* (platform as a service – PaaS).

Поскольку ресурсы облачного провайдера распределяются между множеством облачных пользователей, они могут быть перераспределены, если требования пользователей меняются. Вместо того, чтобы приобретать дополнительные сервера, при временном увеличении коммерческой активности, компания может обратиться к облачному провайдеру с просьбой увеличить количество выделенных ей ресурсов. Интернет позволяет оказывать глобальные услуги облачных вычислений. В этом случае суточная флуктуация в использовании компьютеров усредняется для облачных пользователей находящихся в различных географических областях. Например, когда деловая активность сворачивается

в Западной полусфере, она поднимается в Восточной полусфере. Поэтому глобальный облачный провайдер может обслуживать обе полусферы с меньшим количеством оборудования, чем, если бы он обслуживал пользователей каждой из полусфер в отдельности. Крупнейшими провайдерами облачных вычислений являются такие компании как Amazon, Microsoft, IBM и Google. Однако, небольшие компании, также предлагают услуги в области облачных вычислений, и совместно занимают значительную часть этого рынка. На рис. 4.6 показано распределение мирового рынка облачных вычислений между различными компаниями по состоянию на 2015 год.

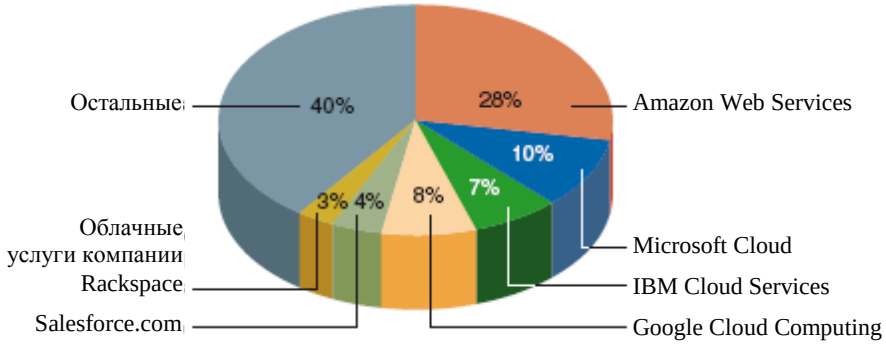

Рис. 4.6. Распределение мирового рынка облачных вычислений в 2015 году

Некоторые крупные коммерческие компании пользуются услугами нескольких облачных провайдеров. В этом случае они имеют более надежную систему резервного копирования и не зависят от одного провайдера. Компании могут быть озабочены вопросами безопасности, когда они рассматривают возможность использования облачных вычислений. Небольшие компании, обычно, приходят к заключению, что крупные облачные провайдеры обеспечивают бóльшую безопасность, чем ту, которую они могут обеспечить себе самостоятельно. Однако большие компании менее оптимистичны и часто используют стратегию *гибридных облачных вычислений* (hybrid cloud computing) которая заключается в том, что облачному провайдеру передается большой объём рутинной работы, а небольшая часть наиболее важных данных и процессов обслуживаются внутренними серверами.

ЗАДАНИЯ ДЛЯ СЕМИНАРСКИХ ЗАНЯТИЙ

1. Ваша знакомая хочет открыть небольшой Web-сайт и посвятить его садоводству. Она уверена, что её многолетний опыт в области садоводства позволил ей накопить знания об инструментах, удобрениях, гербицидах, пестицидах и т.п., необходимые тому, кто хочет заниматься садоводством. На первых порах она не хочет что-либо продавать, но, возможно, изменит свою точку зрения в будущем. Она просто хочет отображать страницы с фотографиями растений, писать и сохранять короткие «know-how» статьи для новичков, а также устанавливать ссылки на другие рекомендации в области садоводства. Ей необходим Ваш совет относительно выбора альтернативы Web-хостинга. Используя поисковый портал, разыщите информацию о стоимости услуг провайдера Web-хостинга (CSP или ISP). Затем оцените стоимость небольшого Web-сайта в терминах минимальной конфигурации аппаратуры и программного обеспечения. Оцените стоимость проектирования и создания сайта, а также ежегодные затраты на поддержку сайта. Затем выберите одну из Web-серверных программ. Оцените стоимость связи с Web. В итоге сделайте оценку двух альтернатив Web-хостинга.

2. Андрей владеет небольшим магазином, продающим ремесленные изделия и сувениры. Он хочет увеличить количество клиентов и расширить регион продаж путём

создания онлайнового отделения своего магазина. Андрей просит Вас помочь оценить стоимость создания онлайнового магазина и стоимость первого года его эксплуатации. Он предполагает, что Web-каталог будет включать информацию, примерно, о 100 товарах, а магазин будет выполнять, примерно, 20 транзакций в день. Андрей просит исследовать предложения двух провайдеров услуг электронной коммерции, предоставляющих услуги в стиле супермаркета. Андрей хотел бы получить следующую информацию.

- Стоимости: единовременная плата за установку, ежемесячная плата; плата за транзакцию.
- Размер дискового пространства, предоставляемого провайдером.
- Возможности продвижения и маркетинга.
- Возможности коммуникации с клиентом, такие как автоматическое подтверждение заказа при помощи электронной почты.
- Тележка для покупок или другие средства автоматизации заказа.
- Средства обновления витрины магазина.
- Возможность получения Web-отчётов провайдера с информацией о посетителях сайта, количества посещений сайта и т.п.

Подберите двух провайдеров услуг электронной коммерции, которые могли бы подойти Андрею и обоснуйте Ваш выбор.

3. Сделайте доклад, посвященный Web-сервисам и расширяющий информацию о Web-сервисах, приведенную в конспекте. Приведите примеры успешного применения Web-сервисов. Опишите, каким образом компании внедряют Web-сервисы и объясните почему использование Web-сервисов лучше чем использование альтернативных подходов к решению проблем в области онлайнового бизнеса.

4. Компании Amazon и Google являются двумя крупными провайдерами услуг облачных вычислений. Каждый из этих провайдеров предлагает различный набор возможностей и использует различную стратегию. Компания Amazon предлагает услуги облачных вычислений через своё отделение Amazon Web Services (AWS). AWS предоставляет клиентам возможность использовать миллионы серверов компании Amazon для покупки нужных им компьютерных мощностей на краткосрочной основе. Компании, использующие AWS должны обеспечивать себя собственными приложениями, базами данных и контентом, а AWS обеспечивает мгновенный доступ к платформе, которая может осуществлять хостинг приложений, резервное копирование и хранение и доставку контента. Компания Google совместно со своими Web-сервисами G Suite фокусирует услуги облачных вычислений на функциональной замене прикладного программного обеспечения, которые коммерческие компании должны покупать и для которых они должны обеспечивать лицензирование и эксплуатацию. Например, Google предлагает свой продукт Gmail для замены собственного сервера электронной почты и рабочие приложения (такие как Google Documents) для замены собственных текстовых редакторов, электронных таблиц, программных средств презентации и управления базой данных. Ознакомьтесь с услугами, предлагаемыми Amazon Web Services и Google Cloud Computing. Подготовьте сообщение, в котором сравните услуги облачных вычислений обеих компаний. Отметьте и обсудите различия в маркетинговой стратегии компаний по продаже услуг облачных вычислений.

5. Отделение Club Car американской компании Ingersoll-Rand производит и продаёт небольшие электромобили для гольф клубов и других потребителей. В 2001 году продажа электромобилей уменьшилась. Для выявления потребностей своих клиентов и увеличения продаж компания инсталлировала всеобъемлющую CRM-систему стоимостью в 2 миллиона долларов, однако опыт её эксплуатации оказался негативным. Система была малополезной и обременительной как для продавцов, так и

для менеджеров по продажам. В результате анализа были обнаружены две главные причины низкой эффективности системы: (1) процесс ввода заказа занимал значительное время продавца и не позволял персонализировать продукт; (2) продавцы не имели доступа к информации, позволяющей осуществлять точный и своевременный прогноз. В 2002 году CRM-система была переделана с фокусировкой на устранение отмеченных причин. Новая система позволяла торговым представителям участвовать в доработке заказа. Отделение смогло упростить деятельность по вводу заказа и сократить время продавца. Продавцы получили доступ к системе и возможность, вместе с клиентами, конфигурировать электромобиль. Продавцы получили доступ к информации о ценообразовании и возможность рассматривать, вместе с клиентами, различные альтернативы цены. Они могли изучать производственный график и осуществлять более точную оценку даты доставки. Доступ к перечисленной информации осуществляется удалённо и в реальном масштабе времени. В итоге, внедрение новой CRM-системы привело к увеличению количества продаж.

- Перечислите типы информации, которые CRM-система отделения Club Car, делает доступной торговым представителям на местах. Для каждого типа информации объясните, как удалённый доступ к этой информации может помочь торговому представителю осуществить продажу.
- Рассмотрите, было бы полезным для торгового представителя Club Car программное обеспечение управления контентом и знаниями. Предложите возможное использование этого программного обеспечения в Club Car.
- Новая CRM-система для Club Car сфокусирована на двух проблемах менеджмента отношений с клиентом. Объясните, почему этот подход работает лучше, чем внедрение всеобъемлющей CRM-системы, которая могла бы отслеживать в реальном масштабе времени всю деятельность отделения, связанную с продажами.
- Опишите преимущества, которые отделение Club Car может получить при использовании программного обеспечения менеджмента отношений с клиентов, ориентированного на облачные вычисления.

6. Подготовьте обзор современного состояния технологий Web-сервисов. Посетите сайты электронного правительства таких городов как Москва и Киев и ознакомьтесь с онлайновыми услугами, которые электронное правительство этих городов оказывает своим гражданам. Ознакомьтесь с состоянием вопроса о создании электронного правительства города Одессы. Составьте список услуг, которые электронное правительство города Одессы должно, с Вашей точки зрения, оказывать гражданам. Опишите, каким образом реализация этих услуг на сайте электронного правительства города Одессы может быть осуществлена средствами технологии Web-сервисов.

5. БЕЗОПАСНОСТЬ ЭЛЕКТРОННОГО БИЗНЕСА

Web-сайты крупных коммерческих компаний и некоммерческих организаций ежеминутно подвергаются атакам потенциальных злоумышленников, квалификация которых колеблется в диапазоне от опыта школьников старших классов и до хорошо подготовленных профессионалов, нанимаемых конкурентами. Программное обеспечение, используемое потенциальными злоумышленниками, как правило, находится в свободном доступе, поэтому правительственные агентства, неправительственные организации, коммерческие компании и индивидуальные пользователи должны ожидать, что их компьютеры могут быть просканированы в любой момент.

Вопросы безопасности систем электронной коммерции должны быть постоянно в фокусе внимания руководителей компаний и организаций, поскольку характер угроз и возможности, атакующих постоянно эволюционируют и совершенствуются.

5.1. Обзор вопросов онлайновой безопасности

Пользователи Интернет озабочены вопросами безопасной работы в онлайне начиная с того времени, когда Интернет стал средством коммуникации в коммерческой деятельности компаний. Эти озабоченности неуклонно возрастали, по мере того, как увеличивалось разнообразие онлайновых транзакций. Сегодня, вопросы безопасности являются одними из наиболее важных, для всех участников онлайновой коммуникации, вне зависимости от вида деловой активности.

5.1.1. Истоки стандартов безопасности компьютерных систем

Один из первых стандартов в области компьютерной безопасности был разработан в Министерстве обороны США и опубликован в конце 1970-х годов в книге «Критерии определения безопасности компьютерных систем» (Trusted Computer System Evaluation Criteria). Публикацию этого стандарта стали называть «Оранжевой книгой» (Orange Book), поскольку её обложка была оранжевого цвета. Текст книги находится в свободном доступе в Интернете. В книге изложены правила контроля доступа, включая разделение конфиденциальной, секретной и высоко секретной информации, а также установлены критерии уровня сертификации компьютеров, с точки зрения безопасности, от уровня D (ненадёжный) до уровня A1 (наиболее надёжный).

Когда компании начали использовать компьютеры в своей деятельности, они адаптировали военные методы безопасности, включая: физический контроль доступа к компьютерам (дверная сигнализация); бейджи/жетоны безопасности, камеры слежения и т.п. В те времена, для работы с большими компьютерами, использовались терминалы, и существовало всего несколько компьютерных сетей, которые располагались в пределах организации, владеющей сетью. Поэтому безопасность могла быть обеспечена контролем за деятельность небольшого количества людей, находящихся за терминалом или в помещении с компьютером. Сегодня, популяция компьютерных пользователей и способов доступа к компьютерным ресурсам возросла драматически, а компьютеры транспортируют «дорогостоящую» информацию, такую как электронные платежи, заказы на приобретение товаров, информацию о крупных финансовых транзакциях. Эти факторы делают постоянный и всеобъемлющий контроль за безопасностью более важным, чем когда бы то ни было.

5.1.2. Компьютерная безопасность и управление рисками

Компьютерная безопасность это защита информационных активов от несанкционированного доступа, использования, изменения или разрушения. Существуют два общих типа безопасности: *физическая безопасность* и *логическая безопасность*. Физическая безопасность включает материальные средства защиты, такие как сирены и звонки для подачи сигналов тревоги, ограждения, противопожарные двери, сейфы или безопасные

хранилища, бомбоубежища и т.п. Защита информационных активов, использующая не физические средства, называется логической безопасностью. Любое действие или объект, представляющие опасность для информационных активов, называется *угрозой*. *Контрмера* это процедура, которая распознаёт, уменьшает или устраняет угрозу. Величина и стоимость контрмеры варьируется в зависимости от важности информационного актива, подвергающегося угрозе.

Маловероятные угрозы могут быть проигнорированы, когда стоимость контрмер превышает ценность информационного актива. Например, целесообразно строить систему защиты компьютерной сети от торнадо в тех регионах, где торнадо является частым явлением (американский штат Оклахома), однако нецелесообразно строить такую систему в регионах, где вероятность торнадо крайне низка (город Одесса). На рис. 5.1 изображена *модель управления рисками* (risk management model) *информационных активов*. Модель иллюстрирует четыре вида деятельности, которые может осуществлять организация/компания в зависимости от степени влияния угрозы (стоимости вреда) на информационный актив и вероятности угрозы. На модели, изображенной на рис. 5.1, торнадо в штате Оклахома нужно поместить во второй квадрант, а торнадо в городе Одессе – в четвёртый квадрант.

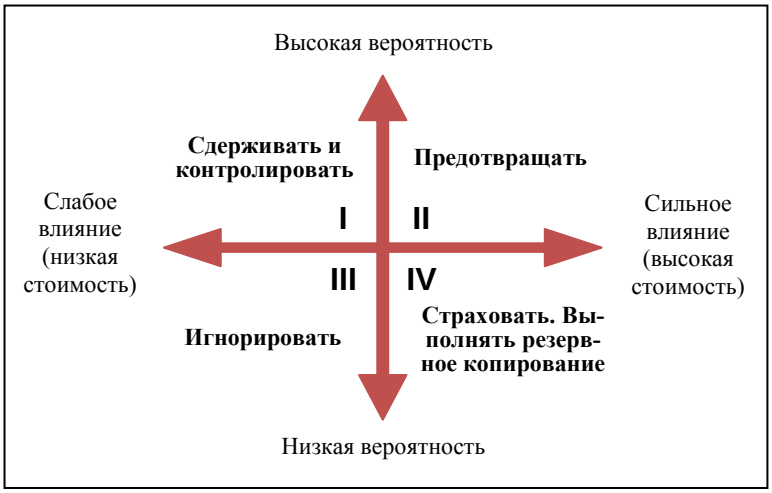

Рис. 5.1. Модель управления рисками информационных активов

Модель на рис. 5.1 может использоваться для защиты систем электронной коммерции от физических и электронных угроз. Примерами электронных угроз является деятельность мошенников или самозванцев, перехватчиков данных и воров. Перехватчик данных (eavesdropper), в этом контексте, это личность, которая может перехватывать и копировать данные, передаваемые в Интернет. Людей, которые пишут программы для получения несанкционированного доступа к компьютерам и компьютерным сетям часто называют хакерами.

Хакер (hacker) это личность, обладающая технологическими знаниями и навыками, и использующая эти навыки для несанкционированного входа в компьютерную сеть с целью похищения или разрушения данных или программного обеспечения или, даже, для разрушения аппаратного обеспечения. Первоначально термин «хакер» использовался в позитивном смысле для обозначения программиста, который в состоянии написать сложный код, тестирующий ограничения применимости технологии. Хотя термин «хакер» всё ещё используется в позитивном смысле, средства массовой информации и общественность чаще применяют его для обозначения тех, кто использует свои навыки в преступных целях.

Для внедрения эффективной схемы безопасности, компании должны идентифицировать угрозы, определить каким образом можно защитить информационные активы, подвергающиеся угрозам и рассчитать стоимость затрат на создание системы защиты своих информационных активов.

5.1.3. Элементы компьютерной безопасности

Компьютерная безопасность включает три основных элемента: секретность, целостность и необходимость (также известная как отказ в обслуживании (denial of service – DoS)). *Секретност*ь (secrecy) относится к защите от несанкционированного предоставления данных и гарантирование подлинности (аутентичности) источника данных. *Целостность* (integrity) относится к предотвращению несанкционированной модификации данных. *Необходимость* (necessity) относится к предотвращению задержек или отказов в доступе к данным.

Угроза целостности данным мало известна широкой публике. Нарушение целостности происходит, например, когда перехватывается сообщение электронной почты и его содержание изменяется, прежде чем сообщение попадает к получателю. Иными словами целостность сообщения нарушается. В этом виде атаки, который называется «человек посередине» (man-in-the-middle) содержание сообщения электронной почты часто изменяется таким образом, чтобы исказить его первоначальное значение.

Нарушение необходимости предполагает предотвращение или задержку доступа к данным. Например, онлайновый злоумышленник может задержать сообщение, содержащее заказ на приобретение акций. Если стоимость акций возрастает за время задержки, то отправитель сообщения терпит убытки. Другое нарушение необходимости включает такую деятельность как подавление Web-сайта огромным количеством запросов от поддельных клиентов, что не позволяет обычным клиентам получить доступ к сайту.

5.1.4. Установление политики безопасности

Любая компания, занимающаяся электронным бизнесом и заботящаяся о защите своих информационных активов, должна придерживаться некоторой политики безопасности. Политика безопасности это утверждения относительно того, какие информационные активы должны быть защищены и почему, кто несёт ответственность за эту защиту, а также какая деятельность является допустимой. Политика безопасности представлена постоянно обновляемым документом, который содержит утверждения относительно физической безопасности, безопасности компьютерной сети, санкционированного доступа, защиты от компьютерных вирусов и восстановления системы после несчастных случаев.

Большинство компаний и организаций придерживаются следующих четырех шагов, при создании своей политики безопасности.

1. Определение информационных активов, которые должны быть защищены, и угроз, от которых эти активы должны быть защищены. Например, компания, которая хранит номера кредитных карт своих клиентов, может решить, что эти номера являются активом, который нуждается в защите.
2. Определение субъектов, которым нужны информационные активы компании. Некоторые из этих субъектов могут находиться за пределами компании (например, поставщики, клиенты, стратегические партнёры).
3. Идентификация доступных или необходимых ресурсы для защиты информационных активов и гарантия доступа к этим ресурсам тем, кто в них нуждается.
4. Используя информацию, полученную в предыдущих трёх шагах, компания создает документально оформленную политику безопасности.

После того как документально оформленная политика безопасности утверждена менеджментом, компания направляет ресурсы на приобретение аппаратного и программного обеспечения, а также физического оборудования, необходимого для внедрения политики безопасности.

Всеобъемлющая политика безопасности должна включать аутентификацию пользователей и реализовывать основные элементы компьютерной безопасности (секретность, целостность и необходимость). Если политика безопасности используется для обеспечения безопасности системы электронной коммерции, она может быть реализована путём выполнения списка требований, перечисленных в таблице на рис. 5.2. Требования,

перечисленные на рис. 5.2, обеспечивают минимальный уровень безопасности для большинства операций в области электронной коммерции.

Требование	Значение
Секретность	Предотвращать чтение сообщений и бизнес-планов, а также получение номеров кредитных карт или получение другой конфиденциальной информации для неавторизованных личностей.
Целостность	Заключать информацию в цифровые конверты так, что компьютер может автоматически обнаружить сообщения, которые были изменены при транзите.
Доступность	Обеспечивать гарантированную доставку сообщения (или его сегмента), так, что потеря сообщения (или его сегмента) всегда могут быть обнаружена.
Управление ключами	Обеспечивать безопасную дистрибуцию и управление ключами, которые необходимы для безопасной коммуникации.
Неотказуемость	Для каждого сообщения предоставлять неопровержимую цепь доказательств его источника и адресата.
Аутентификация	Надёжно идентифицировать клиентов и сервера при помощи цифровых подписей и сертификатов

Рис. 5.2. Требования, обеспечивающие минимальный уровень безопасности в области электронной коммерции

Меры безопасности должны работать совместно для предотвращения несанкционированного чтения, модификации или разрушения информационных активов. Хорошая политика безопасности должна отвечать на следующие вопросы:

- Аутентификация: Кто пытается получить доступ к сайту?
- Контроль доступа: Кому разрешён вход в систему и доступ к сайту?
- Секретность: Кому разрешается видеть избранную информацию?
- Целостность данных: Кому разрешается изменять данные?
- Аудит: Кто (или что) и когда является причиной совершения конкретных событий?

Далее будут рассмотрены вопросы применения политики безопасности к онлайновой деятельности. Материал расположен таким образом, чтобы следовать за процессом обработки транзакции, начиная от клиента и заканчивая Web-сервером, на котором размещён коммерческий сайт. Каждое логическое звено этого процесса включает информационные активы, которые должны быть защищены: компьютер клиента, канал коммуникации, по которому передаются сообщения, а также Web-сервер и компьютеры, которые к нему подключены.

5.2. Безопасность компьютера Web-клиента

Клиентские компьютеры, включая планшеты и смартфоны, должны быть защищены от угроз, которые исходят от программ и данных получаемых из Интернет. Другой угрозой для клиентского компьютера могут быть мошеннические сайты, которые маскируются под легитимные. Такие сайты пытаются, обманным путём, вовлечь своих посетителей в передачу им личной и конфиденциальной информации.

5.2.1. Куки-файлы и Web-маяки

Коммуникация между Web-клиентом и Web-сервером осуществляется множеством независимых передач, поэтому не существует непрерывной во времени связи (открытой сессии) между клиентом и сервером. Куки-файлы (см. подраздел 4.2.2) это небольшие файлы, которые сервер размещает на клиентском компьютере для идентификации посетителей, повторно посещающих сайт. Куки-файлы позволяют серверу обслуживать (без

открытой сессии) функции виртуальной тележки для покупок, путём сохранения информации о посетителе сайта в промежутках между сессиями.

Существуют два способа категоризации куки-файлов: (1) по продолжительности во времени; (2) по источнику.

По продолжительности куки-файлы делят на два вида: *сессионные куки-файлы* (session cookies) и *постоянные куки-файлы* (persistent cookies). Сессионные куки-файлы существуют только в течение сессии и удаляются после её завершения. Постоянные куки-файлы остаются на клиентском компьютере неопределённо долго. Сайты электронной коммерции используют оба этих вида куки-файлов. Например, сессионные куки-файлы могут содержать информацию о шопинге во время текущего визита, а постоянные куки-файлы – информацию об авторизации, которая помогает сайту распознать посетителя при его последующем визите. Каждый раз, когда браузер перемещается по коммерческому сайту, сервер просит клиентский компьютер вернуть ему все куки-файлы, которые он ранее сохранил на этом клиентском компьютере.

Второй способ категоризации делит куки-файлы на два вида в зависимости от их источника. Куки-файлы могут помещаться на клиентский компьютер Web-сайтом сервера, и в этом случае они называются *куки первой стороны* (first-party cookies). Куки-файлы могут, также, помещаться на клиентский компьютер сторонним Web-сайтом, и в этом случае они называются *куки третьей стороны* (third-party cookies). Источником куки-файлов третьей стороны является сайт, отличный от сайта, с которым в данный момент работает клиент. Сайт третьей стороны может транспортировать рекламные сообщения, появляющиеся на страницах сайта, с которым в данный момент работает клиент. Сайт третьей стороны, передающий рекламные сообщения, заинтересован в отслеживании откликов со стороны клиентов, и, если этот сайт размещает рекламные сообщения на большом количестве сайтов, он может использовать постоянные куки-файлы третьей стороны для отслеживания клиентов.

Посетитель Web-сайта может защитить себя от раскрытия частной информации, или от отслеживания при помощи куки-файлов, путём полного отключения функции запоминания куки-файлов в своём браузере. Это наиболее радикальный способ, который обладает тем недостатком, что браузер блокирует все куки-файлы, включая полезные, и клиент должен повторно вносить одну и ту же информацию при повторном посещении сайта. Доступ к ресурсам некоторых сайтов, в полном объеме, не доступен для посетителей, браузеры которых блокируют куки-файлы. Например, большинство онлайновых обучающих курсов на школьных и университетских сайтах, не работают правильно, если браузер студента блокирует куки-файлы. Большинство браузеров могут быть настроены таким образом, чтобы блокировать только куки-файлы третьей стороны или получать согласие посетителя сайта перед сохранением куки-файла.

Некоторые рекламодатели транспортируют (с серверов третьей стороны), на страницы сайта изображения, которые настолько малы, что остаются невидимыми. *Web-маяком* (Web-beacon) называется крошечное графическое изображение, которое сайт третьей стороны размещает на странице другого сайта. Когда клиент загружает такую страницу на свой компьютер, Web-маяк может записать куки-файл на компьютер клиента. Таким образом, единственной целью Web-маяка является обеспечение возможности для сайта третьей стороны (идентичность которого не известна клиенту) разместить свой куки-файл на клиентском компьютере. Интернет рекламодатели иногда называют Web-маяки «*прозрачные GIF-файлы*» (clear GIFs) или «*1-на-1 GIF-файлы*» (1-by-1 GIFs), поскольку они могут быть созданы в виде графических изображений в GIF формате со значением цвета «прозрачный» и размером 1 x 1 пиксель.

5.2.2. Активный контент

Многие Web-сайты используют динамические страницы для создания страниц, содержание которых удовлетворяет потребностям каждого отдельного пользователя. Другим способом персонализации Web-страниц является встраивание программ в страницы. Эти программы называются *активным контентом* (active content) и выполняются на

клиентском компьютере после загрузки страницы, содержащей активный контент. Программы активного контента могут перемещать графические изображения, загружать и проигрывать аудио файлы и выполнять другую работу. Эти программы могут, также, помещать товары в тележку для покупок и вычислять общую сумму счёта, включая налог на продажу, стоимость обработки и доставки. Таким образом, при помощи активного контента можно перенести часть работы по формированию и обработки заказа с сервера на компьютер клиента. Однако, поскольку активный контент является программой, он может представлять угрозу для компьютера клиента.

Для доставки активного контента на компьютер клиента могут использоваться такие средства как куки-файлы, графика, плагины браузера, Java-апплеты, сценарии JavaScript, VBScript и элементы управления ActiveX. Доставка активного контента на компьютер клиента может осуществляться и при помощи вложения в сообщение электронной почты. Настройки большинства браузеров позволяют отключать использование Java-апплетов и JavaScript, однако, поскольку многие сайты используют эти средства для реализации важных функций, пользователи, часто, оставляют их включенными. Языки JavaScript и VBScript являются языками сценариев и позволяют создавать сценарии, выполняемые клиентским компьютером. Апплет это небольшая прикладная программа. Апплеты выполняются Web-браузером и, чаще всего создаются при помощи языка программирования Java. Программа активного контента начинает выполняться браузером автоматически, когда он загружает страницу содержащую активный контент. Настройки большинства браузеров позволяют пользователю ограничить действия Java-апплетов и JavaScript или VBScript сценариев рамками «*песочницы*» (sandbox). Когда Java-апплет или сценарий выполняется в песочнице, программа активного контента не имеет полного доступа к клиентскому компьютеру. Например, Java-апплет не может выполнять действия по вводу или выводу файлов или операции удаления данных. Это предотвращает нарушение секретности (чтение данных) и целостности (модификацию или удаление данных).

Элемент управления ActiveX представляет собой объект, содержащий программу. В отличие от Java кода или JavaScript кода элементы управления ActiveX выполняются только на компьютерах, управляемых операционной системой Windows. Угроза безопасности исходящая от элементов управления ActiveX заключается в том, что после загрузки они выполняются как обычные программы и имеют доступ ко всем ресурсам компьютера, включая операционную систему. Злонамеренный активный контент в виде элемента управления ActiveX может переформатировать жесткий диск, переименовать или удалить файлы, отослать сообщения электронной почты всем адресатам, указанным в адресной книге, или просто выключить компьютер. Поэтому такой активный контент может нарушить все основные элементы безопасности: секретность, целостность и необходимость. Большинство браузеров могут быть настроены таким образом, чтобы предупреждать пользователя об элементе управления ActiveX, предотвращая, таким образом, его загрузку.

Поскольку модуль активного контента встроен в Web-страницу, он полностью невидим для пользователя, воспринимающего эту страницу. Хакеры, стремящиеся нанести повреждения клиентскому компьютеру, могут встроить вредоносный активный контент в Web-страницу, выглядящую вполне безобидно. Эта техника доставки активного контента носит наименование *Троянский конь* (Trojan horse). Троянский конь это программа, спрятанная внутри Web-страницы (другой программы), маскирующей её истинную цель. Троянский конь может сканировать клиентский компьютер и отсылать на сервер хакера частную информацию, нарушая, тем самым, секретность данных. Троянский конь может изменять или удалять информацию, нарушая, тем самым, целостность данных. Один из видов Троянского коня называется *Зомби* (Zombie). Зомби называют программу, которая секретно захватывает чужой компьютер для того чтобы атаковать другие компьютеры. Компьютер, который захватывает программа Зомби, иногда, тоже называют Зомби. Когда Троянский конь захватывает большое количество компьютеров и превращает их в Зомби, личность, запустившая Троянского коня, может управлять всеми этими компьютерами и формировать, так называемую, *бот-сеть* (botnet, сокращение от robotic network). Бот-сеть, также называют *Зомби фермой*, поскольку в ней все компьютеры являются Зомби.

Бот-сеть может действовать как атакующий блок для рассылки спама или совершения других видов атак.

5.2.3. Графика и плагины браузера

Некоторые форматы графических файлов были сконструированы специально для того, чтобы содержать инструкции о том, как представлять графику. Это означает, что любая Web-страница, содержащая графическое изображение, является потенциально опасной, поскольку, если в графику встроен код, то он может причинить вред компьютеру клиента.

Плагины браузера (browser plug-ins) представляют собой программы, расширяющие возможности браузера. Плагины браузера, также, несут угрозу, поскольку могут обрабатывать Web-контент так как это не может делать браузер. Плагины браузера позволяют браузеру выполнять такую полезную работу как проигрывание аудио- или видео-файлов, однако они же могут представлять опасность, поскольку могут выполнять код, скрытый в аудио- и видео-файлах. Этот скрытый код может, например, удалить некоторые или все файлы с клиентского компьютера.

5.2.4. Вирусы, черви и антивирусное программное обеспечение

Большинство пользователей знает, что вложения электронной почты могут нести угрозу для клиентского компьютера. В качестве вложений могут использоваться практически любые файлы (текстовые документы, электронные таблицы, базы данных, изображения и т.п.). Большинство программ, включая программу почтового клиента Web-браузера, отображают вложения путём автоматической загрузки и выполнения ассоциированной программы. Например, текстовый редактор Word автоматически загружается и отображает текстовый документ. Хотя деятельность по отображению текстового документа сама по себе безопасна, макровирусы, находящиеся внутри загружаемых файлов, могут причинить вред компьютеру клиента.

Компьютерный *вирус* (virus) это программа, которая прикрепляет себя к другой программе (хост программе) и начинает работать тогда, когда активируется хост программа. Компьютерный *червь* (worm) это тип вируса, который воспроизводит себя на заражённом компьютере. Компьютерные черви могут быстро распространяться через Интернет. *Макровирус* (macro virus) это тип вируса, которая кодируется как небольшая программа, называемая макрос, и встраивается в текстовые файлы или электронные таблицы, предназначенные для работы с программами, использующими макросы, такими как Microsoft Word или Excel. История компьютерных вирусов, червей и других вредоносных программ начинается в 1980-х годах. В таблице, на рис. 5.3, перечислены некоторые из наиболее известных ранних вредоносных программ и описана их история.

Первым вирусом, ставшим главной мировой новостью, стал вирус ILOVEYOU и его варианты. Вирус ILOVEYOU появился в 2000 году и, как выяснилось позже, был разработан 23-х летним студентом, жившем на Филиппинах. Вирус быстро распространялся и поражал клиентские компьютеры через вложения электронной почты. Он инфицировал любой компьютер того, кто открывал заражённое вложение и засорял систему электронной почты тысячами копий бесполезных сообщений. Вирус быстро распространялся при помощи широко известной клиентской программы электронной почты Microsoft Outlook, поскольку автоматически рассылал сам себя по 300 адресам, хранящимся в адресной книге программы Microsoft Outlook. Кроме того, что вирус воспроизводил сам себя взрывоподобным образом при помощи сообщений электронной почты, он, также причинял другой вред инфицированному компьютеру. Вирус ILOVEYOU разрушал файлы с музыкой и фотографиями, а также разыскивал в инфицированном компьютере пароли пользователя и пересылал эту информацию злоумышленнику, создавшему вирус. В течение, всего лишь, одного дня вирус заразил около 40 миллионов компьютеров более чем в 20 странах мира и причинил ущерб, который оценили в 9 миллиардов американских долларов.

Год	Наименование	Тип	Описание
1986	Brain	вирус	Создан в Пакистане. Вирус инфицировал гибкие диски, которые использовались на персональных компьютерах того времени. Он занимал свободное пространство гибкого диска и препятствовал записи на него данных.
1988	Internet Worm	червь	Автором червя является Роберт Моррис, который распространил этот самовоспроизводящийся и самораспространяющийся вирус через Интернет. Червь остановил работу компьютеров в университетах, военных и медицинских учреждениях по всему миру.
1991	Tequila	вирус	Создан в Швейцарии и распространялся через файлы, загружаемые из Интернет. Вирус записывал себя на жёсткий диск и активизировался каждый раз, когда включался компьютер. Инфицировал исполняемые программы.
1992	Michelangelo	Троянский конь	Активизировался 6 марта в день рождения Микеланджело и затирал значительную часть жёсткого диска инфицированного компьютера.
1993	SatanBug	вирус	Инфицировал выполняемые программы, которые начинали работать неправильно, или останавливались. Вирус был сконструирован так, чтобы взаимодействовать с антивирусными программами и препятствовать его обнаружению.
1996	Concept	макровирус, червь	Один из первых вирусов, который был написан на языке макросов Microsoft Word и распространялся через инфицированные текстовые документы. Когда открывался инфицированный документ, Concept помещал макрос в шаблон документа по умолчанию, что приводило к инфицированию любого нового текстового документа, создаваемого на компьютере.
1999	Melissa	макровирус, червь	Microsoft Word макровирус, который распространялся автоматически при помощи электронной почты. Вирус распространился по всему миру в течение нескольких часов. Компания Microsoft была вынуждена закрыть свои почтовые сервера для того чтобы остановить распространение вируса внутри компании.

Рис. 5.3. Ранние компьютерные вирусы, черви и Троянские кони

В 2001 году интенсивность атак компьютерных вирусов возросла и превысила 40000 случаев нарушения безопасности. Лидерами атак стали программы Code Red и Nimda, представлявшие собой комбинацию компьютерного вируса и червя. Каждый из этих вирусов поразил миллионы компьютеров. Как Code Red, так и Nimda являются примерами *многовекторного вируса* (multivector virus), поскольку они могут проникать в компьютер различными путями (векторами).

Новая версия вируса Code Red, названная BugBear, появилась в 2003 году. Вирус распространился через почтового клиента Microsoft Outlook. Пользователь, получивший зараженное сообщения, даже не должен был открывать вложение, BugBear начинал атаку через «лазейку» безопасности, существующую между Microsoft Outlook и браузером Internet Explorer. После запуска, вирус пытался обнаружить и уничтожить антивирусную программу, а затем инсталлировал Троянского коня, который обеспечивал злоумышленнику доступ к компьютеру и позволял ему загружать на, либо выгружать из компьютера файлы по своему желанию. После этого BugBear рассылал инфицированные сообщения электронной почты. Для этого он использовал уже отправленные сообщения из адресной книги, что часто обманывало получателя. Вирус BugBear было трудно удалить, поскольку он случайным образом переименовывал файлы на каждом инфицированном компьютере. В таблице, на рис. 5.4, приведен обзор перечисленных и других известных вредоносных программ, которые поразили миллионы клиентских компьютеров по всему миру с 2000 по 2007 годы.

Год	Наименование	Тип	Описание
2000	ILOVEYOU	вирус, червь	Вирус попадает в компьютер вместе с вложением почтового сообщения с заголовком ILOVEYOU. Рассылает свою копию по адресам, указанным в адресной книге программы Microsoft Outlook и может разрушать файлы с фотографиями и музыкой.
2001	Code Red	вирус, червь, Троянский конь	Может инфицировать Web-сервера и персональные компьютеры. Повреждает Web-страницу, передаётся от сервера на клиентский компьютер и даёт хакеру возможность контролировать сервер. Вирус может восстанавливаться из скрытых файлов после удаления.
2001	Nimda	вирус, червь	Изменяет Web-документы и некоторые программы на инфицированном компьютере. Создает множество своих копий в файлах с различными именами. Может передаваться через электронную почту, локальные сети и от Web-сервера к WEb-клиенту.
2002	BugBear	вирус, червь, Троянский конь	Распространяется через электронную почту и локальные сети. Обнаруживает антивирусные программы и пытается их дезактивировать. Вирус может регистрировать и сохранять нажатия клавиш и позже передавать их через Троянского коня, который инсталлируется на инфицированный компьютер. Троянский конь позволяет хакеру загружать на компьютер и выгружать из компьютера различные файлы.
2002	Klez	вирус, червь	Передаётся через вложения электронной почты. Перезаписывает файлы, создаёт скрытые копии оригинальных файлов и пытается дезактивировать антивирусные программы.
2003	Slammer	червь	Главной целью этого червя является демонстрация того как быстро червь может передаваться через Интернет. Он инфицировал 75000 компьютеров в течение первых 10 минут своего распространения.
2003	Sobig	Троянский конь	Превращает компьютер в точку ретрансляции спама и передаёт потенциальным жертвам огромное количество почтовых сообщений вместе со своей копией.
2004	MyDoom	червь, Троянский конь	Превращает инфицированный компьютер в Зомби, участвующий в атаке на Web-сайт конкретной компании.
2004	Sasser	вирус, червь	Создан немецким школьником. Ищет компьютеры со специфической уязвимостью в безопасности и инфицирует их. Инфицированный компьютер замедляет работу и должен быть перезагружен.
2005	Zotob	червь, Троянский конь	Инфицирует компьютеры со специфической уязвимостью. Регистрирует нажатия клавиш, копирует содержимое монитора и ворует учётные данные аутентификации. Инфицированный компьютер может использоваться как зомби для массовой рассылки сообщений.
2006	Nyxem	червь, Троянский конь	Дезактивирует программы безопасности и обмена файлами и разрушает документы, созданные Microsoft Office. Активизируется третьего числа каждого месяца и рассылает себя при помощи почтовых сообщений.
2006	Leap	вирус, червь	Называется также Oompa-Loompa. Инфицирует программы, выполняемые под управлением операционной системы Macintosh OS-X. Распространяется через систему обмена сообщениями iChat.
2007	Storm	червь, Троянский конь	Собирает инфицированные компьютеры в бот-сеть через которую распространяет спам. Распространяется через электронную почту.

Рис. 5.4. Компьютерные вирусы, черви и Троянские кони: 2000 – 2007 годы

В начале 2008 года появился и широко распространился вирус Conficker. Вирус инфицировал около 15 миллионов компьютеров и всё ещё остаётся опасным, поскольку может реинсталлировать сам себя после удаления. Масштабы инфицирования привели к тому, что некоторые провайдеры услуг Интернет, фирмы, занимающиеся компьютерной безопасностью и онлайновые компании, сформировали рабочую группу для мониторинга вируса. Рабочая группа продолжала свою деятельность более года, пока существенно не уменьшилось количество компьютеров, инфицированных вирусом Conficker.

В 2010 Троянский конь Stuxnet впервые осуществил новый вид атаки. Впервые Троянский конь, распространяемый операционной системой, (в этом случае Microsoft Windows) был разработан для нанесения ущерба не пользовательским компьютерам общего назначения, а промышленному оборудованию. Мишенью Stuxnet были системы управления, изготовленные немецкой компанией Siemens. Эти системы используются для управления различным промышленным оборудованием, но мишенью для атаки 2010 года были системы, управляющие оборудованием для обогащения урана в Исламской Республике Иран.

В 2011 году две, ранее существующие, вредоносные программы Zeus и SpyEye были использованы для создания серии новых вариантов Троянских коней, мишенью которых была информация о банковских счетах, хранящаяся в компьютерах. Эти новые варианты Троянских коней скрывают свои файлы и ключи регистрации от менеджера файлов операционной системы Windows, что делает их обнаружение трудной задачей. Они могут перехватывать данные кредитных карт или онлайновых банковских операций, вводимые в Web-браузер, и передавать их злоумышленнику.

В конце 2013 года широко распространился Троянский конь под наименованием Cryptolocker, который атаковал компьютеры, управляемые операционной системой Windows. Работая как *программа-вымогатель* (ransomware) Cryptolocker шифровал файлы на инфицированном компьютере и требовал выкуп за получение ключа для их дешифровки. Таким образом, Cryptolocker продемонстрировал ещё один тип угрозы Интернет пользователям со стороны вредоносных программ. Как правило, Cryptolocker попадает на клиентский компьютер через вложение электронной почты, однако является многовекторным и может проникать в компьютер через Web-страницы или другое оборудование компьютерной сети. В 2014 году несколько фирм, занимающихся компьютерной безопасностью, а также производители антивирусного программного обеспечения разместили на своих сайтах ключи для дешифровки файлов, но к этому времени, хакеры, запустившие Cryptolocker, успели получить более 3 миллионов долларов в виде выкупа. Кроме того, сразу же после опубликования этих ключей, появился новый и более изощрённый вариант программы-вымогателя, под наименованием Cryptowall, что привело к необходимости разрабатывать новые ключи для дешифровки.

Комбинация Троянского коня и червя под наименованием Regin была, как считается, разработана разведслужбами в 2011 или 2012 году. Этот Троянский конь широко распространился в 2014 через *поддельные Web-страницы* (spoofed Web pages), созданные хакерами. Его трудно удалить при помощи антивирусных программ, поскольку он постоянно загружается на клиентский компьютер и инсталлирует множество своих версий. Regin может оставаться на инфицированном компьютере в течение длительного времени, регулярно передавая хакеру отчёты об активности пользователя, а также его логины и пароли.

В 2015 году распространился вариант программы-вымогателя под наименованием TeslaCrypt. Эта программа, попав на компьютер, разыскивала файлы программного обеспечения компьютерных игр, шифровала их и требовала выкуп за ключ для расшифровки файлов и доступа к игре. В течение нескольких месяцев после распространения TeslaCrypt, подразделение компании Cisco, под наименованием Talos Group разместило в Web инструментальную программу для дешифровки файлов, пораженных TeslaCrypt. Владельцы инфицированных компьютеров могли получить эту программу бесплатно. В таблице, на рис. 5.5, приведен обзор вредоносных программ, появившихся в период с 2008 по 2015 годы.

Год	Наименование	Тип	Описание
2008	Conficker	червь, Троянский конь	Может реинсталлировать себя после удаления, и по сей день инфицирует около 5 миллионов компьютеров. Может запускать массовую спам атаку или атаку типа «отказ от обслуживания» на любой Web-сервер.
2009	Clampi	червь, Троянский конь	Находился в «спящем» состоянии много лет и был активирован в 2009 году. Похитил логины и пароли более чем у 4000 сайтов финансовых институтов. Злоумышленники могут использовать эту информацию для совершения покупок или похищения финансовых средств.
2009	URLzone	червь, Троянский конь	Наблюдает за активность пользователя и перехватывает сессию, когда пользователь входит в сайт финансового института, который червь запрограммирован распознавать. Переводит деньги со счёта жертвы на счёт сообщника, получающего свою долю. На эти деньги покупаются товары, которые отсылаются на зарубежный адрес злоумышленника.
2010	Stuxnet	червь, Троянский конь	Распространяется через Microsoft Windows и поражает управляющие программы, разработанные для оборудования компании Siemens. Первый червь, созданный для атаки на промышленное оборудование. Эксперты считают, что он был создан для повреждения Иранского оборудования для обогащения урана.
2010	VBManie	вирус, Троянский конь	Передается почтовыми сообщениями с заголовком «here you have». В сообщении утверждается, что вложение содержит обещанный документ.
2011	Antispyware 2011	вирус, Троянский конь	Представляется антивирусной программой и дезактивирует настоящую антивирусную программу. Блокирует доступ в Интернет, поэтому настоящая антивирусная программа не может получить обновления для восстановления.
2011	ZeuS/SpyEye variants	червь, Троянский конь	Эти два Троянских коня были объединены для создания серии новых вариантов, предназначенных для похищения информации об онлайновых банковских операциях, находящейся на клиентских компьютерах.
2013	Cryptolocker	червь, Троянский конь	Шифрует файлы на инфицированном компьютере и требует выкуп за получение ключей, необходимых для расшифровки файлов.
2014	Regin	червь, Троянский конь	Инфицирование происходит при посещении поддельных Web-станиц со встроенным червём, который, затем, повторно реинсталлирует свои дополнительные версии, что затрудняет его обнаружение. Предназначен для длительного наблюдения за операциями на инфицированном клиентском компьютере.
2015	TeslaCrypt	червь, Троянский конь	Вариант червя Cryptolocker, который обнаруживает игровые программы, инсталлированные на инфицированном компьютере, шифрует игровые файлы и требует выкуп за предоставление ключей для расшифровки файлов.

Рис. 5.5. Компьютерные вирусы, черви и Троянские кони: 2008 – 2015 годы

Антивирусное программное обеспечение (antivirus software) обнаруживает компьютерные вирусы или компьютерных червей на клиентском компьютере и, либо удаляет их, либо делает их неработоспособными. Антивирусные программы эффективны только в том случае, если они используют актуальные файлы антивирусных данных. Файлы антивирусных данных содержат идентификационную информацию, необходимую для обнаружения вирусов на компьютере клиента. Поскольку новые вирусы появляются регуляр-

но, файлы антивирусных данных должны постоянно обновляться. В этом случае антивирусная программа сможет обнаружить и нейтрализовать новые вирусы.

Некоторые Web-системы электронной почты, такие как Gmail и Yahoo! Mail, автоматически сканируют вложения электронной почты антивирусными программами прежде чем доставить почту адресату. В этом случае антивирусные программы выполняются почтовым сервером. Одной из наиболее известных компаний, производящей и распространяющей антивирусное программное обеспечение является Лаборатория Касперского, которая осуществляет свою деятельность более чем в 200 странах мира.

5.2.5. Цифровые сертификаты

Одним из способов контроля угроз со стороны активного контента является использование цифровых сертификатов. *Цифровой сертификат* (digital certificate) представляет собой код, встроенный в Web-страницу и удостоверяющий подлинность отправителя. Цифровой сертификат включает, также, средства для отсылки зашифрованного сообщения отправителю Web-страницы. Цифровой сертификат снабжается цифровой подписью, которая выполняет ту же функцию, что и фотография в паспорте. Цифровая подпись доказывает, что держателем сертификата является сущность, идентифицируемая сертификатом. В случае, когда на клиентский компьютер загружается программа, снабжённая сертификатом, то сертификат гарантирует, что программа не поддельная и была разработана конкретной компанией. Идея цифрового сертификата, в случае загружаемой программы, в том, что если пользователь доверяет конкретному разработчику программы, то он должен доверять и самой программе, поскольку, как доказывает сертификат, она создана именно этим разработчиком.

Цифровые сертификаты используются для различных типов онлайновых транзакций, включая электронную коммерцию, электронную почту и электронные трансферты денежных средств. Цифровой сертификат подтверждает подлинность Web-сайта для покупателя и, в некоторых случаях, может подтверждать подлинность покупателя для Web-сайта. Браузер и сервер обмениваются цифровыми сертификатами автоматически и невидимо, когда запрашивают подтверждение подлинности каждого из участников транзакции.

Цифровые сертификаты выдаются организациям или отдельным личностям специальными *центрами сертификации* (certification authority). Центры сертификации требуют от лиц и организаций, подающих заявку на сертификат, предоставить им данные, доказывающие идентичность личности или организации. Если центр сертификации удовлетворён полученными данными, он выдаёт сертификат. Затем центр сертификации подписывает сертификат и эта подпись подтверждает истинность данных сертификата и прикрепляется к сертификату в форме открытого ключа шифрования. Ключ шифрования «открывает» сертификат любому, кто получил сертификат вместе с публикацией, которую он удостоверяет. Цифровой сертификат нелегко подделать и он включает шесть основных компонентов.

- Данные, идентифицирующие владельца сертификата, такие как фамилия, наименование организации, адрес и т.п.
- Открытый ключ шифрования владельца сертификата.
- Даты, в пределах которых, сертификат является действующим.
- Серийный номер сертификата.
- Наименование организации, выдавшей сертификат.
- Цифровая подпись организации, выдавшей сертификат.

Ключ шифрования представляет собой число (обычное длинное двоичное число), которое используется алгоритмом шифрования для шифрования сообщения. Длинный ключ шифрования обеспечивает более надёжную защиту от дешифрования чем короткий.

Данные, идентифицирующие владельца сертификата, варьируются от одного центра сертификации к другому. Например, от личности, желающей получить сертификат, могут, в одном случае, потребовать паспорт, а в другом – нотариально заверенные отпе-

чатки пальцев. Центры сертификации, обычно, публикуют свои требования на Web-сайтах.

Существует небольшое количество центров сертификации, поскольку выдача сертификатов связана с высоким уровнем доверия и только несколько компаний обладают репутацией, необходимой для успешной продажи цифровых сертификатов. Наиболее известными являются такие два международных центра сертификации как Thawte и Symantec Enterprise.

После того, как стало известно, что хакеры смогли получить фальшивые сертификаты, стало ясно, что центры сертификации проводят недостаточную проверку тех, кому выдают сертификаты. Это заставило многие центры сертификации разработать набор более строгих проверочных шагов, и в 2008 году были приняты новые критерии проверки. Центры сертификации, которые следовали этим, более строгим, критериям проверки, получили право выдавать новый тип цифровых сертификатов, который получил наименование *сертификат с расширенной проверкой подлинности* (Extended Validation Secure Sockets Layer certificate или сокращённо EV-SSL certificate). Для выдачи EV-SSL сертификата, центр сертификации должен подтвердить юридическое существование организации путём проверки регистрации юридического имени, номера регистрации, адреса регистрации и физического адреса организации. Центр сертификации должен, также, проверить право организации на использование доменного имени и полномочия организации на запрос о получении EV-SSL сертификата.

Ежегодная плата за цифровые сертификаты колеблется в диапазоне от 100 до, более чем, 1000 долларов, в зависимости от их характеристик (например, надёжность шифрования или принадлежность к EV-SSL сертификатам), а также от того приобретается ли сертификат отдельно или вместе с сертификатами для других Web-сайтов, принадлежащих компании. Срок действия цифрового сертификата завершается через некоторый промежуток времени (обычно равный одному году). Это, встроенное в сертификат, временно́е ограничение обеспечивает бóльшую надёжность, поскольку держатель сертификата должен периодически подтверждать своё право на сертификат. Сертификат становится недействительным либо по истечении времени его действия, либо, если он аннулируется центром сертификации. Если центр сертификации обнаруживает, что Web-сайт нарушает условия выдачи сертификата, он отказывает в выдаче нового сертификата и аннулирует существующий сертификат.

Web-браузеры информируют посетителя сайта о наличии EV-SSL сертификата у сайта. В адресном окне таких браузеров как Chrome и Firefox, слева от URL, появляется имя организации, выдавшей сертификат, и символ замочка, окрашенные в зелёный цвет. В адресном окне браузера Opera, слева от URL, появляется символ замочка, окрашенный в зелёный цвет. Кликнув этот символ можно получить информацию, как о сертификате, так и об организации, выдавшей сертификат.

Процесс получение и поддержки цифрового сертификата занимает значительное время администратора Web-сайта. В 2014 году была создана группа, включающая правозащитную организацию Electronic Frontier Foundation, коммерческие компании Mozilla, Cisco и др., а также ряд университетских исследователей, которая начала работу над тем, чтобы сделать цифровые сертификаты общедоступными и бесплатными. Эта группа, получившая наименование *Исследовательская Группа по Интернет Безопасности* (Internet Security Research Group – ISRG) стремиться сделать безопасный протокол HTTPS (вместо небезопасного протокола HTML) стандартным способом управления информационными потоками между Web-браузером и Web-сервером. Группа считает, что для этого цифровые сертификаты должны быть бесплатными и доступными в автоматическом режиме.

5.2.6. Стеганография

Термин *стеганография* (steganography) описывает процесс сокрытия информации (например, командной информации) внутри порции другой информации. Информация, скрытая при помощи стеганографии, может, затем, использоваться со злонамеренными целями. Часто, компьютерные файлы различных форматов содержат избыточные или не-

существенные данные, которые могут быть замещены другими данными. Эти другие данные не могут быть обнаружены без соответствующих декодирующих программ. Стенография обеспечивает способ сокрытия зашифрованного файла внутри другого файла-контейнера таким образом, что обычный наблюдатель не может обнаружить в файле-контейнере присутствие зашифрованного файла. В этом двух шаговом процессе, шифрование файла делает его нечитаемым, а стеганография – невидимым.

Многие специалисты в области компьютерной безопасности убеждены, что террористическая организация Аль-Каида использовала стеганографию, для сокрытия распоряжений и других сообщений, в изображениях, которые сообщники размещали на Web-сайтах, при подготовке к атаке на Нью-Йорк 11 сентября 2001 года. Сообщения, скрытые при помощи стеганографии, чрезвычайно трудно обнаружить. Этот факт в комбинации с тем фактом, что в Web существуют миллионы изображений, привлекают к стеганографии международные террористические организации и вызывают глубокую озабоченность правительств и профессионалов в области безопасности. Более подробную информацию о стеганографии студенты могут получить на Web-сайте Information Hiding: Steganography and Digital Watermarking.

5.2.7. Физическая безопасность для клиентского оборудования

В прошлом физическая безопасность была основной для больших компьютеров, которые реализовывали такие бизнес функции как составление платежных ведомостей или счетов. Появление компьютерных сетей сделало возможным управлять этими бизнес функциями непосредственно при помощи клиентских компьютеров. Поэтому, важными стали вопросы физической безопасности клиентских компьютеров. Многие меры физической безопасности, используемые сегодня, остались такими же, как и в ранние годы применения компьютеров в бизнесе, однако появились и некоторые новые интересные технологии.

Оборудование, считывающее отпечатки пальцев теперь доступно и для настольных компьютеров. Это оборудование, стоимостью менее 1000 долларов, обеспечивает более надёжную защиту, чем традиционный подход с использованием пароля. В дополнение к оборудованию, считывающему отпечатки пальцев, компании могут использовать другое, более точное, биометрическое оборудование безопасности. Биометрическое оборудование безопасности использует биологические показатели личности для её идентификации. Это оборудование включает: (1) электронный блокнот, который фиксирует подпись и нажим, который оказывает человек, ставящий подпись; (2) сканер рисунка кровеносных сосудов сетчатки глаза или цвета радужной оболочки; (3) сканер, считывающий отпечаток всей ладони, а не только пальцев, а также рисунок вен на обратной стороне ладони.

5.2.8. Безопасность мобильного клиентского оборудования

По мере того, как всё большее количество людей использует мобильное клиентское оборудование, такое как планшетные компьютеры и смартфоны, для доступа в Интернет, пропорционально возрастает и беспокойство о безопасности этого оборудования. Угрозы безопасности мобильного клиентского оборудования могут быть простыми, например, угрозы, связанные с потерей или кражей смартфона или планшета. Эти угрозы могут быть более сложными, например, угрозы атаки Троянского коня или вируса или угрозы со стороны приложения, которое транслирует персональную информацию.

Первым шагом в обеспечении безопасности мобильного оборудования является установка пароля доступа. Это может предотвратить или, по крайней мере, задержать получения доступа к персональной информации в вашем смартфоне вору, укравшему смартфон.

Почти все мобильные устройства содержат программы, которые позволяют их владельцам инициировать «удалённую очистку» в том случае, если устройство украдено. Удалённая очистка уничтожает все персональные данные, хранящиеся на устройстве, включая электронную почту, текстовые сообщения, контактную информацию, фотогра-

фии, видео, а также все типы файлов с документами. Если мобильное устройство не содержит программу удалённой очистки, то такая программа может быть добавлена в виде соответствующего приложения. Большинство корпоративных почтовых серверов могут выполнять удалённую очистку любого мобильного устройства, принадлежащего работникам компании, при помощи специальной программы, инсталлированной на мобильное устройство.

Web-сайты, содержащие вредоносные программы, могу легко инфицировать мобильное клиентское оборудование. Троянские кони и вирусы могут проникать в планшетные компьютеры и смартфоны через инфицированные Web-сайты и вложения электронной почты. Поэтому многие пользователи мобильного клиентского оборудования инсталлируют антивирусные программы на свои смартфоны и планшетные компьютеры.

Приложения для мобильных устройств, содержащие вредоносные программы или передающие персональную информацию злоумышленнику называются *мошенническими приложениями* (rogue apps). Для устранения мошеннических приложений магазин Apple App Store тестирует все мобильные приложения, прежде чем санкционирует их продажу. Магазин Android Market не так интенсивно проверяет мобильные приложения как Apple, однако все Android приложения сделаны так, что запрашивают разрешение пользователя на доступ к специфической информации, хранящейся на устройстве. Приложения запрашивают это разрешение в тот момент, когда пользователь инсталлирует приложение на устройство. Для того, чтобы избежать попадания мошеннических приложений на мобильный компьютер эксперты Android Market рекомендуют пользователям мобильного оборудования внимательно читать обзорную информацию о приложения перед его инсталляцией и не торопиться инсталлировать новые приложения, снабжённые примитивными описаниями. Они также рекомендуют покупать мобильные приложения только в магазине Android Market.

5.3. Безопасность канала коммуникации

Интернет служит каналом коммуникации между покупателем (в большинстве случаев клиентским компьютером) и продавцом (в большинстве случаев серверным компьютером). Наиболее важный факт, который необходимо помнить при изучении безопасности этого канала коммуникации, заключается в том, что Интернет не был спроектирован, чтобы быть безопасным. Хотя предтечей Интернет и является военная компьютерная сеть, в проект этой сети не были включены какие-либо существенные элементы безопасности. Сеть была спроектирована так, чтобы обеспечить избыточность, позволяющей ей работать даже если одна или несколько линий коммуникации повреждены. Иными словами, целью коммутации пакетов в Интернет является создание множества альтернативных путей, по которым может передаваться важная военная информация. Военные пересылают важную информацию в зашифрованном виде, поэтому содержание сообщения останется секретным, даже если оно будет перехвачено по пути. Таким образом, безопасность сообщений, проходящих через военные сети (предтечи Интернет), обеспечивалась программами шифровки и дешифровки, оперировавшими независимо от сети. Такой подход к безопасности сохранился и при дальнейшем развитии Интернет. Никакие существенные компоненты безопасности сети, как таковой, не стали её неотъемлемой частью.

Сегодня, Интернет остаётся, во многом, неизменным по отношению к своему оригинальному и небезопасному статусу. Пакеты сообщения перемещаются в Интернет по незапланированному пути от исходной точки к точке назначения. Отдельный пакет проходит через множество промежуточных компьютеров сети, прежде чем достигнет точки назначения. Маршрут пакета может изменяться каждый раз, когда он отправляется из одной и той же исходной точки в ту же самую точку назначения. Поскольку пользователь не может контролировать маршрут пакетов, и не знает какие промежуточные компьютеры они пересекли, то некий посредник может читать, изменять и удалять пакеты. Таким образом, безопасность любого сообщения, передаваемого через Интернет, подвергается угрозам секретности, целостности и необходимости.

5.3.1. Угрозы секретности

Угроза секретность это та угроза безопасности, которая наиболее часто упоминается в популярных публикациях в средствах массовой информации. Понятию «секретность» близко по смыслу (но не тождественно) понятие «приватность», которому также уделяется много внимания. *Секретность* (secrecy) означает защиту от несанкционированного доступа к информации, а *приватность* (privacy) – защиту индивидуальных прав на неразглашение личной информации. Секретность связана с вопросами внедрения различных физических и логических механизмов, в то время как приватность относится к юриспруденции. Классическим примером различия между понятиями «секретность» и «приватность» является электронная почта. Компания может защищать свою электронную почту от угрозы нарушения секретности при помощи шифрования. Приватность электронной почты связана с ответом на вопрос: «Кому принадлежат сообщения электронной почты: компании или индивидуальным работникам?» и, вообще говоря, предполагает запрет на чтение руководителем компании электронной почты своих работников.

Одной из существенных угроз для электронной почты является воровство персональных данных, включающих номера кредитных карт, фамилии и адреса. Воровство такого рода может произойти, когда кто-либо передаёт свои персональные данные при помощи Web, поскольку злоумышленник может записать информационные пакеты и проанализировать информацию, содержащуюся в них. Подобные проблемы могут возникнуть и при передаче сообщений электронной почты. Программы, называемые *программами-ищейками* (sniffer programs) могут записывать информацию, проходящую через компьютер или маршрутизатор, обрабатывающий Интернет трафик. Использование программы-ищейки аналогично подключению к телефонной линии и записи разговора. Программы-ищейки могут читать сообщения электронной почты и незашифрованный трафик между сервером и клиентом с данными о логинах и паролях пользователей и номерами кредитных карт.

Эксперты в области безопасности периодически обнаруживают *электронные дыры* (electronic holes), называемые *лазейками* (backdoors) в программном обеспечении электронной коммерции. Лазейкой, в смысле безопасности, называется элемент программы (или отдельная программа), позволяющий запускать и использовать программу без прохождения нормальной процедуры аутентификации. Программисты, часто, с целью экономии времени, встраивают такие лазейки в программу во время её тестирования. Иногда программисты забывают удалить лазейку, после завершения тестирования программы, либо умышленно сохраняют её.

Лазейка в программе позволяет любому, кто знает о её существовании, причинять вред пользователю программы путём отслеживания транзакций либо удаления или воровства данных. Консалтинговые фирмы, занимающиеся безопасностью, обнаружили, что широко используемая программа тележки для покупок Cart32 имеет лазейку, через которую злоумышленник может узнать номер кредитной карты покупателя. Эта лазейка образовалась в результате неумышленной ошибки в программировании и была немедленно ликвидирована после обнаружения. Однако, многие онлайновые покупатели, использовавшие эту программу, подвергались риску воровства номеров их кредитных карт.

Воровство кредитных карт является очевидной проблемой, однако злоумышленник может перехватить и конфиденциальную корпоративную информацию, которая может быть гораздо более ценная, чем информация о кредитных картах. Кредитные карты имеют ограничения на величину кредита, а украденная корпоративная информация, такая как копии чертежей, формула вещества или маркетинговый план могут стоить миллионы долларов.

Рассмотрим пример иллюстрирующий, каким образом онлайновый перехватчик может получить конфиденциальную информацию. Предположим, что пользователь авторизуется на сайте при помощи формы с текстовыми полями для ввода фамилии, физического адреса и адреса электронной почты. После того как пользователь заполнит текстовые поля, он передаёт её Web-серверу для обработки. Некоторые Web-сервера отслеживают данные, записанные в текстовые поля, путём размещения их в конце URL сервера (который появляется в адресном поле пользовательского Web-браузера). Этот длинный

URL (с прикреплёнными данными из текстовых полей) включается во все HTTP запросы и ответы, которые путешествуют между сервером и браузером пользователя. К этому моменту никаких нарушений секретности нет. Предположим, однако, что пользователь решил, не дожидаясь ответа от сервера, посетить другой сайт. В эту секунду сервер другого сайта может захватить URL предыдущего сайта путем копирования его из HTTP запроса, отосланного браузером. В этом случае, любой человек, имеющий доступ к серверу второго сайта может прочесть ту часть URL, которая содержит конфиденциальную информацию, введенную пользователем в текстовые окна во время авторизации на первом сайте.

В 2013 году была совершена крупнейшая атака типа «человек посередине» (man-in-the-middle). Уязвимость в *Протоколе Граничного Шлюза* (Border Gateway Protocol), который используется для маршрутизации Интернет трафика, позволила злоумышленникам более 38 раз похитить трафик, направляемый в правительственные агенства США, офисы корпораций и другие места. Злоумышленники не были идентифицированы, а похищенный трафик был существенного задержан и перенаправлен через компьютеры, находящиеся на значительном удалении. В одном случае пакет, направленный из одной точки города Денвер (США) в другую точку того же города был перенаправлен на компьютер, находящийся в Исландии. Специалисты по безопасности в фирме, которая обнаружила эту атаку, не смогли определить были ли похищенные пакеты модифицированы или разрушены. После этого случая уязвимость в протоколе Border Gateway Protocol была устранена.

Пользователи постоянно открывают информацию о себе, когда они работают с Web. Эта информация включает IP адреса и тип используемого браузера. Такая экспозиция IP адреса может рассматриваться как брешь в безопасности. Поэтому, некоторые компании и организации предлагают *анонимные Web-сервисы*, которые скрывают персональную информацию посетителей сайта. Эти сервисы могут обеспечивать необходимую меру приватности Web-пользователям, заменяя фактический IP адрес посетителя сайта IP адресом анонимного Web-сервера. Когда пользователь посещает сайт, то сайт загружает IP адрес анонимного сайта, а не фактический IP адрес посетителя.

Использование таких Web-сервисов может сделать анонимным, но утомительным процесс посещения Web-сайтов, поскольку посетитель сайтов должен вручную вводить URL каждого посещаемого сайта в текстовое окно на домашней странице Web-сервис. Для того, чтобы облегчить этот процесс некоторые компании, такие, например, как Anonymizer, предлагают плагины браузера, которые пользователи могут скачать и инсталлировать с ежегодной оплатой подписки. Сайт ShadowSurf.com предлагает бесплатные и анонимные онлайновые услуги браузера.

Tor представляет собой браузер, находящийся в свободном доступе, и гарантирующий анонимность работы в Web. Использование Tor браузера позволяет скрыть личность пользователя и защитить Web-соединения от различных видов слежки. Дополнительной опцией Tor является обход блокировок Web-сайтов со стороны Интернет провайдеров. Tor случайным образом изменяет маршрут Интернет трафик через свою сеть, состоящую более чем из 5000 компьютеров, что позволяет скрывать онлайновую активность пользователя от правительственного и частного надзора.

5.3.2. Угрозы целостности

Угроза целостности, называемая, также, *активным прослушиванием* (active wiretapping) существует тогда, когда неавторизированная сторона имеет возможность изменять поток информационных сообщений. Субъектом нарушения целостности может быть, например, сумма депозита в потоке сообщений незащищённой банковской транзакции. Нарушение целостности следует за нарушением секретности, поскольку злоумышленник, который изменяет информацию, должен иметь возможность читать и интерпретировать эту информацию. В отличие от угрозы секретности, которая предполагает, что неавторизованная сторона может просто читать информацию, угроза целостности может привести

к изменению поведения личности или корпорации, если были изменены критически важные данные, содержащиеся в потоке информационных сообщений.

Кибервандализм является примером нарушения целостности. *Кибервандализм* (cybervandalism) означает умышленное повреждение страницы Web-сайта и является электронным эквивалентом разрушения частной собственности или рисованием граффити на различных предметах. Кибервандализм имеет место каждый раз, когда кто-либо замещает нормальный контент Web-страницы своим собственным контентом, часто, оскорбительного содержания.

Маскировкой (masquerading) или *подменой/спуфингом* (spoofing) называется использование поддельного Web-сайта вместо реального и является средством нанесения ущерба реальному Web-сайту. *Серверы доменных имён* (domain name servers – DNSs) это компьютеры, которые поддерживают справочники, связывающие доменные имена и IP адреса. Злоумышленники могут использовать уязвимости в программах, которые работают на этих серверах, для замены IP адреса реального сайта на IP адрес поддельного сайта с целью обмана посетителей реального сайта.

Например, хакер может создать фиктивный Web-сайт замаскированный под сайт компании, имеющий доменное имя www.widgets.com, а затем, используя уязвимость в программном обеспечении DNS, заменить IP адрес сайта www.widgets.com на IP адрес фиктивного сайта. После этого все посещения сайта www.widgets.com будут перенаправлены на фиктивный сайт, а хакер получает возможность изменить количество заказанного товара и адрес доставки. *Атака с нарушением целостности* (integrity attack) состоит из перехвата заказа, изменения заказа и отправки изменённого заказа на сервер реальной компании для выполнения. Сервер реальной компании не знает об атаке целостности, поэтому он просто проверяет номер кредитной карты покупателя и направляет заказ на выполнение.

Многие известные сайты электронной коммерции, такие как Amazon.com, AOL, eBay и PayPal стали жертвами атак с нарушением целостности. Некоторые из схем этих атак комбинировали спуфинг с рассылкой спама. Злоумышленники рассылали миллионы почтовых спам сообщений от имени компании, подвергшейся спуфингу. Спам сообщения включали ссылки на поддельную Web-страницу, которая выглядела точно как страница реального сайта. Жертве предлагали авторизоваться, а иногда, даже, ввести информацию о кредитной карте. Такая атака, в результате которой захватывается конфиденциальная информация клиента, называется *фишинговая экспедиция* (phishing expedition). Часто жертвами фишинговой экспедиции становятся посетители Web-сайтов онлайновых банковских и платежных систем (таких как PayPal).

5.3.3. Угрозы необходимости

Угроза необходимости часто выражается в *атаке задержки* (delay attack), *атаке отказа* (denial attack) или атаке *отказ в обслуживании* (denial-of-service – DoS). Целью таких атак является нарушение процесса нормальной обработки данных компьютером или полный отказ от обработки данных. Например, искусственное замедление времени отклика на запрос клиента к коммерческому сайту может побудить его перейти на сайт конкурента и больше не возвращаться к «медленному» сайту. Атака компьютерного червя в 1998 году (см. рис. 5.3), от которой пострадали тысячи компьютерных систем, подключённых к Интернет, была первой зафиксированной DoS атакой.

Хакеры могут использовать бот-сеть для того чтобы запустить атаку на Web-сайт (или множество Web-сайтов) одновременно со всех компьютеров бот-сети. Такая форма атаки называется *распределенная атака отказа в обслуживании* (distributed denial-of-service (DDoS) attack).

Во время DoS атаки может быть удалена информация из компьютера, подвергшегося атаке. Одна из DoS атак была нацелена на компьютеры, на которых была инсталлирована бухгалтерская программа компании Quicken. Компьютер злоумышленника смог использовать средства электронных платежей этой программы для перевода денег на банковский счет злоумышленника. В другой DoS атаке против таких высокопрофессио-

нальных сайтов как Amazon.com и Yahoo! хакеры использовали бот-сеть для рассылки потоков пакетов данных на эти сайты. В результате серверы сайтов были перегружены и не могли обеспечить доступ к сайту легитимных пользователей. Прежде чем запустить DoS атаку, злоумышленники заранее идентифицировали множество уязвимых компьютеров и загрузили на них программы, которые позволили запустить одновременную атаку со всех этих компьютеров.

5.3.4. Угрозы физической безопасности каналов коммуникации Интернет

Интернет изначально был спроектирован так, чтобы противостоять атакам на его физические линии связи. Проект Интернет базируется на компьютерных сетях с коммуникацией пакетов, и это предохраняет его от прекращения работы при атаке на отдельную линию связи в сети.

Несмотря на эту особенность, связь с Интернет, для индивидуального пользователя, может быть прервана путём разрушения линии связи между компьютером пользователя и компьютером Интернет провайдера. Поэтому крупные компании и организации (а также сами Интернет провайдеры) часто обладают множеством физических линий связи с магистральными роутерами, через различных провайдеров доступа. Если какая-либо линия связи становится перегруженной или недоступной, то трафик переключается на линию связи другого провайдера доступа для того, чтобы компания, организация или Интернет провайдер (и все его клиенты) оставались подключёнными к Интернет.

5.3.5. Угрозы для беспроводных сетей

Локальные компьютерные сети могут использовать *беспроводные точки доступа* (wireless access points – WAPs) для обеспечения связи между компьютерами и другими мобильными устройствами в пределах 150 метров (см. подраздел 2.6.5 в конспекте лекций по дисциплине Электронная коммерция). Если беспроводная сеть не защищена, то любой человек, находящийся в этой зоне, может войти в сеть и получить доступ ко всем её ресурсам. Эти ресурсы могут включать: любые данные, находящиеся на любом из компьютеров сети; сетевые принтеры; сообщения, передаваемые по сети; а также свободный доступ в Интернет, если локальная сеть связана с Интернет. Безопасность связи в беспроводной локальной сети определяет *Протокол Беспроводного Шифрования* (Wireless Encryption Protocol – WEP), представляющий собой набор правил для шифрования передачи от беспроводного оборудования к WAPs.

Компании, которые имеют большие беспроводные компьютерные сети, обычно следят за тем, чтобы WEP протокол был задействован на всём беспроводном оборудовании. Однако небольшие компании и отдельные личности, эксплуатирующие беспроводную сеть, часто не включают WEP. Большинство WAPs поставляются пользователям с логином и паролем, установленными по умолчанию. Компания, которая инсталлирует такой WAP, может забыть изменить логин и пароль, установленные изготовителем. Это предоставляет злоумышленнику возможность проникновения в сеть.

В некоторых городах, с большой концентрацией беспроводных сетей, злоумышленники перемещаются по улицам на машинах, оборудованных компьютерами, способными обнаруживать доступные беспроводные сети. Такие злоумышленники называются *вардрайверами* (wardrivers). Когда вардрайвер обнаруживает открытую беспроводную сеть (или WAP с общеизвестным логином и паролем, установленными по умолчанию) он, может нарисовать на здании специальную метку при помощи мела. Такая метка сообщает другому злоумышленнику, что неподалёку находится беспроводная сеть в которую можно легко войти. Такая практика называется *варчокинг* (warchalking). Некоторые злоумышленники, занимающиеся варчокингом, создают сайты, на которых размещают карты крупнейших городов мира с указанием местонахождения открытых для доступа беспроводных сетей. Компании, которые хотят избежать проникновение злоумышленников в их беспроводные сети, должны держать включенным WEP протокол на всём беспро-

водном оборудовании и всегда устанавливать новые логин и пароль для беспроводных точек доступа.

Одной из первых жертв атаки с проникновением в беспроводные сети была компания Best Buy, являющаяся крупным розничным продавцом бытовой электроники в США. В ряде своих физических магазинов компания использовала торговые точки в виде беспроводных терминалов. Беспроводные терминалы могли легко перемещаться из одной части магазина в другой, что улучшало обслуживание больших потоков покупателей, по сравнению с терминалами, расположенными в фиксированном месте. К сожалению Best Buy не задействовало протокол WEP в этих беспроводных терминалах. Один из покупателей, который только что приобрел плату беспроводной связи для своего переносного компьютера, решил запустить на нём программу-ищейку. В этот момент он находился в автомобиле на парковке магазина. Этот покупатель смог перехватывать данные с беспроводных терминалов, включая детали транзакций и те данные, которые, по его мнению, были номерами кредитных карт. Компания Best Buy прекратила использование беспроводных терминалов, когда эта история появилась на страницах некоторых сайтов.

5.3.6. Шифрование

Шифрованием (encryption) называется кодирование информации при помощи компьютерной программы, базирующейся на математическом алгоритме и специальном секретном ключе, с целью представление информации в виде бессмысленной строки символов. Наука, которая изучает шифрование, называется *криптография* (cryptography). Криптография отличается от стеганографии, которая занимается сокрытием текстового файла внутри графического файла, таким образом, что текстовый файл становится невидимым при обычном восприятии графического файла. Криптография не скрывает текст, а превращает его в другой текст, который, при обычном восприятии, представляет собой строку случайных текстовых символов, цифр и знаков пунктуации.

Алгоритмы шифрования

Программа, которая преобразует обычный текст, который, в этом случае, называется *открытый или незашифрованный текст* (plain text) в *зашифрованный текст* (cipher text), называется *программой шифрования* (encryption program). Программа шифрования использует алгоритм, базирующийся на некоторой математической модели, который называется *алгоритмом шифрования* (encryption algorithm).

Сообщения шифруются непосредственно перед их передачей через компьютерные сети. После того как сообщение получено адресатом, оно расшифровывается при помощи *программы расшифровки* (decryption program).

Одно из важных свойств программ шифрования заключается в том, что даже в том случае, когда кто-либо знает детали алгоритма шифрования, он всё равно не сможет расшифровать сообщение не зная ключ, который использовала программа шифрования. Способность зашифрованного сообщения противостоять внешним атакам, направленным на расшифровку сообщения, зависит от размера ключа (количество битов в ключе), который использовался при шифровании. Большинство экспертов в области шифрования считают, что 128-битный ключ может обеспечить адекватную безопасность при передаче данных, однако, сегодня, широко используются также 192-битные и 256-битные ключи. Центры сертификации, продающие цифровые сертификаты, часто используют шифрование с 2048-битными ключами. Некоторые из них перешли на шифрование с 4096-битными ключами. Достаточно длинный ключ обеспечивает невозможность расшифровки закодированного сообщения.

Тип ключа и программы шифрования, используемые для конвертирования открытого текста в зашифрованный текст, подразделяют шифрование на следующие три способа шифрования: хэш-кодирование; ассиметричное шифрование; симметричное шифрование.

Хэш-кодирование

Хэш-кодированием (hash-coding) называется процесс, который использует *хэш-алгоритм* (hash-algorithm) для вычисления числа, соответствующего некоторому сообщению и называемого *хэш-значением* (hash value). Хэш-значение для сообщения является аналогом отпечатков пальцев для человека, поскольку уникально для каждого сообщения. При помощи хэш-кодирования можно обнаружить факт изменения сообщения во время его пересылки. Для этого необходимо сравнить хэш-значение сообщения, которое вычислено на стороне отправителя с хэш-значением сообщения, которое вычислено на стороне получателя. Если, во время пересылки, произошло изменение сообщения, то его исходное хэш-значение не совпадёт с хэш-значением, вычисленным на стороне получателя.

Ассиметричное шифрование

Ассиметричное шифрование (asymmetric encryption) или *шифрование с открытым ключом* (public-key encryption) осуществляет шифровку и расшифровку сообщений с использованием *двух связанных цифровых ключей*. В системе шифрования с открытым ключом один из двух ключей, называемый *открытым ключом* (public key), находится в свободном доступе и предоставляется любому, заинтересованному в безопасной коммуникации с обладателем обоих ключей. Открытый ключ используется для шифрования сообщений при помощи одного из нескольких алгоритмов шифрования перед его передачей получателю. Второй ключ, называемый *закрытый ключ* (private key), находится у получателя сообщений и используется для расшифровки сообщений.

Рассмотрим пример, иллюстрирующий работу системы шифрования с открытым ключом. Пусть Алексей и Татьяна используют ассиметричную систему шифрования. Если Алексей хочет послать зашифрованное сообщение Татьяне, он должен получает открытый ключ Татьяны из одного из нескольких публичных источников. Затем, используя этот открытый ключ, он шифрует и отправляет своё сообщение Татьяне. После того как сообщение зашифровано, только Татьяна может его расшифровать при помощи своего закрытого ключа. Поскольку пара ключей уникальна, то только один закрытый ключ может «открыть» сообщение, зашифрованное при помощи соответствующего открытого ключа и наоборот. В свою очередь, Татьяна может послать зашифрованное сообщение Алексею, используя его открытый ключ при шифровании. Когда Алексей получает зашифрованное сообщение от Татьяны, он использует свой закрытый ключ для его расшифровки. Если Алексей и Татьяна пользуются электронной почтой, то сообщения электронной почты остаются зашифрованными только при их транспортировке. После того, как сообщение получено на клиентский компьютер и расшифровано, оно сохраняется в виде обычного текста.

Одна из наиболее популярных технологий, используемая сегодня для имплементации шифрования с открытым ключом, называется *Довольно Хорошая Секретность* (Pretty Good Privacy – PGP). Технология PGP была предложена в 1991 году Филиппом Циммерманом, который начал продавать её коммерческим компаниям, но разрешал бесплатное использование индивидуальным пользователям. Технология PGP использует несколько различных алгоритмов шифрования с открытым ключом. Сегодня, индивидуальные пользователи могут получить бесплатную версию PGP на одном из сайтов, а коммерческие компании – приобрести лицензию у компании Symantec.

Симметричное шифрование

Симметричное шифрование (symmetric encryption) или *шифрование с закрытым ключом* (private-key encryption) осуществляет шифровку и расшифровку сообщения при помощи алгоритмов, использующих только один цифровой ключ, такой, например, как 456839420783. Поскольку при шифровании и дешифровании используется один и тот же ключ, то этот ключ должен быть известен как отправителю, так и получателю сообщения.

Достоинством симметричного шифрования является высокая скорость и эффективность, как процесса шифрования, так и процесса дешифрования сообщений. Однако закрытый ключ должен сохраняться в тайне. Если закрытый ключ оказывается в публичном доступе, то все сообщения, ранее зашифрованные при помощи этого ключа, могут быть расшифрованы и, поэтому, ключ должен быть изменён.

Проблемой симметричного шифрования является процедура распространение новых закрытых ключей уполномоченным сторонам, для соблюдения безопасности и контроля над ключами, поскольку безопасная передача любых данных (включая новые закрытые ключи) требует их шифрования. Симметричное шифрование плохо работает в таких больших средах как Интернет с огромным количеством пользователей, обменивающихся сообщениями, поскольку каждая пара пользователей, которая хочет обмениваться зашифрованными сообщениями, должна иметь свои собственные закрытые ключи. Ясно, что это требует чрезмерно большого количества закрытых ключей, которые должен хранить каждый пользователь. Однако, использование симметричного шифрования является общеупотребительным в таких высоко засекреченных средах, как банковская или военная.

Сравнение ассиметричной и симметричной систем шифрования

Система шифрования с открытым ключом обладает некоторыми преимуществами, по сравнению с системой шифрования с закрытым ключом. Во-первых, в системе шифрования с открытым ключом используется относительно небольшое количество уникальных ключей, необходимых для обмена зашифрованными сообщениями, между большим количеством пользователей. Если, например, n пользователей хотят обмениваться друг с другом зашифрованными сообщениями, то для этого требуется только n уникальных закрытых ключей, что гораздо меньше, чем количество закрытых ключей, требуемых в случае использования систем шифрования с закрытым ключом.

Во-вторых, распространение ключей, в системе шифрования с открытым ключом, не является проблемой. Открытый ключ каждого пользователя может быть размещен в открытом доступе и не требуется предпринимать никаких специальных мер для дистрибуции этих ключей.

В-третьих, система шифрования с открытым ключом делает возможным имплементацию *цифровой подписи* (digital signature). Отправитель может поставить электронную подпись на электронном документе, зашифровать его и отправить адресату. Важно, что в дальнейшем отправитель не сможет отказаться от этой подписи, поскольку система шифрования с открытым ключом предполагает, что только отправитель шифрованного сообщения может включить в него свою цифровую подпись.

Система шифрования с открытым ключом обладает некоторыми недостатками. Один из недостатков заключается в том, что система шифрования с открытым ключом «работает» значительно медленнее, чем система шифрования с закрытым ключом. Дополнительное время, расходуемое на шифрование и дешифрование, может быть крайне нежелательным фактором в том случае, когда отдельные личности и/или компании осуществляют коммерческую деятельность с использованием Интернет. В ряде случаев система шифрования с открытым ключом не замещает систему шифрования с закрытым ключом, а служит её дополнением. Например, система шифрования с открытым ключом может использоваться для передачи закрытых ключей уполномоченным сторонам с тем, чтобы, в дальнейшем, эти ключи могли быть применены при организации дополнительных и более эффективных, с точки зрения безопасности, сеансов коммуникации в Интернет.

Рис. 5.6 представляет графическую иллюстрацию хэш-кодирования, системы шифрования с закрытым ключом и системы шифрования с открытым ключом. Рисунок 5.6a иллюстрирует хэш-кодирование; рисунок 5.6b – систему шифрования с закрытым ключом; рисунок 5.6c – систему шифрования с открытым ключом.

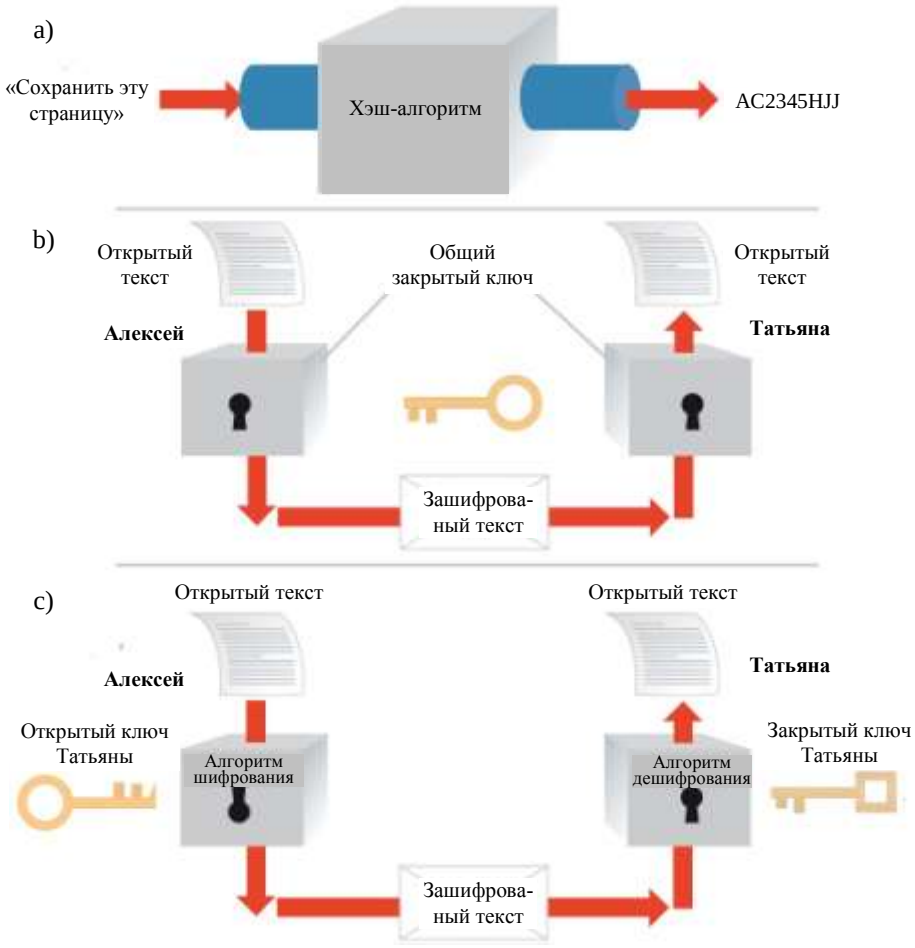

Рис. 5.6. Способы шифрования: a) хэш-кодирование; b) шифрование с закрытым ключом; c) шифрование с открытым ключом

5.3.7. Шифрование в Web-браузерах

Для организации безопасного сеанса связи между Web-сервером и Web-клиентом применяются два протокола безопасных соединений, использующих шифрование: (1) протокол, названный *Уровень Защищённых Сокетов* (Secure Sockets Layer – SSL), разработанный компанией Netscape Communications и (2) *Безопасный Протокол Передачи Гипертекста* (Secure Hypertext Transfer Protocol или S-HTTP), разработанный компанией CommerceNet. Оба протокола позволяют серверному и клиентскому компьютерам осуществлять безопасный сеанс связи, управляя деятельностью по шифрованию и дешифрованию передаваемых данных. Однако, цели этих протоколов отличаются. Целью протокола SSL является обеспечение безопасного соединения между двумя компьютерами, а целью протокола S-HTTP – обеспечение безопасности для каждого индивидуального сообщения.

Уровень Защищённых Сокетов (SSL)

Протокол SSL предполагает этап «знакомства», во время которого клиентский и серверный компьютеры обмениваются кратким пакетом сообщений. В этих сообщениях клиент и сервер договариваются об уровне безопасности, который будет использоваться для обмена цифровыми сертификатами и выполнения других задач. Вначале, клиентский и серверный компьютеры идентифицируют друг друга. После идентификации протокол SSL шифрует и дешифрует все информационные потоки между компьютерами. Иными

словами, вся информация как HTTP запроса, так и HTTP ответа передаётся в зашифрованном виде. Поскольку все данные, циркулирующие между SSL-сервером и SSL-клиентом, передаются в зашифрованном виде, то потенциальный онлайновый перехватчик сможет получить только бессмысленную последовательность символов.

Протокол SSL может обезопасить различные типы коммуникации между компьютерами, а не только HTTP сеансы связи. Например, при помощи SSL можно обезопасить FTP сеанс связи, обеспечивая безопасную загрузку и выгрузку важных документов, электронных таблиц и других данных. Протокол SSL может обезопасить сеанс связи с удаленным компьютером при помощи программы Telnet когда, например, удалённый пользователь авторизуется на корпоративном хост компьютере. Программа Telnet и протокол FTP (File Transfer Protocol) рассматривались в подразделе 3.4.2.

Протокол SSL предполагает генерацию закрытого ключа для каждого зашифрованного сеанса связи. Длина этого ключа может быть различной (128 бит или 256 бит). Чем длиннее ключ, тем больше сопротивляемость шифрованных данных внешним атакам. Браузер, который участвует в SSL сеансе связи, показывает, что сеанс связи является зашифрованным. Большинство браузеров используют, для этого, иконку в строке состояния. После того как SSL сеанс связи завершается закрытый ключ уничтожается и никогда более не используется в последующих SSL сеансах.

Для реализации безопасного сеанса связи между Web-сервером и Web-клиентом используется комбинация шифрования с открытым ключом (ассиметричная система) и шифрования с закрытым ключом (симметричная система). Браузер генерирует закрытый ключ, а затем шифрует его, используя открытый ключ сервера. Открытый ключ сервера находится в цифровом сертификате, который сервер пересылает браузеру на этапе «знакомства». После того, как браузер зашифровал закрытый ключ, он отсылает его серверу. Сервер, в свою очередь, дешифрует сообщение при помощи закрытого ключа.

Работу протокола SSL при обмене данными между браузером (SSL клиентом) и Web-сервером (SSL сервером) можно описать следующим образом.

1. Когда браузер посылает запрос на связь с безопасным Web-сервером, называемый «привет от клиента», сервер отвечает сообщением, называемым «привет от сервера». Во время этого этапа «знакомства», определяется алгоритм шифрования, поддерживаемый обоими компьютерами и длина ключа.
2. Затем браузер запрашивает у сервера его цифровой сертификат, доказывающий идентичность сервера. В ответ сервер посылает браузеру сертификат, подписанный одним из известных центров сертификации.
3. Браузер проверяет серийный номер сертификата сервера, сравнивая его с открытыми ключами центров сертификации, хранящимися в браузере. Если открытый ключ центра сертификации подтверждается, то подтверждается и цифровой сертификат. На этом завершается процесс аутентификации, и браузер отсылает серверу клиентский сертификат, а также зашифрованный закрытый ключ, который будет использоваться во время сеанса. Когда сервер получает эту информацию, он инициирует безопасный сеанс связи с использованием полученного закрытого ключа, который теперь становится общим и для браузера и для Web-сервера.
4. После установления безопасного сеанса связи, запросы браузера принимаются сервером, который формирует и отсылает соответствующие ответы. Во время безопасного сеанса связи клиент может совершать покупки, оплачивать счета или торговать акциями не беспокоясь об угрозах безопасности для информации, передаваемой между двумя компьютерами.

Начиная с этого момента, открытый ключ более не используется в сеансе связи. Данные, которые циркулируют между сервером и клиентом, шифруются с использованием общего закрытого ключа, который, часто называют *ключом сеанса* (session key). Когда сеанс завершается, ключ сеанса уничтожается.

При каждом новом соединении между клиентом и безопасным сервером, описанная выше, работа повторяется, начиная с этапа «знакомства». Рис. 5.7 иллюстрирует процесс

SSL «знакомства», который происходит до того, как клиент и сервер начинают обмениваться информацией, зашифрованной при помощи закрытого ключа.

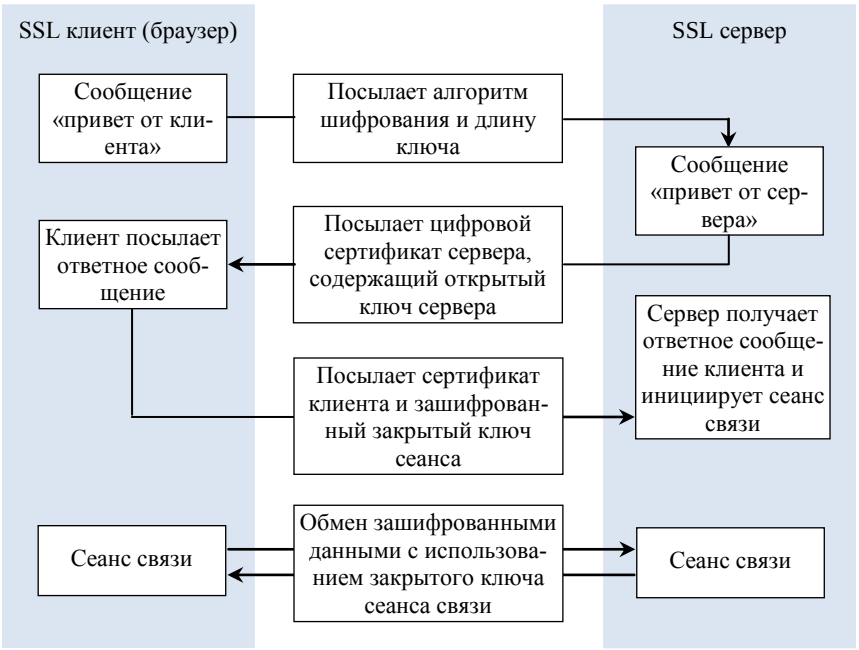

Рис. 5.7. Начальный этап сеанса связи протокола SSL

Безопасный Протокол Передачи Гипертекста (S-HTTP)

Безопасный протокол передачи гипертекста (S-HTTP) является расширением протокола HTTP и обеспечивает множество средств обеспечения безопасности, такие как аутентификацию клиента и сервера, спонтанное шифрование, а также невозможность отказа от авторства запросов и ответов. Протокол S-HTTP использует симметричное шифрование (закрытый ключ) для секретного обмена информацией и ассиметричное шифрование (открытый ключ) в процессе аутентификации клиента и сервера. Условия безопасности протокола S-HTTP устанавливаются во время первоначального сеанса связи между клиентом и сервером. Этот процесс предложения и принятия (или отклонения) различных условий безопасной передачи данных называется *обсуждением сеанса* (session negotiation).

Протокол S-HTTP устанавливает безопасность сеанса на этапе «знакомства» (похожем на этап «знакомства» протокола SSL), включая описание безопасности в заголовки пакетов сообщений. Заголовки определяют использование шифрования с закрытым ключом, аутентификацию сервера и клиента, а также целостность сообщения. После того, как клиент и сервер достигли соглашения об условиях безопасной передачи данных, все последующие сообщения сеанса связи помещаются в *безопасный контейнер*, называемый конвертом. Этот *безопасный конверт* инкапсулирует зашифрованное сообщение, что обеспечивает секретность, целостность и аутентификацию клиента и сервера. Протокол S-HTTP используется некоторыми Web-серверами, однако, всё чаще заменяется протоколом SSL.

5.3.8. Хэш-алгоритм, дайджест сообщения и цифровая подпись

Трудно предотвратить изменения, которые может сделать злоумышленник в сообщении, перехватив его во время передачи. Однако, существуют технологии, которые позволяют детектировать такие изменения. Для детектирования изменения в сообщении используется хэш-алгоритм. Хэш-алгоритм, примененный к контенту сообщения, форми-

рует хэш-значение, называемое, также, *дайджест сообщения* (message digest). Дайджест сообщения представляет собой число, уникальное для каждого сообщения. Компьютер, получивший сообщение, может вычислить дайджест полученного сообщения и сравнить его с дайджестом исходного сообщения. Если оба дайджеста совпали, то сообщение не было изменено во время передачи. Если дайджесты не совпали, то получатель может запросить повторную передачу сообщения.

Хэш-алгоритм не является идеальным средством, поскольку находится в свободном доступе и широко известен. Например, сообщение, содержащее заказ на покупку может быть перехвачено, адрес доставки и количество приобретаемого товара изменены, а дайджест сообщения сгенерирован заново. После этого новое сообщение и новый дайджест могут быть направлены продавцу. Продавец, получив сообщение, вычисляет его дайджест и убеждается, что он совпадает с присланным дайджестом. Продавец делает неверный вывод о том, что сообщение не было изменено во время передачи. Для того чтобы предотвратить такой вид мошенничества, *отправитель должен шифровать дайджест своего сообщения при помощи закрытого ключа*.

Зашифрованный дайджест сообщения, созданный с использованием закрытого ключа, называется *цифровой подписью* (digital signature). Заказ на покупку, сопровождаемый цифровой подписью, снабжает продавца информацией, идентифицирующей отправителя и уверенностью в том, что сообщение не было изменено во время передачи. Продавец расшифровывает полученный дайджест, используя открытый ключ отправителя, затем вычисляет дайджест сообщения при помощи хэш-алгоритма и сравнивает оба дайджеста. Если дайджесты совпали, то отправитель сообщения аутентифицирован. Отметим, что только истинный отправитель может быть автором сообщения, поскольку только при помощи закрытого ключа отправителя можно зашифровать сообщение таким образом, что оно будет успешно расшифровано соответствующим открытым ключом на стороне получателя. Из этого следует невозможность отправителя отказаться от авторства сообщение, что особенно важно для транзакций, осуществляемых в системах электронной коммерции типа бизнес-бизнес. Рис. 5.8 иллюстрирует процесс формирования и пересылки цифровой подписи и аутентификации отправителя.

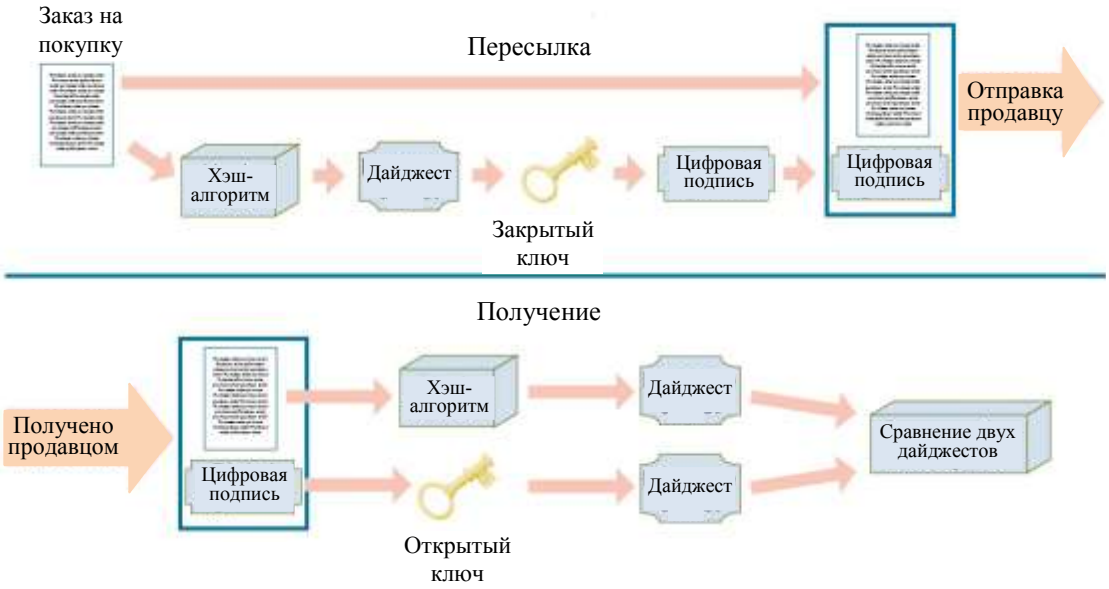

Рис. 5.8. Отправка и получение сообщения, снабженного цифровой подписью

Одновременное шифрование и дайджеста и контента сообщения гарантируют высокий уровень секретности при передаче сообщений через Интернет. Сегодня, в большинстве стран, цифровая подпись имеет такой же правовой статус, как и обычная подпись.

5.4. Безопасность серверного компьютера

Сервер является третьим звеном в цепи электронной коммерции «клиент-Интернет-сервер». Одной из забот администратора Web-сервера является установление, документирование и внедрение политики безопасности, направленной на минимизацию влияния угроз на Web-сервер.

5.4.1. Угроза атаки на пароль

Одним из наиболее чувствительных файлов, находящихся на Web-сервере, является файл, хранящий пары значений: «имя пользователя – пароль». Злоумышленник, прочитавший этот файл, может получить доступ к конфиденциальной информации под видом легитимного пользователя. Для уменьшения рисков такого рода большинство Web-серверов хранит информацию, необходимую для аутентификации пользователей, в зашифрованных файлах.

Пароль, который выбирает пользователь, может быть источником угрозы. Иногда пользователи выбирают пароли, значения которых легко восстановить, такие как имя, фамилия и год рождения, имя домашнего животного, девичья фамилия матери, имя ребёнка, номер телефона пользователя, акронимы, используемые в организации и т.п. Программы, осуществляющие *атаку с перебором по словарю* (Dictionary attack) циклически перебирают электронный словарь, пытаясь использовать каждое слово в словаре в качестве пароля.

Пароль, украденный однажды, обеспечивает доступ к серверу и может оставаться необнаруженным в течение длительного времени. Многие организации требуют от пользователей создавать пароли, включающие комбинацию букв, цифр и специальных символов, которые с очень низкой вероятностью могут находиться в словаре, при атаке с перебором по словарю. Другие организации используют проверку по своим собственным словарям, как превентивную меру. Когда пользователь выбирает новый пароль, программа проверяет этот пароль на совпадение со своим собственным словарем, и если такое совпадение обнаруживается, то пароль отвергается. На рис. 5.9 приведены примеры паролей, ранжированные от очень слабых к очень сильным.

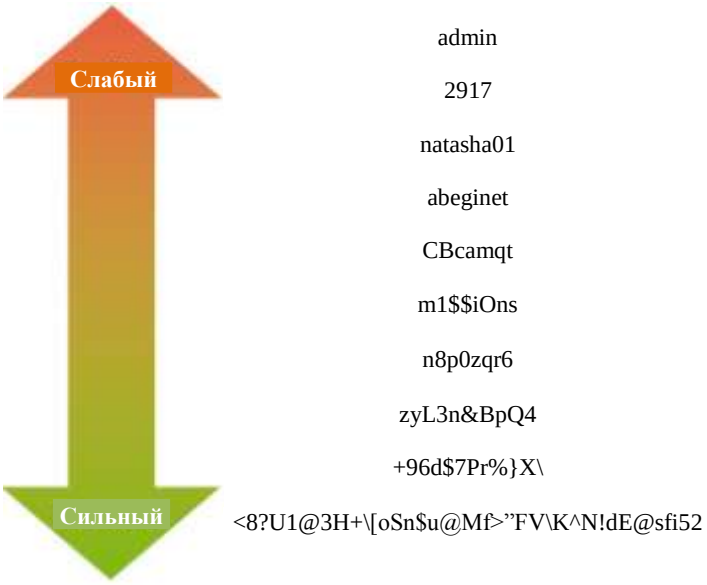

Рис. 5.9. Примеры паролей, от очень слабых к очень сильным

Существует большое количество онлайновых ресурсов, помогающих создать сильный пароль. Одним из наиболее уважаемых ресурсов такого типа является Gibson Research Corporation Ultra High Security Password Generator.

Некоторые эксперты в области безопасности рекомендуют использовать ключевую фразу вместо того, чтобы создавать сложный пароль. *Ключевая фраза* (passphrase) представляет собой последовательность слов или текст, которые легко запомнить, но которые достаточно сложны для того чтобы служить либо хорошим паролем, либо подсказкой для запоминания хорошего пароля. Примером ключевой фразы на английском языке может служить предложение «The road to success is always under construction!» (дорога к успеху всегда на ремонте). При необходимости эту ключевую фразу можно использовать для формирования пароля. Для этого, например, можно использовать первые буквы каждого слова и восклицательный знак в конце фразы, а также символ «$» вместо буквы «s». В итоге получаем пароль в виде «Trt$iauc!».

Другим подходом к решению проблемы запоминания большого количества логинов и паролей является использование программы, называемой менеджер паролей. Популярным менеджером паролей является программа LastPass. LastPass – бесплатная программа для хранения паролей, разработанная компанией LastPass. Она существует в виде плагинов для большинства браузеров. *Менеджер паролей* (password manager) гарантирует безопасное хранение всех пользовательских паролей. Вместо того, чтобы помнить множество отдельных паролей для каждой онлайновой учётной записи, пользователь должен помнить только один *основной пароль* (master password) для доступа к самому менеджеру паролей. Большинство менеджеров паролей работают автоматически. Когда пользователь открывает Web-страницу, требующую авторизации, менеджер паролей проверяет, храниться ли у него логин и пароль пользователя для входа в эту страницу. Если это так, то менеджер паролей вводит их в соответствующие поля на Web-странице. Главной заботой пользователя менеджера паролей является уверенность в том, что основной пароль является достаточно надёжным, поскольку хакер, получивший доступ к основному паролю, мгновенно получает доступ ко всем учётным записям пользователя.

5.4.2. Угрозы для базы данных

Системы электронной коммерции хранят данные о клиентах, а также осуществляют поиск информации о продуктах в базах данных, связанных с Web-сервером. Базы данных, связанные с Web-сервером, кроме информации о клиентах и продуктах, хранят ценную частную информацию, раскрытие или изменение которой может нанести компании непоправимый ущерб. Большинство систем управления базами данных включают средства, обеспечивающие безопасность, которые базируются на использовании пары «имя пользователя – пароль». После того, как пользователь авторизовался, он получает доступ к некоторым частям базы данных. Однако некоторые системы управления базами данных либо хранят пары «имя пользователя – пароль» в незашифрованной таблице, либо вообще не используют средства, обеспечивающие безопасность, полагаясь на систему безопасности Web-сервера. Если неавторизованный пользователь получает чьи-то данные, необходимые для аутентификации, он может, под видом легитимного пользователя, получить доступ к конфиденциальной и ценной информации. Программа типа Троянский конь, спрятанная в прикладной системе базы данных, может раскрыть информацию, хранящуюся в базе данных, путём изменения прав доступа к этим данным для различных групп пользователей. Троянский конь может, даже, полностью отменить контроль доступа к базе данных, предоставляя всем, включая злоумышленников, полный доступ к данным, хранящимся в базе.

5.4.3. Другие угрозы, базирующиеся на переполнении буферной области памяти

Угрозами для Web-сервера могут быть программы, выполняемые сервером. Программы, написанные на языках Java или C++, которые передаются клиентом на Web-сервер, или те программы, которые находятся на сервере, во время работы, часто используют буферную область памяти или буфер. Буфер предназначен для временного хранения данных, прочитанных из файла или базы данных. Буфер необходим всякий раз, когда имеет место любая операция ввода или вывода данных, а его использование существенно

ускоряет обработку данных, участвующих в обмене с файла или базы данных. Программы, которые заполняют буфер данными, могут привести к сбою в работе буфера, переполнив его данными и вытеснив часть данных за пределы области памяти, выделенной для буфера. Такой сбой в работе буфера называется ошибкой *переполнения буфера* (buffer overrun или buffer overflow). Причиной переполнения буфера, обычно, является ошибка в программе, работающей с буфером. Однако переполнение буфера может быть преднамеренным и являться результатом атаки зловредной программы. Компьютерный червь Internet Worm, появившийся в 1988 году (см. таблицу на рис. 5.3) является именно такой программой. Он создавал условия переполнения буфера и, в конечном итоге, поглощал всю память, что приводило к невозможности дальнейшей работы компьютера.

Более коварная версия *атаки переполнения буфера* (buffer overflow attack) записывает команды в критические участки памяти компьютера, и, когда зловредная программа завершает работу по переполнению буфера, компьютер возобновляет её работу путём загрузки во внутренний регистр компьютера адреса основного кода атакующей программы. Такой тип атаки может причинить существенные повреждения серверу, поскольку зловредная программа, возобновляющая свой контроль над компьютером, получает возможность открывать и разрушать файлы. Хорошая технология программирования позволяет исключать ошибки в коде, приводящие к неумышленному переполнению буфера. Аппаратное обеспечение и операционные системы некоторых компьютеров ограничивают эффект от переполнения буфера, который создается умышленно для причинения вреда компьютеру.

Почтовые сервера могут подвергаться атаке, во время которой серверу намеренно посылается избыточное количество почтовых сообщений. Атака, называемая *почтовая бомба* (mail bomb), означает, что сотни, или даже тысячи пользователей одновременно отсылают сообщения электронной почты одному конкретному адресату. Такая атака может быть запущена командой хорошо организованных хакеров, однако более вероятно, что она организуется одним или несколькими хакерами, которые контролируют большое количество Зомби компьютеров, захваченных Троянскими конями. Поток почтовых сообщений, полученный на адрес мишени для почтовой бомбы, превышает ограничение на размер почтовых сообщений и может привести к сбою в работе почтовой системы.

5.4.4. Угрозы физической безопасности Web-серверов

Web-сервер и тесно связанные с ним компьютеры, такие как серверы базы данных и серверы транзакций, которые используются для снабжения коммерческого Web-сайта данными и возможностью обрабатывать транзакции, должны быть защищены от физического повреждения. Для многих компаний эти компьютеры стали хранилищами важных данных (информация о клиентах, продуктах, продажах, покупках и платежах) и являются важной частью функции генерации дохода. Как ключевые физические ресурсы системы электронной коммерции эти компьютеры должны иметь высокий уровень защиты против угроз их физической безопасности. Именно поэтому коммерческие компании часто используют аутсорсинг для хостинга серверов и передают обслуживание своих серверов компаниям, которые имеют возможность обеспечить более надёжную защиту серверным компьютерам, чем сама коммерческая компания.

Многие компании осуществляют резервное копирование контента серверов и сохраняют копии на удалённом оборудовании. Если функционирование Web-сервера критично, для продолжающейся деятельности компании, она может полностью дублировать свои сервера на удалённом оборудовании. В случае выхода из строя основной системы, все операции в Web могут быть переданы дублирующему оборудованию менее чем за одну секунду. Примерами коммерческой деятельности, которая требует полного дублирования серверной системы компании, являются системы резервирования на авиалиниях, торговые системы фондовых брокеров и банковские платежные и расчётные системы.

Некоторые коммерческие компании полагаются на Интернет провайдера в обеспечении физической безопасности своих серверов. Интернет провайдеры, обычно, предлагают заключить дополнительное соглашение к основному договору о хостинге, в котором

оговариваются условия по обеспечению безопасности серверов. Другие компании нанимают небольшие фирмы, специализирующиеся на обеспечении физической безопасности серверной системы. Стоимость услуг этих фирм колеблется в диапазоне от 200 до 2000 долларов в месяц.

5.4.5. Контроль доступа и аутентификация

Контроль доступа и аутентификация относятся к вопросу контролирования того, кто или что имеют доступ к Web-серверу. Большинство людей, работающих с Web-сервером, получают к нему доступ, с помощью удалённого клиентского компьютера. Аутентификацией мы называем проверку идентичности той сущности, которая запрашивает доступ к компьютеру. Такой сущностью может быть человек или компьютерная программа. Точно также как пользователи могут аутентифицировать серверы, с которыми они взаимодействуют, серверы могут аутентифицировать индивидуальных пользователей. Когда серверу требуется позитивная идентификация пользователя, он может запросить клиента прислать сертификат.

Сервера могут аутентифицировать пользователей несколькими способами. Во-первых, сервер может проверить цифровую подпись пользователя, содержащуюся в сертификате, с использованием открытого ключа пользователя. Если сервер не может расшифровать цифровую подпись пользователя, содержащуюся в сертификате, то он делает вывод, что сертификат получен не от его истинного владельца, и отклоняет запрос на доступ. Во-вторых, сервер может проверить временну́ю отметку на сертификате для того чтобы убедиться, что не истёк срок его действия. Сервер отклоняет доступ для тех пользователей у которых истёк срок действия сертификата. В-третьих, сервер может использовать *систему обратной связи* (callback system), в которой программа сервера сверяет имя и адрес клиентского компьютера пользователя со списком авторизованных клиентских компьютеров.

Имена пользователей и пароли также нуждаются в защите. Для аутентификации пользователей, с использование пары «имя пользователя-пароль», сервер должен обладать базой данных, в которой хранятся эти пары. Большинство серверов хранят имя пользователя в виде обычного текста, а пароль в зашифрованном виде. Когда имя пользователя хранится в виде обычного текста, а пароль зашифрован, система проверяет достоверность пользователя путём сравнения введённого имени с именем, хранящимся в базе данных, а пароль сравнивается с зашифрованным паролем, хранящимся в базе данных. Если оба пароля совпадают, то авторизация принимается. Поэтому в большинстве систем даже администратор не может сообщить пользователю его забытый пароль. Вместо восстановления забытого пароля администратор должен предложить новый временный пароль, который пользователь может, в последующем, изменить и сохранить.

Имя пользователя и пароль могут быть сохранены в куки-файле на клиентском компьютере, что даёт клиенту преимущества, поскольку он имеет возможность получать доступ к участкам сайта, требующим авторизации, без ввода имени и пароля. Однако, следует помнить, что куки-файлы хранятся на клиентском компьютере в виде обычного текста, поэтому имя пользователя и пароль в куки-файле видимы любому, кто имеет доступ к клиентскому компьютеру.

Web-сервера часто обеспечивают безопасность файлов при помощи списка управления доступом, который ограничивает доступ к файлам. В *список управления доступом* (access control list – ACL) включены имена тех пользователей, которые могут получать доступ к файлу. Каждый файл снабжён своим списком управления доступом. Когда клиентский компьютер запрашивает у сервера доступ к некоторому файлу или документу, снабжённому списком управления доступом, сервер проверяет, находится ли клиент в ACL этого файла. Такая система контроля особенно удобна для ограничения доступа к файлам, размещённым на серверах интранет сетей, в которых пользователь может получать доступ к информации, которая предназначена только для него. Web-серевер может осуществлять точный контроль доступа к своим файлам путём классификации доступа на: (1) доступ с возможностью только чтения файла, или (2) доступ с возможностью и

чтения и редактирования файла. Например, некоторым пользователям сети интранет разрешается читать файл с данными о наёмных работниках корпорации, но не разрешается его редактировать. Редактирование этого файла разрешается только менеджеру отдела управления трудовыми ресурсами (отдела кадров) и эта привилегия доступа указана в ACL наряду с именем и паролем менеджера.

5.4.6. Брандмауэры

Брандмауэром (firewall) называется программное обеспечение или комбинация программного и аппаратного обеспечения, которое устанавливается в компьютерной сети для контроля трафика, проходящего в сеть и из сети. Для реализации функций брандмауэра обычно используется отдельный компьютер. Брандмауэр является средством межсетевой защиты и устанавливается между локальной сетью и Интернет, или между локальной сетью и другой локальной сетью, которая может представлять угрозу. Оперирование брандмауэров основано на следующих принципах.

- Весь трафик между сетью, снабжённую брандмауэром, и внешней сетью должен проходить через брандмауэр.
- Только трафик, детерминированный политикой безопасности компании, может проходить через брандмауэр.
- Сам брандмауэр неуязвим от внешнего проникновения.

Сеть, снабженная брандмауэром, часто называется *надёжной сетью* (trusted network), а внешняя сеть – *ненадёжной сетью* (untrusted network). Работая как фильтр, брандмауэр пропускает в надёжную сеть только сообщения, разрешённые политикой безопасности. Например, брандмауэр, реализующий некоторую политику безопасности, может пропускать в надёжную сеть (и из надёжной сети) HTTP трафик, но не пропускать трафик FTP или Telnet. При помощи брандмауэров можно разделять одну физическую корпоративную сеть на несколько логических частей и, например, не разрешать персоналу, одного из отделов компании, получать допуск к информации другого отдела этой же компании.

Крупные корпорации, обладающие множеством территориально распределённых сайтов должны инсталлировать брандмауэры в каждом месте, где есть внешнее подключение корпоративной сети к Интернет. Такая система гарантирует непроницаемый *периметр безопасности* для всех сетей корпорации. Все брандмауэры периметра должны реализовывать одну и ту же политику безопасности. В противном случае один из брандмауэров может разрешать проникновение в корпоративную сеть тех сообщений, которые запрещаются другими брандмауэрами. Без согласованной политики безопасности нежелательный доступ к сети, через брешь в одном из брандмауэров, может поставить под угрозу информационные активы всей корпорации.

Компании должны удалить всё ненужное программное обеспечение со своих брандмауэров. Небольшое количество программ в брандмауэре уменьшает шансы на выявление брешей в безопасности программного обеспечения брандмауэра. Поскольку компьютер брандмауэра используется только как средство межсетевой защиты, на нём должны размещаться только операционная система и прикладные программы, предназначенные для реализации функций брандмауэра. Физический доступ к брандмауэру должен быть ограничен консолью, подключенной непосредственно к компьютеру брандмауэра. Менеджеры компании должны запрещать удалённое администрирование брандмауэром для того чтобы избежать угроз внешней атаки на брандмауэр под видом администратора.

Брандмауэры разделяются на следующие типы или категории: (1) брандмауэр типа фильтр пакетов; (2) брандмауэр типа сервер шлюза и (3) брандмауэр типа прокси-сервер.

Брандмауэр типа *фильтр пакетов* (packet-filter firewalls) проверяет все данные, которыми обменивается надёжная сеть и внешняя сеть. При пакетной фильтрации проверяются источник, адрес доставки и порты входящих пакетов. Запрет или разрешение на

передачу пакетов в надёжную сеть базируется на предопределённом наборе правил в программном обеспечении брандмауэра.

Брандмауэр типа *сервер шлюза* (gateway server) фильтрует трафик в зависимости от того какое приложение посылает запрос. Сервер шлюза ограничивает доступ к надёжной сети для специфических приложений, таких как Telnet, FTP и HTTP. В отличие от техники пакетной фильтрации, брандмауэры уровня приложений фильтруют запросы и регистрируют их на уровне приложений, а не на более низком уровне IP протокола. Брандмауэр типа сервер шлюза осуществляет классификацию, регистрацию и анализ запросов. Примером политики, реализуемой сервером шлюза, является разрешение на проход в надёжную сеть для всех входящих FTP запросов, но блокировка всех исходящих FTP запросов. Такая политика не позволяет пользователям надёжной сети загружать на свои компьютеры потенциально опасные программы из Интернет.

Брандмауэр типа *прокси-сервер* (proxy server) взаимодействует с Интернет «от имени и по поручению» надёжной сети. Когда браузер настроен на использование брандмауэра типа прокси-сервера, то запрос браузера передаётся в Интернет непосредственно брандмауэром. Когда из Интернета приходит ответ на запрос, то прокси-сервер передаёт его браузеру. Прокси-сервер используется, также, как большая кэш-память для Web-страниц.

Современные компании часто нанимают на работу сотрудников, выполняющих свои функции дистанционно при помощи домашних компьютеров, а также сотрудников с мобильными компьютерами. Это увеличивает количество компьютеров, которые должны быть защищены при помощи брандмауэров и носит наименование проблема *расширения периметра* (perimeter expansion). Проблема расширения периметра причиняет особые беспокойства тем компаниям, у которых имеются наёмные работники или субподрядчики, использующие ноутбуки для доступа к конфиденциальной информации компании со всех типов сетей и из различных мест.

Хакеры тратят много времени и усилий пытаясь получить доступ к серверам компаний. Поэтому компании часто инсталлируют системы обнаружения вторжения как часть своих брандмауэров. *Система обнаружения вторжения* (intrusion detection system) спроектирована таким образом, что она осуществляет мониторинг попыток зарегистрироваться на сервере и анализа этих попыток, путём сравнения с шаблонами, характерными для хакерских атак.

Как только система обнаружения вторжения выявляет вероятную атаку, она блокирует дальнейшие попытки регистрации, которые осуществляются с того же IP адреса, до тех пор, пока менеджер по безопасности не проверит и не проанализирует попытки доступа и не решит, являются ли они атакой на сервер.

По мере того, как всё большее количество компаний полагаются на облачные вычисления в ключевых видах деятельности, возрастает необходимость в обеспечении безопасности в облачной среде. Разработка брандмауэров, предназначенных для облачных вычислений, продвигается вперёд быстрыми темпами, но всё же отстаёт от спроса на такие брандмауэры. Вместо реализации отдельной политики безопасности для каждого сервера, такие брандмауэры должны навязывать единую политику для всех серверов в облаке. Одна из проблем разработки брандмауэров в облачной среде заключается в том, что сервера в облаке не работают стационарно, а разворачивают или сворачивают свою деятельность в зависимости от потребности в их ресурсах.

В дополнение к компьютерам брандмауэрам, которые компании устанавливают для защиты своих компьютерных сетей, существуют программные брандмауэры, предназначенные для защиты индивидуальных клиентских компьютеров. Такие брандмауэры часто называют *персональные брандмауэры* (personal firewalls). Использование персональных брандмауэров является важным инструментом при решении проблемы расширения периметра безопасности во многих компаниях. Часто пользователи домашних компьютеров инсталлируют персональные брандмауэры на свои компьютеры. Дополнительную информацию о защите домашнего компьютера при помощи персональных брандмауэров можно найти на сайте Gibson Research Shields Up!

ЗАДАНИЯ ДЛЯ СЕМИНАРСКИХ ЗАНЯТИЙ

1. Представьте себе некоторую онлайновую компанию, которая продаёт на своём Web-сайте снаряжение и принадлежности для туризма, скалолазания и альпинизма. Компания предлагает около 1200 различных наименований товаров, а её сайт ежедневно посещают примерно 1000 человек. Компания осуществляет около 200 продаж в день, со средней стоимостью транзакции в 372 доллара, и доставляет заказы своим покупателям с двух территориально распределенных сладов. Компания принимает все основные типы кредитных карт и самостоятельно осуществляет их обработку. Данные о транзакциях сохраняются в базе данных на отдельном сервере базы данных. Сервер базы данных и Web-сервер располагаются в отдельном помещении в офисе компании. Разработайте и опишите политику безопасности для компании. Рассмотрите существующие угрозы с учётом того, что в базе данных хранятся номера кредитных карт клиентов компании. При работе над политикой безопасности используйте образцы и шаблоны политики безопасности других компаний, а также рекомендации по разработке политики безопасности, которые Вы найдете в Web.

2. Многие компании и организации полагаются на брандмауэры для предотвращения или обнаружения угроз информационной безопасности, источником которых являются внешние сети. Осуществите поиск в Web, и разыщите информацию о том, какие задачи, связанные с инсталляцией брандмауэра, необходимо решать коммерческой компании в том случае, когда она часть своей системы электронной коммерции реализует при помощи облачных вычислений. Опишите и проанализируйте эти задачи с точки зрения проблемы расширения периметра безопасности.

3. Представьте, что Вы разработали мобильное приложение, которое позволяет пользователям безопасно хранить свои пароли на смартфонах или планшетных компьютерах. Приложение включили в свои списки онлайновые магазины Google Play и Apple App Store. Некоторые компании, такие, например, как TrustArc предлагают услуги в области гарантий безопасности, которые могут убедить потенциальных покупателей в том, продукт, которые они применяют, является безопасным и может быть использован. Посетите сайт компании TrustArc (или сайт другой компании, которая, в качестве третьей стороны, предлагает услуги по обеспечению гарантий безопасности для онлайновых продавцов). Сделайте обзор услуг, которые предлагает эта компания. Сфокусируйте внимание на услугах, полезных для разработчиков мобильных приложений. Оцените эти услуги и сделайте вывод о том, какими из них и почему Вы бы хотели воспользоваться при дистрибуции своего приложения.

4. Разыщите три Web-сайта, которые обладают цифровыми сертификатами с расширенной проверкой подлинности (EV-SSL). Обратите внимание не то, что некоторые коммерческие сайты, которые обладают EV-SSL сертификатом, не отображают символ сертификата в адресном окне браузера до тех пор пока Вы либо не авторизуетесь на сайте, либо не поместите какой-либо товар в тележку для покупок. Для каждого сайта укажите центр сертификации, выдавший EV-SSL сертификат. Сделайте краткий обзор этого центра сертификации, а также объясните, почему, с Вашей точки зрения, сайт решил нести дополнительные расходы, покупая EV-SSL сертификат.

5. Американская компания Bibliofind была основана в 1996 году и специализировалась на продаже редких и коллекционных книг. В 1999 году компания Bibliofind была поглощена компанией Amazon.com, однако сайты обоих компаний функционировали независимо. В 2001 году сайт компании Bibliofind был взломан хакерами. Злоумышленники получили доступ к Web-серверу компании и заменили страницы сайта на

их искажённые версии. Компания была вынуждена закрыть свой сайт и предпринять полное исследование его безопасности. Когда специалисты компании внимательно проверили все случаи авторизации на сервере компании, они обнаружили, что порча Web-страниц на сайте является только «вершиной айсберга». Анализ показал, что хакеры получали доступ к компьютерам компании в течение четырёх месяцев. За это время они смогли, через Web-сервер, получить доступ к серверам транзакций, на которых хранилась персональная информация 98 тысяч клиентов компании (фамилии, адреса и номера кредитных карт). Персональные данные о клиентах хранились на серверах в виде обычного текста. Последующее расследование хищения персональных данных не смогло выявить злоумышленников.

- Объясните, каким образом Bibliofind могла использовать брандмауэры для предотвращения доступа злоумышленников к серверам транзакций. В каких местах компьютерной сети нужно было установить брандмауэры, и какими правилами они должны были руководствоваться для фильтрации трафика.
- Объясните, каким образом шифрование могло бы помочь предотвратить ущерб от проникновения в сеть Bibliofind или минимизировать его эффект.
- В законодательстве ряда стран закон, который предписывает компаниям информировать своих клиентов о случаях похищения их персональных данных во время хакерских атак на сервера компаний. До введения в действие этого закона, многие компании возражали против него, аргументируя свои возражения тем, что закон породит множество судебных исков, затрудняющих функционирование компаний. Предложите аргументы «за» и «против» такого рода законов.

6. Представьте, что Вы работаете консультантом по информационным технологиям в крупной компании, которая производит и продаёт промышленное оборудование (оборудование для сборочных линий, оборудование для упаковочных линий, гидравлическое оборудование и т.п.). Директор компании предложил Вам участвовать в разработке новой маркетинговой идеи. Идея заключается в том, чтобы создать Web-сайт, совместно с тремя другими компаниями, производящими оборудование, функционально дополняющее оборудование, производимое Вашей компании. Кроме информации об оборудовании и сопутствующих технологиях, сайт должен содержать страницы, на которых клиенты компаний смогут размещать информацию о продаже своего оборудования, бывшего в употреблении. По мнению директора это будет способствовать ускорению обновления оборудования клиентами компании. Команда, занимающаяся разработкой сайта, идентифицировала несколько проблем в области безопасности, которые необходимо решить при создании сайта. Вам поручено изучить две технологии в области безопасности: цифровые сертификаты и шифрование, а также рассмотреть применимость этих технологий для обеспечения безопасности будущего сайта.
   - Подготовьте два отчёта для участников команды разработчиков сайта: (1) отчёт о цифровых сертификатах и (2) отчёт о шифровании. Каждый отчёт должен объяснять суть технологии и описывать несколько типовых примеров их применения.
   - Предположите, что проект сайта одобрен и внедрён, а разработчики сайта приняли решение требовать от всех клиентов, участвующих в проекте, получить цифровые сертификаты. Подготовьте отчёт, адресованный клиентам, выразившим желание работать с сайтом, в котором объясните, почему они должны получить цифровые сертификаты, как необходимое условие участия в проекте.