ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
ГОУВПО «Пермский государственный университет»

К.А. Юрков, Л.Н. Лядова, А.В. Хлызов, Г.В. Климов

Технологии создания систем электронной коммерции

Учебно-методическое пособие

Пермь 2007

УДК 681.3
ББК 32.97
Ю74

Юрков К.А.

Ю74 Технологии создания систем электронной коммерции: учеб.-метод. пособие / К.А. Юрков, Л.Н. Лядова, А.В. Хлызов, Г.В. Климов; Перм. ун-т. – Пермь, 2007. – 80 с.: ил.

ISBN 5-7944-1049-3

Рассматриваются основные понятия, используемые в литературе, посвященной описанию технологий и инструментальных средств создания систем электронной коммерции. Дается описание различных секторов рынка электронной коммерции. Приводятся типовые технологические решения, применяемые при разработке систем электронной коммерции различного назначения.

Пособие предназначено для студентов, изучающих современные информационные технологии и их применение для создания информационных систем в различных предметных областях. Может быть полезно преподавателям, ведущим занятия по дисциплинам, связанным с изучением и использованием технологий e-commerce.

Рецензент – доктор физ.-мат. наук, профессор, директор учебного центра «Информатика» *С.В. Русаков*

Печатается в соответствии с решением редакционно-издательского совета Пермского государственного университета

Данное пособие является победителем конкурса, проведенного Пермским государственным университетом в ходе реализации инновационной образовательной программы «Формирование информационно-коммуникационной компетентности выпускников классического университета в соответствии с потребностями информационного общества» в рамках приоритетного национального проекта «Образование».

УДК 681.3
ББК 32.97

ISBN 5-7944-1049-3

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время средства электронной коммерции (e-commerce) широко используются в различных областях: в банковской сфере, розничной торговле, при проведении сделок между бизнес-партнерами. Однако зачастую понятие электронной коммерции в издаваемых книгах сужается до рассмотрения систем розничной торговли с использованием возможностей Internet.

Невозможно представить деятельность современной фирмы, корпорации без использования средств вычислительной техники (ВТ), информационных систем (ИС), созданных на базе современных информационных технологий. Эти средства внедрены во все сферы деятельности. С этой точки зрения любую информационную систему, любые средства, обеспечивающие деятельность коммерческих структур (в частности, системы поддержки принятия решений, управления электронными документами и пр.), можно отнести к средствам электронной коммерции. Однако это – слишком широкое понимание. В данном пособии рассматриваются технологии и средства, традиционно относящиеся к системам e-commerce.

Цель данного пособия – познакомить преподавателей и студентов с различными секторами электронной коммерции, возможностями используемых в них средств, а также применяемых для разработки таких систем технологий и инструментальных средств.

Особое внимание уделяется банковскому сектору электронной коммерции, платежным системам, а также средствам защиты систем e-commerce.

Пособие предназначено в первую очередь для студентов механико-математического факультета (специальность/направление «Прикладная математика и информатика»), изучающих соответствующий спецкурс. Студенты данной специальности получают фундаментальные знания в области информационных технологий (ИТ), осваивают различные инструментальные средства создания систем различного назначения. Данный курс расширяет

перечень традиционных дисциплин, позволяет познакомиться с одной из наиболее перспективных областей применения полученных знаний.

Книга также может быть полезна и студентам других факультетов, в частности экономического факультета, которые в своей практической работе должны будут использовать описанные в пособии средства.

ОСНОВЫ ЭЛЕКТРОННОЙ КОММЕРЦИИ

В настоящих условиях в более выигрышных условиях находится тот, кто опережает конкурентов по объему, достоверности и своевременности получения доступной для анализа и использования информации. Развитие информационных технологий создает новую реальность – информационное сообщество. Прежде ресурсы и технологии, необходимые для экономического развития, были жестко связаны с территориями. В настоящее время главными ресурсами становятся финансы, интеллект и информация, которые обладают свойством мобильности. Это свойство усиливается с развитием Internet как среды существования и распространения информации.

Развитие информационных технологий привело к появлению нового понятия – электронный бизнес (e-business), или электронная коммерция (e-commerce).

Электронная коммерция – это любая форма бизнеса, в котором бизнес-процессы, взаимодействие между субъектами происходят с помощью электронных технологий, т.е. для ведения бизнеса (организации документооборота, финансовых расчетов и прочих операций) используется вычислительная техника, с ее помощью реализуется сбор, хранение и обработка электронной информации, обмен электронными документами.

Это определение является очень широким и давно используется в таком толковании. В последнее время термин «электронная коммерция» чаще используют в более узком смысле – любое использование сети Internet для ведения бизнеса (организации документооборота и платежей, продажи товаров, предоставления

услуг и т.п.). Однако это определение слишком сужает рассматриваемую область.

В данном пособии мы будем рассматривать все средства, применяемые для осуществления финансовых операций, торговли и заключения и проведения сделок между бизнес-партнерами с использованием ИТ.

Этапы развития электронной коммерции

Термин «электронный бизнес» появился практически одновременно с появлением ЭВМ и началом их использования для решения коммерческих задач, реализации коммерческих расчетов (60-е гг. XX в.). Основой вычислительных систем коммерческого назначения в то время являлись большие универсальные компьютеры – мэйнфреймы, это была эпоха коммерческих «mainframe-based» приложений. Примерами таких приложений стали программы, автоматизировавшие решение задач в сфере транспортных услуг (заказ билетов, обмен данными между различными службами при подготовке рейсов и т.п.), задач учета производства и реализации товаров и услуг и т.д.

При решении различных задач было разработано несколько индустриальных стандартов для реализации подобных систем. Согласование этих стандартов в США позволило создать новый стандарт для организации электронного обмена данными между организациями – EDI (Electronic Data Interchange), который получил название ANSI X.12 (host-based). Этот стандарт был ориентирован на различные транспортные системы.

При разработке стандарта для обмена данными в Англии была выбрана ориентация на торговлю. В результате появился набор стандартов Tradacoms для международной торговли. Эти стандарты Европейская экономическая комиссия приняла в качестве международных стандартов GTDI (General-purpose Trade Data Interchange standards).

Поскольку сосуществование двух стандартов препятствовало развитию торгового бизнеса, были предприняты усилия по объединению стандартов обмена информацией. В 80-е и 90-е гг. XX в. разработан международный стандарт EDIFACT

(Electronic Data Interchange for Administration, Commerce and Transport), принятый ISO. В качестве транспортной системы EDIFACT использует стандарт электронной почты X.400. В 1997 г. было намечено окончательное объединение стандартов, но реально это не произошло, так как появилась возможность проведения операций электронной коммерции через Internet.

Расширение Internet, развитие Web-технологий заставили произвести коррекцию планов развития электронного бизнеса. Появился новый тип бизнеса – розничная торговля и оказание услуг через Internet (иногда (ошибочно!) только этот тип коммерции и называют электронной коммерцией).

Передача информации через Internet является более дешевой, чем организация документооборота при помощи передачи электронной почты через частные сети. Для обеспечения эффективного использования Internet как среды для организации электронной коммерции был разработан стандарт EDIINT (EDIFACT over Internet) на базе электронной почты, а позднее появился еще один стандарт – OBI (Open Buying on the Internet), главная идея которого – ориентация на открытые системы (в нем декларируются принципы соответствия программного обеспечения электронной коммерции открытым Internet-стандартам). OBI опирается на EDIINT, но он охватывает значительно больший класс вопросов стандартизации всех форм взаимодействия между организациями, вовлеченными в полный цикл покупки–продажи–поставки товаров.

Современный этап характеризуется широким использованием технологий мобильного бизнеса.

Вопросы для самопроверки

1. Дайте определение понятия «электронная коммерция» в широком и в узком смысле.
2. Перечислите этапы развития электронной коммерции. Охарактеризуйте стандарты и технологии систем e-commerce, связанные с каждым этапом.

Секторы рынка электронной коммерции

Организация взаимодействия в рамках электронной коммерции зависит от субъектов электронной коммерции и конкретного сектора рынка электронной коммерции.

Существует три типа субъектов электронной коммерции:

- *Финансовые институты* – различные финансовые организации (в первую очередь – банки, так как именно в банках все остальные субъекты электронного бизнеса имеют свои счета, по которым производится реальное движение средств, соглашение о котором регламентируется платежными схемами электронной коммерции, в частности, электронной Internet-коммерции).
- *Бизнес-организации* – любые организации, использующие для реализации бизнес-процессов и взаимодействия средства электронной коммерции (в настоящее время к этому типу в первую очередь причисляют организации, продающие или приобретающие что-либо через Internet).
- *Клиенты* – покупатели или потребители услуг на рынке электронной коммерции.

Взаимодействие между субъектами этих трех типов можно представить с помощью схемы, показанной на рис. 1, где стороны треугольника представляют различные типы субъектов, а стрелками показаны связи между ними.

Все стандарты, выработанные в области электронной коммерции, были первоначально ориентированы на взаимодействие между бизнес-организациями (на рис. 1 этот тип взаимодействия показан дугообразной стрелкой). Этот сектор рынка электронной коммерции называется *сектор «бизнес-бизнес» (business-to-business, B2B), или «компания-компания»*. В этом секторе электронной коммерции существуют различные взаимоотношения между организациями: *производители* товара продают его через своих *поставщиков* (*suppliers*) или через *дистрибьютеров* (*distributors*), которые работают, в свою очередь, через дилеров (dealers) и перекупщиков (реселлеров – resellers). В том случае, когда деловым партнером бизнеса выступает тот или иной госу-

дарственный институт, обычно выделяют отдельный сектор «*бизнес-правительство*» *B2G (business-to-government, B2G).*

Сектор рынка электронной коммерции, в котором клиент (конечный покупатель) приобретает что-либо для себя (взаимодействие на рис. 1 показано стрелкой, направленной со стороны клиента к бизнес-организациям), называется *розничным сектором электронной коммерции (retail sector)*. Такие взаимоотношения называют также *B2C* – (*business-to-consumer*). *Торговые компании* (*merchants*), работающие на этом секторе ранка, предлагают на продажу товары различных *поставщиков*.

Финансовый сектор рынка электронной коммерции делится на две части: банки и все остальные финансовые институты: фондовый рынок, брокерские компании, процессинговые компании, осуществляющие финансовые транзакции.

Наиболее распространенными услугами в финансовом секторе рынка электронной коммерции являются услуги по обработке счетов и чеков, поэтому основная часть этого сектора принадлежит банкам.

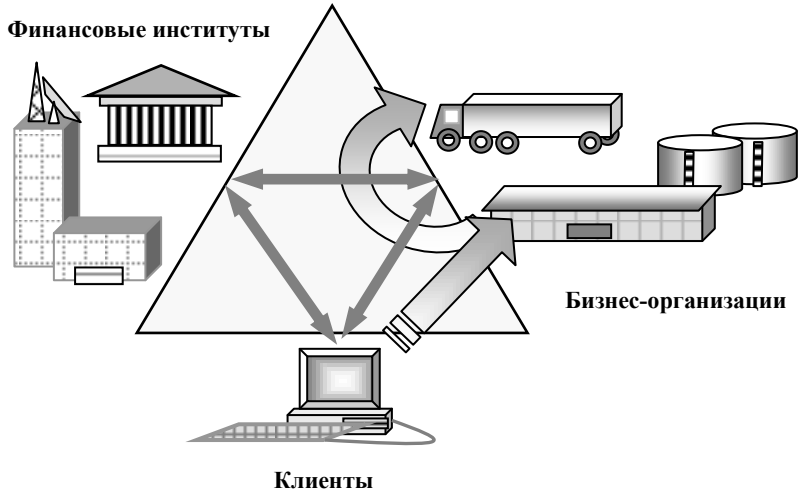


Рис. 1. Субъекты электронной коммерции и их взаимодействие

Банковский сектор подразделяется на несколько секторов:
- сектор «клиент-банк» – сектор предоставления банковских услуг организациям;
- сектор «home banking» – предоставление услуг по обслуживанию частных лиц;
- межбанковский сектор – банки обычно используют для взаимодействия традиционные стандарты SWIFT или каких-либо клиринговых компаний, взаимодействие реализуется в рамках стандарта FinancialEDI.

Основной услугой финансового сектора рынка является *обработка чеков и счетов* (*bill payment processing services*).

В настоящее время банки предлагают своим клиентам (от частных лиц до крупнейших компаний) управление банковскими счетами в реальном масштабе времени и из любой точки планеты, имеющей доступ в сеть. Развитие этих услуг привело к появлению новых терминов – *e-banking* (*электронный банкинг*) и *Internet-banking*.

Электронный банкинг – это технология удаленного банковского обслуживания, позволяющая клиенту получать банковские услуги, не посещая банковский офис. В развитии услуг *удаленного банкинга* (как для физических лиц, так и для организаций эту технологию оказания услуг иногда называют *home-banking*) можно выделить несколько этапов:
- *телефонный банкинг* (telephone-banking) – обслуживание счетов по телефону – банковский сервис, основанный на использовании возможностей телефонов с тональным набором номера;
- *видео-банкинг* (*video-bankign*) – система интерактивного общения клиента с персоналом банка;
- *PC-банкинг* (*PC-banking*) – технологии, позволяющие клиенту с помощью персонального компьютера и модема напрямую (не через Internet) подключаться к серверам банка и совершать банковские операции;
- *Internet-банкинг (Internet-banking)* – сетевой банкинг (*net-banking*, *on-line banking*) – оказание услуг банками по дистанционному управлению счетами через Internet.

Internet-банкинг является логическим продолжением предшествовавших ему разновидностей удаленного банкинга. В настоящее время термины *е-банкинг* и *Internet-банкинг* часто используют как синонимы. Для удаленного банковского сервиса для корпоративных клиентов используют еще одно название – *corporate Internet-banking*.

Удаленное управление счетами обычно подразумевает оказание следующих услуг: операции со своими счетами (проверка состояния счетов, балансы, выписки, перевод средств с одного счета на другой), переводы и оплата услуг и товаров (разовые и периодические платежи), инвестирование средств (депозиты, ценные бумаги, валютные операции) и даже кредитование, а также предоставление клиенту информационной поддержки и сопутствующих услуг. По статистике более 80% всех банковских операций клиент может осуществить, находясь за компьютером дома или в своем офисе.

Наиболее развит Internet-банкинг в США: уже в конце 1998 г. 4,5 млн семей совершали банковские операции через Internet, прирост числа пользователей составил более 40%. По прогнозам консалтингового агентства Booz, Alen & Hamilton к концу 2000 г. число потребителей банковских Internet-услуг в мире должно было превысить 16 млн человек.

Такой сервис в настоящее время является неотъемлемой частью Internet-бизнеса, интегрирующего системы *B2C*, *B2B*, *e-trading* (электронная торговля на биржах) и др. Именно финансовый сектор является базовым для развития других секторов электронной экономики.

В России электронный бизнес (широко используется термин *электронная торговля* – ЭТ, хотя это более узкое понятие) активно развивается. По данным SETonline, за 2006 г. только сектор *B2B* продемонстрировал рост оборотов более чем на 50%. Активно развиваются также секторы *B2C* (*business-to-consumer*) и *B2G* (*business-to-government*).

Категории участников рынка электронной коммерции показаны в табл. 1. Основные показатели рынка электронной коммерции (ЭК) в России приведены в табл. 2.

Таблица 1. Категории участников электронной торговли, 2007

Сектор	Представители сектора	Годовой объем оборота 2006, млн дол.	Годовой прирост оборота 2006-2005, %	Число участников рынка	Годовой прирост числа участников, %
B2B	Независимые операторы электронных торгов (e-marketplace)	1200	87	19	28
	Корпоративные закупочные площадки (e-procurement)	4300	46	54	22
	Системы электронной дистрибуции (e-distribution)	650	38	13	30
	Всего по B2B	**6150**	**54**	**86**	**25**
B2C	Internet-магазины	1500	49	900	31
B2G	Специализированные организации (закупки / продажа)	2450	22	29	24

Таблица 2. Общие показатели рынка электронной торговли, 2007. Источник: SETonline, НАУЭТ, 2007 г.

Оборот рынка ЭТ, млрд дол.	10,1
Доля рынка ЭТ в структуре ВВП, %	1,04%
Доля рынка ЭТ в структуре корпоративных закупок, %	2,4%.

Отметим, что *B2G* и *B2B* сектора развиваются параллельно, практически не пересекаясь. Так, согласно аналитикам из Tender.Pro: «Государство обязывает госсектор использовать конкурсные методы закупок, стимулируя этим электронные закупки. А бизнес никто не обязывает, поэтому если они выбирают такой способ, то выбирают его сознательно из соображений экономической выгоды. При этом государство свело все виды электронных закупок только к аукциону, а коммерческому сектору доступны и аукционы, и тендеры, и запросы котировок».

По результатам исследования европейского агентство по Internet-исследованиям, Gemius SA, электронная коммерция в России находится на начальной стадии развития, но обладает огромным потенциалом. Исследование мнений и предпочтений рос-

сийских пользователей Internet относительно покупок в Internet-магазинах и online-аукционах проводилось посредством «online pop-up опросников», отбиравших респондентов, используя cookies. Выводы из результатов исследования таковы: электронная коммерция в России находится на начальной стадии развития, но обладает огромным потенциалом. 98% российских Internet-пользователей знают о возможности совершать online-покупки, но фактически совершали их немногим более половины (примерно 53%). Online-покупки до сих пор не считаются достойной альтернативой обычным магазинам. Тем не менее, 68% покупателей приобретают товары по Internet несколько раз в году и чаще. Как выяснили эксперты, 43% узнают из Internet о мобильных новинках; 45% примерно раз в год заказывают по Internet туристические услуги; а около 50% несколько раз в год online-покупают косметику, компьютерные игры и детские товары. Более четверти покупателей (27%) считают, что увеличению числа покупок будет способствовать снижение цен. В то же время покупатели как Internet-магазинов (56%), так и online-аукционов (43%) отмечают среди их преимуществ более низкие цены, чем в обычных магазинах. Основная проблема в развитии электронной коммерции – недоверие операциям, совершаемым через Internet: 43% покупателей считают online-покупки рискованными, и в большинстве случаев оплата товара производится наличными. Отказ от покупки в Internet-магазинах или на online-аукционах происходит чаще всего вследствие сложности самой процедуры покупки (31%), отсутствия возможности увидеть товар вживую (27%) и опасения, что оплата через Internet небезопасна (23%).

В табл. 3 приведены объемы сделок всего рынка электронной коммерции за 1996 г. и прогнозы, которые были сделаны для 2000 г. Современное состояние различных секторов рынка электронной коммерции значительно превышает прогнозировавшиеся показатели, что во многом связано, в частности, с развитием мобильного бизнеса.

Как видно из данных табл. 3, наиболее динамично развиваются финансовый сектор и сектор «бизнес-бизнес». Из 7 млрд дол. оборота электронной коммерции в 1997 г. 6 млрд дол. приходится на сектор «бизнес-бизнес».

Таблица 3. Объемы сделок рынка электронной коммерции

Сектор рынка электронной коммерции	1996 г.	2000 г.
«Бизнес-бизнес»	$600 млн.	$66 470 млн.
Финансовый сектор	$200 млн.	$23 000 млн.
Розничный сектор	$530 млн.	$7 170 млн.

Примечание. В таблице показаны данные маркетинговых исследований и прогнозов Forrester Research

Розничный сектор электронной коммерции также все более активно использует Internet-технологии. Иногда именно его называют электронной коммерцией, но правильнее было бы называть его сектором Internet-торговли.

По данным исследования Ernst & Young сегментации потребительского рынка, в декабре 1997 г. розничный рынок электронной коммерции составляет по различным группам товаров следующие части: книги – 24%, компакт-диски – 18%, электроника – 12%, спортивные товары и игрушки – 12-13%, программное обеспечение – 9%, другие товары – 27%.

Использование Internet-технологий выгодно для банков вследствие нескольких причин. Наиболее важной из них является получаемая банками выгода от сокращения затрат на обработку транзакций при использовании для их передачи открытых каналов сети Internet (табл. 4).

Таблица 4. Стоимость обработки банковских транзакций

Способ передачи транзакции	Стоимость
Стандартная банковская транзакция	$1.08
Стандартная банковская транзакция, передаваемая по выделенным каналам корпоративной банковской системы	$0.54
Стандартная банковская транзакция, передаваемая по коммутируемым каналам корпоративной (клиент-банк)	$0.26
Стандартная банковская транзакция, передаваемая по открытым каналам сети Internet	$0.13

Примечание. Источник данных – отчет компании Booz Alen & Hamilton (1996 г.) (Таблица взята с российского сайта Некоммерческого партнерства CommerceNet.)

В действительности стоимость одной Internet-операции для банка может быть еще ниже – она может составлять от 0,01 дол. до 0,13 дол.

Банки, специализирующиеся на Internet-сервисе, имеют явное преимущество по сравнению с обычными банками по уровню процентных ставок по депозитам, кредитам, а также по стоимости обслуживания. (Например, усредненная ставка по депозитам в обычных банках США по данным www.money-rates.com составляет 3,43% годовых, а в Internet-банках – 4,53%; совокупная стоимость годового обслуживания, выраженная в процентах годовых, в обычных банках составляет 3,08%, а в Internet-банках – 1,30%.)

Кроме того, использование Internet для оказания банковских услуг дает еще ряд *преимуществ*:

- Internet позволяет отказаться от специализированных программ – клиенту нет необходимости покупать и устанавливать специальное программное обеспечение, он может использовать вместо них обычный браузер; для этого клиент должен лишь получить в банке имя и пароль для входа в систему, а также ключи для создания электронных подписей. Однако применение на клиентских местах специализированных программ позволяет повысить безопасность проведения операций.
- Пользователь имеет возможность получить через Internet множество дополнительных услуг: просмотр оперативной информации (тарифы, условия размещения депозитов, ставки, выписки по счетам и т.п.) и образцов документов, возможность производить платежи и т.д.
- Internet-банкинг позволяет банкам сохранить свою клиентскую базу: переезжая на новое место, можно остаться клиентом прежнего банка.
- Пользователь получает возможность управлять своими счетами из любой точки планеты, где есть доступ к Internet. При этом платеж по филиальной сети идет примерно 20 минут.
- Банк имеет возможность следить за предпочтениями клиентов, проводить гибкую адресную политику. Есть воз-

можность реализации концепции «розничного банка»: благодаря современным технологиям решается проблема развития операций с «мелкой» клиентурой без создания чрезмерно громоздкой и дорогой филиальной сети.

– Internet-банкинг легко интегрируется в Internet-коммерцию: в дополнение к Internet-банкингу реализуются система электронной коммерции для взаимодействия корпоративных клиентов банка (*B2B*) и система *B2C* для оказания компаниями – клиентами банка услуг клиентам – физическим лицам. При реализации этих услуг в полном объеме заказчик может выбрать товар на электронной «витрине», получить счет и оплатить его через автоматизированную систему банка. В то же время поставщик получает сведения о заказе. Доставка товара осуществляется фирмой-продавцом или специальным агентством. При этом гарантируется своевременность прохождения платежей (оплата производится в реальном времени). Товары могут оплачиваться со счета и/или при помощи пластиковой карты.

Основной проблемой Internet-банкинга является обеспечение безопасности расчетов и сохранности средств на счетах клиентов. Защита обеспечивается специальными аппаратными и программными средствами. Причем эти средства должны быть установлены как в банковской системе, так и на стороне клиента.

Еще одна слабая сторона Internet-банкинга – процедура внесения денег на счет. Для «полувиртуального» банка, предоставляющего услуги и через Internet, и «off-line», эта проблема легко решается – достаточно посетить реальный банк. Для пополнения же счетов без визитов в банк требуются дополнительные затраты – почтовые и банковские переводы облагаются комиссионными.

Первый банк, обслуживающий клиентов через Internet, появился в США в 1995 г. Это был Security First Network Bank (www.sfnb.com). К началу 2000 г. в США более 90% из первых 50 крупнейших банков имеют программы Internet-банкинга. В России первым банком, начавшим обслуживание клиентов через Internet, стал Автобанк (www.avtobank.ru). Подробную информацию о российских банках, предлагающих Internet-сервис в

России, можно получить через Internet (www.internetfinance.ru, www.bankir.ru и др.).

Вопросы для самопроверки

1. Назовите основные секторы рынка электронной коммерции.
2. Перечислите этапы развития технологий электронного банкинга.
3. Назовите преимущества электронного банкинга. Сравните возможности различных технологий удаленного банкинга.
4. Какие услуги получает пользователь розничного сектора электронной коммерции. Охарактеризуйте возможности этого сектора, применяемые в нем технологии.

Практические задания

1. Найдите в Internet информацию о наиболее известных Internet-магазинах и услугах, оказываемых с помощью Internet. Укажите соответствующие ссылки.
2. Какие товары и услуги предоставляются через Internet? Укажите соответствующие ссылки. Проанализируйте состояние розничного рынка электронной коммерции на основе доступной в Internet информации.

Инструментарий электронной коммерции

Сектор «бизнес-бизнес» электронной коммерции развивается через общенациональные стандарты (EDI – Electronic Data Interchange). Концепция EDI состоит в следующем: каждая организация имеет свои собственные прикладные бизнес-системы (приложения системы управления производством, системы складского учета, бухгалтерии и т.п.) и EDI-шлюз (EDI gateway), через который организация обменивается стандартными сообщениями со всеми другими организациями. Единое EDI-пространство организуется поверх различных телекоммуникационных протоколов (X.25, TCP/IP и др.) и поверх электронной почты и Internet

(рис. 2). Таким образом, любая организация, входящая в EDI-сообщество, получает возможность работать со всеми EDI-партнерами, независимо от их числа.

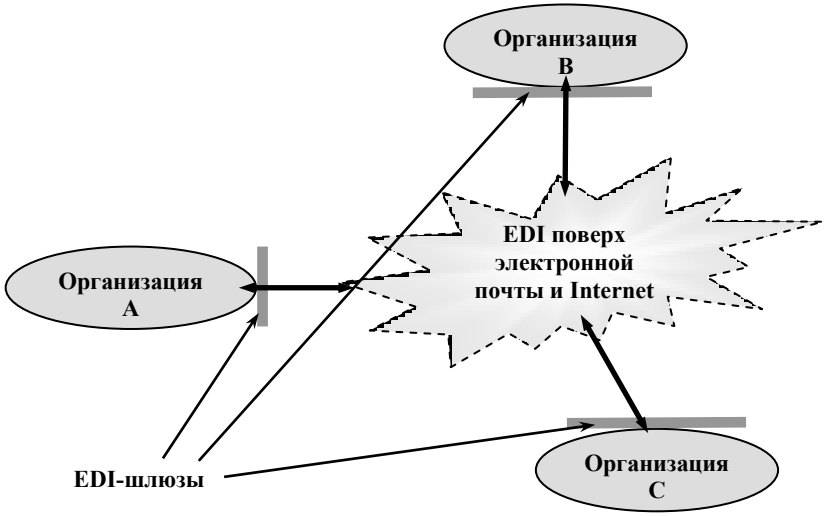


Рис.2. Взаимодействие организаций на основе EDI

В настоящее время происходит миграция от EDI к так называемым Web-Based-EDI, т.е. EDI, построенным на Web-серверах, позволяющим организовать взаимодействие через Internet. Это снижает стоимость EDI-систем и делает их полностью транзакционными.

Инструментальные средства электронной коммерции можно условно разделить на несколько групп:

- бизнес-приложения,
- Internet-магазины,
- средства связи с финансовыми организациями через различные платежные системы,
- средства мобильного бизнеса,
- шлюз в EDI-систему.

Программное обеспечение, используемое организациями, зависит от характера их деятельности и связей, установленных с другими организациями.

Если организация ориентирована на прямые продажи товаров через Internet-магазины (является субъектом розничного сектора электронной коммерции – retail), то эта организация является продавцом и она должна владеть Internet-магазином или взять его в аренду (рис. 3). Клиенты получают доступ к «витрине» магазина с помощью обычных средств навигации в Internet, оформляя свои покупки на сайте организации, представляющем Internet-магазин.

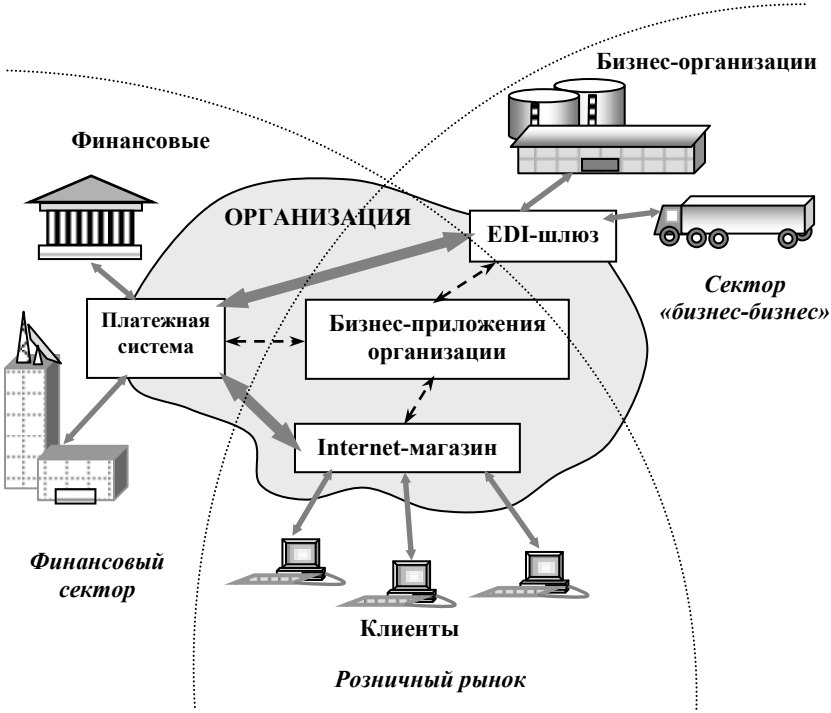


Рис. 3. Инструментарий электронной коммерции

Если организация взаимодействует с другими организациями (является субъектом сектора «бизнес-бизнес» электронной коммерции), то для нее возникает необходимость установить взаимодействие с партнерами в on-line режиме по транзакционной схеме. Таким образом, в секторе «бизнес-бизнес» предполагается прямое взаимодействие между бизнес-процессами в разных организациях-партнерах.

Связь организации с финансовыми институтами необходима в любом случае. Схема платежной системы зависит от предложений со стороны банков, клиентом которых является данная организация, от процессинговых центров и т.д. Организации вынуждены подстраиваться под предлагаемые ими схемы расчетов. В платежных схемах электронной коммерции должны быть реализованы прямые интерфейсы и к Internet-магазинам, и к EDI.

Internet-торговля составляет лишь небольшую долю рынка электронной коммерции, но именно в секторе розничной торговли появился новый стандарт – SET (система «безопасных электронных транзакций»). В рамках SET решаются технические проблемы взаимодействия трех субъектов рынка электронной коммерции. Но вместе с тем SET не решает вопросы документооборота между организациями, не затрагивает вопросы стандартизации традиционного финансового сектора рынка электронной коммерции (home-banking, клиент-банк). Кроме того, этот стандарт ориентирован на то, что основным платежным средством являются электронные карточки, которые при использовании Internet в качестве среды для проведения операций не являются лучшим решением.

Основными производителями инструментария для создания систем электронной коммерции в мире являются компании Ariba, Broadvision, iCAT, IBM, Information Builders, Intershop Communications, Microsoft, Netscape, Open Market, Oracle, VeriSign.

Вопросы для самопроверки

1. Сформулируйте основные положения концепции EDI.
2. Охарактеризуйте развитие EDI-систем.
3. Назовите основные категории инструментальных средств e-commerce.
4. Охарактеризуйте требования, которым должны удовлетворять системы электронной коммерции, создаваемые для различных секторов рынка e-commerce.
5. Где происходит «пересечение» различных категорий систем. Объясните ответ.

Практические задания

1. Сравните возможности наиболее популярных Internet-магазинов и используемые технологические решения, оцените интерфейс пользователя. Приведите соответствующие ссылки и обоснуйте свои выводы.
2. Представьте типовую структуру Internet-магазина. Какие функциональные возможности реализованы?
3. Найдите в Internet информацию о средствах создания систем розничной торговля. Какие возможности они обеспечивают?
4. Используя свободно распространяемые средства создания Internet-магазинов, разработайте прототип системы розничной торговли через Internet. Подготовьте руководство по эксплуатации и электронную презентацию разработанной системы.

Электронные платежные системы

Развитие Internet-экономики невозможно без развития эффективных, охватывающих максимальное число участников рынка платежных систем.

Внедрение электронных технологий, реализация на их основе новых инструментов проведения операций в сфере банковской деятельности началось более двадцати лет назад. В настоящее время широко внедряются так называемые электронные банковские системы, использующие все новые инструментальные средства (электронные деньги (e-cash), смарт-карты (smart-card) и т.д.), а также возможности, предоставляемые Internet.

Существуют различные классификации электронных платежных систем. В зависимости от того, чем оперируют электронные платежные системы (ЭПС), их можно условно классифицировать по трем основным типам:

1) карточные системы,

2) операторы цифровой наличности,

3) платежные шлюзы.

К первым относятся ЭПС, работающие с обычными банковскими картами (Visa, MasterCard и т.д.). Системы второго типа оперируют с так называемой цифровой наличностью – некой

внутренней валютой, которую можно обналичить у соответствующих участников ЭПС. Платежные шлюзы представляют собой синергию карточных систем и операторов цифровой наличности, предоставляя широкие возможности для взаимной конвертации и способов оплаты товаров и услуг в Internet. Стоит отметить, что значительная часть существующих ЭПС относится именно к шлюзам, несмотря на то, что многие из них выделяют определенный тип платежей как доминирующий.

Карточные системы

Рассмотрим более детально эти два типа электронных платежных систем. Начнем с традиционных систем карточных счетов. Прием пластиковых карт Internet-магазинами – уже давно свершившийся факт: кредитки принимает в настоящее время огромное количество Internet-магазинов во всем мире. Вместе с тем, в России количество последних незначительно в связи с рядом обстоятельств (как субъективных, так и объективных), существенно замедляющих развитие данного сервиса. Тем не менее оплата с помощью кредиток в Internet-магазинах пользуется огромной популярностью во всем мире. Не последнюю роль (причем с обеих сторон) здесь играет психологический фактор: электронные деньги нельзя «подержать в руках». Это обстоятельство приводит к тому, что при использовании кредитной пластиковой карточки ее владелец обычно тратит значительно большие суммы, нежели при расплате наличными. Очевидно, что это обстоятельство не может не радовать Internet-магазины.

Данная тенденция характерна не только для Internet-магазинов. Оффлайновые продавцы также весьма охотно работают с кредитными карточками. Это обстоятельство свойственно как для мирового рынка, так и для российского, несмотря на то, что кредитные карты здесь только начинают приобретать популярность. Примечательно, с дебетовыми («зарплатными») пластиковыми картами Internet-магазины практически не работают. Так, согласно исследованию, проведенному компанией IMCA по заказу MasterCard, российские граждане при использовании кредитных карт в среднем тратят на 30% больше средств, чем при применении дебетовых.

Вообще, по данным IMCA, в среднем в России по одной кредитной карте в месяц тратится около 8,5 тыс. руб., в то время как аналогичный показатель по дебетовым картам составляет на 2 тыс. руб. меньше. Причем, как показало исследование IMCA, для тех, кто пользуется пластиковой карточкой не реже 4 раз в месяц, эти же показатели составляют 13,5 тыс. руб. и 9,15 тыс. руб. на каждую карту соответственно. Наряду с продавцами в этой системе есть еще одна заинтересованная сторона – сами банки, которые очень часто стимулируют использование кредитных карт, устанавливая более высокие проценты за снятие денег по кредиткам, чем в случае пользования дебетовыми картами. В результате владельцу кредитки выгоднее расплачиваться именно ею, а не наличными, что приводит к проявлению указанного выше психологического фактора.

Все сказанное применимо к Internet-магазинам в еще большей степени: деньги по кредитке «легко тратятся» и карточку не надо «держать в руках». Выгода для Internet-магазина и удобство для пользователя очевидны. Тем не менее, и здесь имеется множество подводных камней.

Для пользователя эти «камни» связаны, прежде всего, с большими рисками в плане утери данных о своей кредитной карте, и, как следствие, потерям денег. Кроме того, ситуация осложняется еще и тем, что при осуществлении электронного платежа по карточке нет практически никакой возможности однозначно идентифицировать плательщика, чтобы убедиться, что он расплачивается собственными картами. Отсутствие чека с подписью дает потенциальную возможность (в том числе и настоящим владельцам карт, вступившим в сговор со злоумышленником) получения отказа от осуществления той или иной покупки. В результате Internet-магазинам выставляются так называемые чарджбэки (штрафы, возвраты), от количества которых зависят не только репутация Internet-магазина, платежной системы и банка-эквайера, но даже сама возможность дальнейшей работы.

Как отмечают аналитики, ущерб от мошенничества с кредитными картами в мире достигает многих миллиардов долларов в год, что отражается на лояльности пользователей (особенно потенциальных) к использованию электронных платежей. Мошенничество с электронными картами создает проблемы и для

второй стороны – Internet-магазинов, а также всех участников электронного платежа. Причем для продавцов (в нашем случае – Internet-магазинов) эти проблемы оказываются наиболее существенными.

Рассмотрим более детально схему прохождения электронного платежа (рис. 4).

Рис. 4. Типовая схема реализации электронного платежа

Прежде всего необходимо определить основных участников схемы. Прием (процессинг – обработка) пластиковых карт в качестве средств оплаты товаров и услуг в Internet называется Internet-эквайрингом. Основные участники электронного платежа:

1) покупатель,
2) Internet-магазин,
3) банк-эмитент (банк, выдавший карточку),
4) банк-эквайер (банк, который проводит первичную обработку транзакции и обеспечивает весь спектр операций с карточками, реализуемый партнерами),
5) платежный сервер (электронная платежная система, обеспечивающая безопасность прохождения платежа и многое другое).

Стоит отметить, что существуют схемы и без использования платежного сервера, но они в настоящее время практически не используются вследствие огромных рисков.

Таким образом, карточная электронная платежная система фактически является гарантом безопасного транспорта карточных данных к процессинговому центру банка-эквайера. Безусловно, в реальности эти системы выполняют значительно более широкие функции и предлагают множество сервисов, но основное их назначение именно таково.

С юридической точки зрения карточные электронные платежные системы являются обычным агентом в управлении операциями с карточным счетом владельца карты. По сути, они оперируют лишь записями о деньгах в банке, но никак не с самими деньгами. Типичные представители этого класса систем в России – компании Cyberplat, Assist, Chronopay и др. Примечательно, что подобные системы пока не получили широкого распространения в России, в то время как Internet-платежи по картам очень популярны за рубежом, где пластиковые карты являются основным платежным средством. В нашей же стране наиболее популярны электронные платежные системы второго типа – оперирующие с цифровой наличностью. Рассмотрим их подробнее.

Системы цифровой наличности

Огромные масштабы мошенничества привели к появлению принципиально нового типа электронных платежных систем, которые работают не с картами, а с собственной валютой, эквивалентной согласно определенному курсу реальным деньгам. Пользователь, зарегистрировавшийся в системе, получает собственный Internet-кошелек – по сути, его счет в конкретной электронной платежной системе. Пополнив этот виртуальный кошелек реальными деньгами, владелец «электронного бумажника» получает возможность использовать находящиеся в нем средства для оплаты товаров и услуг в партнерских Internet-магазинах системы.

Пополнение счета происходит различными способами (в зависимости от системы): это и специальные предоплаченные карты, и банковский перевод, и почтовый перевод, и внесение денег

на счет наличными в специализированных киосках и даже банкоматах банков-партнеров электронной платежной системы, а также наличными в специальных обменных пунктах. Возможно также пополнение «кошелька» путем обмена в электронных обменных пунктах. Вывод денег из системы обычно весьма запутан и неудобен (для пользователя – для самой системы такая схема максимально выгодна). В результате пользователь получает некое хранилище, положить в которое деньги значительно проще, чем «достать» их в случае необходимости (большие проценты, малое количество способов вывода денег и пр.). Вместе с тем для использования самих денег, лежащих в Internet-кошельке клиента, создано огромное количество вариантов.

Основное преимущество электронных платежных систем, оперирующих цифровой наличностью, – возможность осуществления анонимных платежей.

Основы цифровой наличности заложил Давид Чаум, создав технологию eCash. Несмотря на то, что электронные деньги достаточно прочно вошли в повседневную жизнь многих людей, перспективы развития таких систем и их будущее достаточно неопределенны, что обусловлено неопределенностью юридического статуса самих систем. Строго говоря, даже называть их электронными платежными системами не совсем верно, так как они оперируют виртуальными единицами (так, WebMoney называет себя «системой имущественных прав», а «Яндекс.Деньги» – «предоплаченный финансовый продукт»). Вместе с тем данные платежные системы принимают весьма активное (и все более возрастающее) участие не только в электронной коммерции, но и в товарно-денежном обороте страны.

Примечательно, что приверженцы платежных систем с цифровой наличностью делают большой акцент на безопасность своих Internet-кошельков и платежей. Когда-то именно этот аспект (в связи мошенничеством с карточными платежами в Internet) оказался решающим для появления такого типа систем. Некоторые платежные системы цифровой наличности даже предложили в свое время сервис по пополнению Internet-кошельков с карточек, справедливо полагая, что это позволит значительно увеличить популярность таких систем. Популярность действительно возросла, но прежде всего – у мошенников, благодаря той же

анонимности. Так, например, в течение менее чем полугода с момента запуска подобного сервиса в WebMoney мошенники изъяли около 1,5 млн WMR (1 WMR = 1 руб.).

Вместе с тем системы «цифровой наличности» хорошо развиваются, имеют свою аудиторию и идеально подходят для решения целого ряда задач. В ряде случаев пользоваться такими системами удобнее и проще, чем карточными.

Электронные платежные системы в России

Как отмечалось выше, действующие в России ЭПС можно разделить на три основные категории:

1) традиционные карточные системы,

2) платежные шлюзы,

3) системы цифровой наличности.

Первый тип ЭПС оперирует с обычными банковскими картами при оплате товаров и услуг в Internet. К ним можно отнести голландскую ЭПС ChronoPay.

Платежные системы второго типа – шлюзы – интегрируют различные типы ЭПС и провайдеров услуг, включая карточные ЭПС, системы цифровой наличности и т.д., предоставляя единый интерфейс для оплаты в единой системе. Подавляющее большинство российских ЭПС также достаточно условно можно отнести к этому типу. Это такие системы, как Assist (ориентируется на карточные системы, однако работает и с цифровой наличностью), CyberPlat (включает также Internet-банкинг), «Рапида», RUpay (интегрирует более 20 различных способов приема платежей в Internet-магазине), Fethard и др.

К системам третьего типа относятся так называемые системы цифровой наличности – ЭПС, эмитирующие свою собственную валюту определенного номинала, которую можно обналичить согласно установленному курсу системы. К ЭПС данного типа относятся «Яндекс.Деньги» и WebMoney. Косвенно к подобным системам можно отнести и e-port, основным платежным

средством которого является единая предоплаченная карта собственной эмиссии.

Сделать грамотные оценки оборота игроков рынка платежных систем достаточно сложно в силу того, что большинство систем, работающих на рынке, имеют принципиально разные бизнес-модели. Применение среднегодовых показателей роста определенных ЭПС («Яндекс.Деньги», «Рапида» и др.) к месячным оборотам, например, годовой и двухгодовой давности, которые официально известны, приведет лишь к очень грубым оценкам, вероятно, значительно отличающимся от реальных либо в меньшую, либо в большую сторону.

Тем не менее для понимания качественной картины некоторые оценки все-таки сделать можно (основные показатели приведены в табл. 5).

Для «Рапиды» это сделать сложнее – слишком давно были объявлены последние достоверные данные по обороту компании (по итогам августа 2003 года выручка системы за месяц составила около 2 млн дол.). Бизнес «Рапиды» за указанный период развивался достаточно неравномерно, поэтому любая оценка, основанная на среднегодовых показателях роста в целом по рынку для схожих систем («Рапида» не сообщает даже относительных цифр динамики оборота), будет слишком грубой.

Примечательно, что такая большая структура, как «Яндекс.Деньги», также не раскрывает своих оборотов. Тем не менее выручку «Яндекс.Деньги» по итогам 2005 г. можно оценить. По данным самой компании, этот показатель по итогам августа 2005 г. составил 300 млн руб. При учете ряда критериев можно оценить среднемесячную выручку «Яндекс.Деньги» на уровне около 10,45 млн дол. Таким образом, по итогам 2005 г. выручка «Яндекс.Деньги» составила, по оценкам CNews Analytics, около 125 млн дол.

Таблица 5. Ключеевые показатели ЭПС

Система	Год основания	Тип	Оборот	
			2004 г.	2005 г.
Киберплат	1997	Платежный шлюз/карточная система/Internet-банк	459	1120
КредитПилот	1999	Платежный шлюз	н/д	н/д
Рапида	2001	Платежный шлюз	~2/мес.	н/д
ОСМП	2004	Платежный шлюз	83	498
Платежные системы	2005	Платежный шлюз	-	28,5
Элекснет	2000	Система по приему платежей	190,9	346,6
Яндекс.Деньги	2002	Система цифровой наличности	н/д	125*
Assist	1998	Платежный шлюз/карточная система	25	40
ChronoPay	2003	Карточная система	-	7**
e-port	1999	Платежный шлюз	325,2	740,5
Fethard	2001	Платежный шлюз	н/д	100
MoneyMail	2005	Платежный шлюз	н/д	н/д
RUpay	2002	Платежный шлюз	н/д	н/д
WebMoney	1998	Система цифровой наличности	338,9	647,9

Совокупный оборот 10 из 14 рассмотренных систем по итогам 2005 г. составил 3,5 млрд дол., что почти на 148% больше аналогичного показателя 2004 г. Среднегодовой прирост выручки указанных систем по итогам 2005 г. составил 178%. При этом максимальную положительную динамику продемонстрировала компания ОСМП, оборот которой по итогам 2005 г. вырос на 500%.

Примечательно, что из указанных 3,5 млрд дол. чуть более 3,3 млрд дол., или свыше 94%, приходится на выручку 5 электронных платежных систем – «Киберплат», ОСМП, e-port, WebMoney и «Элекснет». Причем из указанных игроков первые три имеют относительно близкие бизнес-модели, WebMoney же «выбивается» из этого списка и в этом смысле значительно опе-

режает ближайших конкурентов в своем сегменте, например систему «Яндекс.Деньги». «Элекснет» также имеет отличную от других модель: бизнес компании преимущественно построен на эксплуатации масштабной сети терминалов самообслуживания.

Очевидно, что максимальные обороты демонстрируют системы, бизнес-модели которых оптимизированы под прием платежей в пользу операторов мобильной связи. Огромное количество потенциальных потребителей делают это сегмент очень емким и достаточно легко доступным. Internet-бизнес значительно сложнее. Кроме того, платежеспособная аудитория Рунета еще не подготовлена для осуществления действительно массовых платежей в Internet. Так, по итогам 2005 г. некоторые эксперты оценивают объем российского рынка B2C на уровне 800 млн дол., что почти в 10 раз меньше, чем оборот одного Internet-магазина Amazon.com и в 100 раз меньше B2C-рынка США. Для сравнения: оборот 20 крупнейших российских Internet-магазинов по итогам 2005 г. едва превысил 300 млн дол.

B2C сегмент активно развивается в России, причем показатели роста достигают 50% в год. Достаточно активно развивается и сегмент C2C. Высокая положительная динамика наблюдается и у российского рынка банковских карт. В результате в Рунете появляется все больше электронных платежных систем. Некоторые из них рассматриваются в данном обзоре. Но по оценкам экспертов можно насчитать около 20-30 так или иначе действующих российских электронных платежных систем. Так, в 2005 г. появилась платежная система «Система», оборот которой уже по итогам рассматриваемого периода составил 28,5 млн дол. О высоком потенциале российского рынка говорит еще и тот факт, что все большее число иностранных игроков обращает на него внимание. На российский рынок вышла и голландская карточная платежная система Chronopay, которая рассматривает Россию как один из приоритетных регионов для своей деятельности.

На 2005 г. наибольший успех по занятию рынка сопутствовал платежным шлюзам и ЭПС цифровой наличности (рис. 5). Так, оборот компании CyberPlat по итогам 2005 г. увеличился на 144% и достиг 1 120 млн дол. Таким образом, «рекордная символическая планка» выручки, составляющая в 1 млрд дол. преодолена. Примечательно, что доходы игроков растут фактически в

геометрической прогрессии – только по итогам мая 2006 г. оборот CyberPlat превысил 200 млн дол.

Второе место по обороту по итогам 2005 г. заняла компания e-port, оборот которой в отчетном периоде увеличился на 127% по сравнению с 2004 г. и составил 740,5 млн дол. Третье место заняла компания WebMoney, оборот которой по итогам 2005 г. по титульным знакам WMR превысил 3 млрд 263 млн., а по титульным знакам WMZ – 534 млн 236 тыс. Рост по сравнению с аналогичными показателями 2004 г. составил 145% и 83% соответственно. Пересчет по среднему курсу доллара США к рублю по итогам 2005 г. (28,7 руб./дол.) показывает, что оборот WebMoney по итогам 2005 г. превысил 647 млн дол.

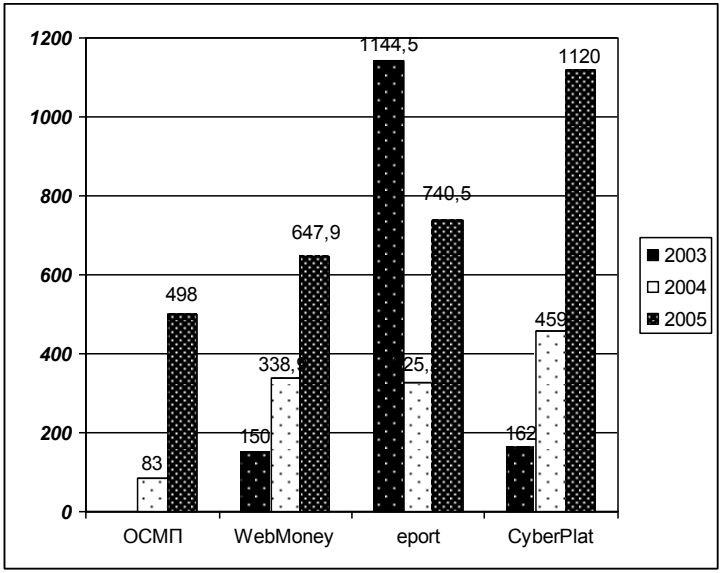


Рис. 5. Динамика оборота крупнейших ЭПС России, млн дол.

Совокупный оборот четырех крупнейших электронных платежных систем России (CyberPlat, e-port, WebMoney и ОСМП) по итогам 2005 г. увеличился почти на 150% по отношению к 2004 г. и превысил 3 млрд дол. При этом темпы роста за предыдущий период (2004/2003 гг.) были еще выше. Соответствующие

показатели тогда составили 164% и 1,2 млрд дол. Стоит отметить, что компания ОСМП вышла на рынок только в 2004 г., тогда ее оборот составил 83 млн дол. Однако уже по итогам 2005 г. выручка ОСМП увеличилась почти на 500% по сравнению с 2004 г. и достигла значимых показателей – 483 млн дол.

Почти 40% от указанного совокупного оборота (37,3%) по итогам 2005 г. приходится на выручку компании CyberPlat. Оставшиеся три компании из «большой четверки ЭПС» приблизительно поровну делят почти 1,9 млрд дол. Тем не менее сравнивать указанные платежные системы по оборотам не совсем корректно из-за абсолютно разных моделей бизнеса всех четырех ЭПС. Так, CyberPlat и e-port собирают практически все свои доходы за счет приема платежей в счет оплаты услуг сотовой связи (у обеих компаний доля платежей за мобильную связь в структуре оборота достигает 97-99%). Компания CyberPlat получает более 15% выручки каждого из операторов «большой тройки» России. Аналогичная ситуация наблюдается у ОСМП – доля платежей в пользу операторов связи в обороте данной ЭПС достигла по итогам 2005 г. 98%. Однако ОСМП помимо дилерской сети, достаточно активно развивает направление организации терминалов самообслуживания. Впрочем, лидирующим игроком на этом рынке является компания «Элекснет».

Успех таких ЭПС очевиден – произвольный размер транзакции, который они обеспечивают, позволил им быстро снискать огромную популярность. Действительно, возможность не покупать скретч-карты минимум за 150 руб., но при этом пополнить свой баланс более мелкими суммами, например, 20-30 руб., очень удобна. И большинство людей, оплачивающих услуги мобильной связи в магазинах, киосках, банкоматах и т.д., даже не подозревают, кто служит провайдером данной услуги. Разумеется, бизнес-модель WebMoney кардинально отличается от указанной.

Различия в бизнес-моделях указанных ЭПС заметны и в структуре оборота компаний. Так, CyberPlat и e-port получают почти 99% своего оборота с дилерской сети, в то время как доля платежей в Internet составляет у данных ЭПС менее 1%. У WebMoney, напротив, практически весь оборот проходит по платежам в Internet. Принимая во внимание многочисленные различия в бизнесе трех рассматриваемых ЭПС, можно отметить,

что сопоставляются они лишь для получения качественной картины рынка электронных платежей.

Об условности приведенной выше классификации ЭПС говорит и тот факт, что даже те системы, которые формально можно отнести к платежным шлюзам, существенно различаются между собой. Так, Assist специализируется исключительно на платежах в Internet, преимущественно осуществляемых по банковским картам. Оборот компании по итогам 2005 г. вырос на 60% по сравнению с финансовыми показателями 2004 г. и достиг 40 млн дол. Другая карточная ЭПС, работающая на российском рынке, – голландская ChronoPay – заработала в рассматриваемом периоде 7 млн дол. Заметим, что ChronoPay – очень молодая система, которая была образована лишь в 2003 г., а на российский рынок вышла лишь в 2005 г. Оборот ChronoPay на европейском рынке по итогам 2005 г. составил 45 млн дол.

Как уже упоминалось, практически весь оборот компаний e-port и CyberPlat приходится на дилерскую сеть, и оба игрока делают основной акцент на ее развитии. В качестве ключевого критерия масштабности дилерской сети обычно приводится такой параметр, как количество точек приема платежей.

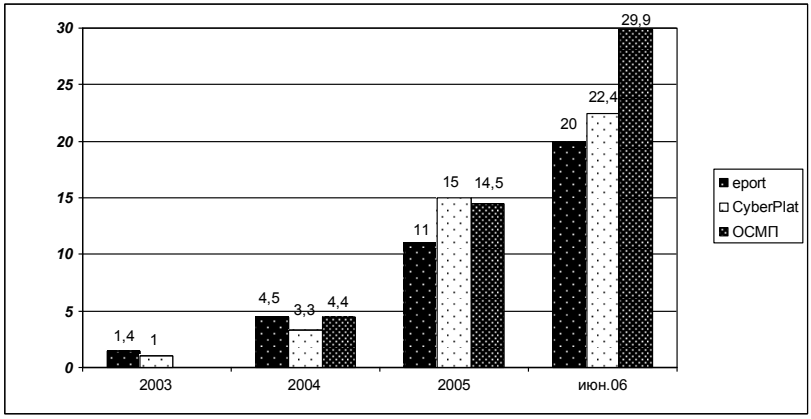
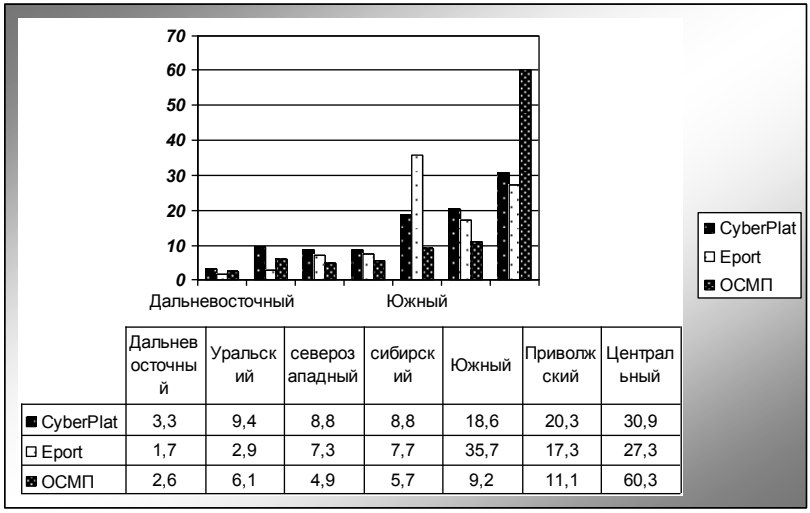


Рис. 6. Динамика количества точек приема платежей, тыс. шт.

По итогам 2005 г. лидером по указанному параметру стала компания CyberPlat, дилерская сеть которой составила в рассматриваемом периоде свыше 15 тыс. точек приема платежей (рис. 6).

Причем уже в июне 2006 г. это количество увеличилось до 22,4 тыс. Показатели e-port несколько скромнее – около 11 тыс. по итогам 2005 г. и 20 тыс. по итогам июня 2006 г. Аналогичные показатели характерны для компании ОСМП, которая также активно развивает дилерскую сеть и по количеству точек приема платежей по итогам июня 2006 г. стала лидером рынка; хотя, как отмечают игроки рынка, увеличение за полгода почти вдвое количества точек приема платежей, вызывает некоторое удивление.

Интересно также проанализировать региональную структуру точек приема платежей e-port и CyberPlat (рис. 7). Наибольшее количество точек приема платежей CyberPlat находится в Центральном федеральном округе (6 920), в то время как у e-port на первом месте по количеству точек неожиданно оказывается Южный федеральный округ (здесь присутствует 5 682 точки, причем больше половины из них (52%) приходится на три республики – Дагестан, Чечню и Ингушетию (1 934, 650 и 373 соответственно)). У CyberPlat на три указанных три субъекта Южного федерального округа приходится в 4 раза меньше точек приема платежей, чем у e-port – 1 398 (1 366, 3 и 29 точки соответственно).



	Дальневосточный	Уральский	северозападный	сибирский	Южный	Приволжский	Центральный
CyberPlat	3,3	9,4	8,8	8,8	18,6	20,3	30,9
Eport	1,7	2,9	7,3	7,7	35,7	17,3	27,3
ОСМП	2,6	6,1	4,9	5,7	9,2	11,1	60,3

Рис. 7. Региональная структура точек приема платежей

Центральный федеральный округ у компании e-port занимает лишь второе место – 4 347 точек оплаты. У CyberPlat же на втором месте следует Приволжский федеральный округ (4 554 точек), у e-port этот же округ занимает третье место (2 754 точек). Венчает тройку лидеров у CyberPlat южный федеральный округ (4 159 точек). Примечательно, что у обеих компаний развитый Северо-западный федеральный округ уступает Сибирскому (1 962 против 1 967 точек приема платежей у CyberPlat, и 1 219 против 1 183 точек приема платежей у e-port).

Региональная структура точек приема платежей ОСМП имеет ярко выраженный акцент на присутствие в Центральном федеральном округе. На этот регион приходится свыше 60% всех точек приема платежей компании. На втором месте – Приволжский федеральный округ, в котором расположено чуть более 11% точек приема платежей. Замыкает тройку лидеров Южный федеральный округ – здесь ОСМП обладает 2 770 пунктами оплаты (9,2%). Хотя во всех остальных федеральных округах России ОСМП имеет схожее с Южным присутствие.

Как уже упоминалось, все три компании ориентированы на развитие дилерской сети. В частности, CyberPlat активно развивает партнерскую программу. Так, партнер CyberPlat не обязательно должен иметь юридические (договорные) отношения с компаниями, которые он привлекает в платежную систему, кроме того, он также не обязан быть дилером CyberPlat. После заключения соглашения основная обязанность партнера – осуществление поиска торгово-сервисных точек, желающих организовать прием платежей. На основе заключенного соглашения и по результатам работы партнера ему выплачивается вознаграждение, размер которого составляет 0,1% от месячного объема платежей привлеченного дилера.

Партнерская программа e-port в основном касается Internet и базируется на размещении различных информеров по оплате услуг (разумеется, через e-port) на сайте компании-партнера. Дилерская программа ОСМП построена на активном стимулировании партнеров различными ценными призами и бонусами по итогам оценки работы того или иного дилера по жесткой системе критериев. Все дилеры ОСМП делятся на 5 категорий по объему приема платежей. По итогам 2005 г. максимальная доля прихо-

дилась на I категорию (крупнейшую: объем приема платежей свыше 60% дилеров, принимающих участие в партнерской программе, превышает 9 млн руб.).

Классификация способов платежей

Рассмотрим варианты классификации способов платежей.

Идентификационные карточки уже долгое время широко применяются в сфере бизнеса. Наиболее известным примером таких карточек является кредитная карта.

Долгое время были распространены так называемые *магнитные карточки*, которые содержат идентификационный номер пользователя карты, ключ шифрования и некоторые контрольные данные, используемые совместно с паролем пользователя, подтверждающим его подлинность. Ключ шифрования применяется для шифрования сообщения о сделке при пересылке его в компьютер банка.

Интеллектуальные карточки (или *смарт-карты*) кроме магнитных полосок, хранящих перечисленную выше информацию, содержат также и микропроцессоры с небольшим объемом памяти.

Смарт-карта – это пластиковая карта со встроенным микропроцессором, выполняющим функции контроля доступа к памяти смарт-карты и производящим ряд специфических функций. Функции микропроцессоров определяются назначением карты: носитель идентификационной информации и финансовых данных в системах оплаты телефонных разговоров и электронных расчетов (финансовые карты), хранение данных (в том числе криптографических ключей), карты контроля, обеспечивающие физический доступ к некоторым объектам. Архитектура любой интеллектуальной карты предусматривает наличие нескольких типов памяти, используемых для хранения данных различного назначения и программного обеспечения карты, системы ввода/вывода, предназначенной для обмена данными с внешними устройствами, встроенной системы безопасности, обеспечивающей защиту данных, хранящихся и обрабатываемых в сматр-карте (это может быть специальный криптографический сопро-

цессор, осуществляющий функции криптографического преобразования данных).

Для обеспечения безопасности смарт-карт при применении их в платежных системах используется двусторонняя аутентификация, основанная на криптографических протоколах типа «запрос-ответ», и аутентификация пользователя карты (с помощью специального кода или биометрических методов идентификации пользователей).

Электронные деньги являются эквивалентом бумажных денег, обладающим собственными свойствами: их можно пересылать по Internet или телефонным каналам; их легко размножить и скопировать, как и любую другую электронную информацию, следовательно, необходимо обеспечить уникальность каждой электронной банкноты. Кроме того, при использовании электронных денег необходимо обеспечить секретность проведения операций. Таким образом, реализация электронных денег требует использования специальных криптографических протоколов.

Существующие платежные системы могут быть построены на основе смарт-карт или с использованием Internet, в них могут быть реализованы различные схемы проведения платежей (рис. 8).

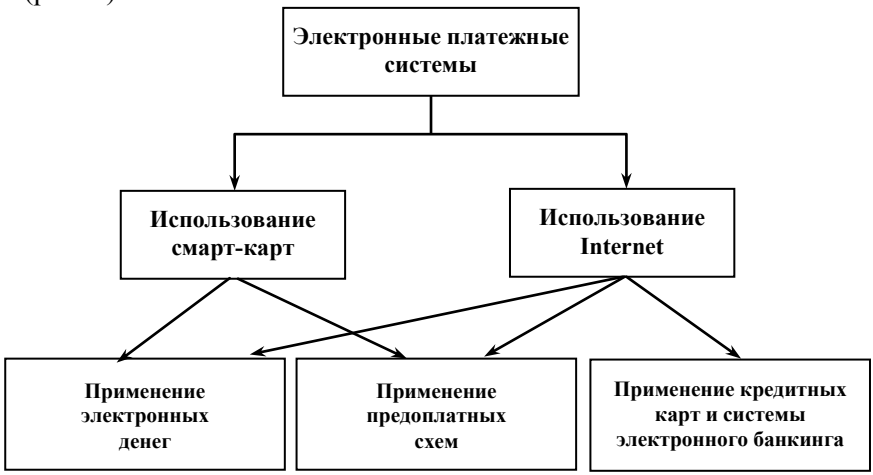


Рис. 8. Классификация платежных систем

Примером платежной схемы, построенной на основе понятий «электронные деньги» и «интеллектуальные карты» («смарт-карты»), является платежная система Mondex. Система Mondex – это система электронных наличных. Она использует смарт-карты и электронные деньги как форму представления денежных средств, хранящихся на смарт-картах. Электронные наличные могут быть загружены на смарт-карту через компьютер, соединенный с Internet, или через специальные устройства (в качестве таких устройств могут выступать банковские или телефонные аппараты). Карта может использоваться как для платежей в Internet, так и через специальные автономные устройства.

На рис. 9 представлена архитектура платежной системы Mondex.

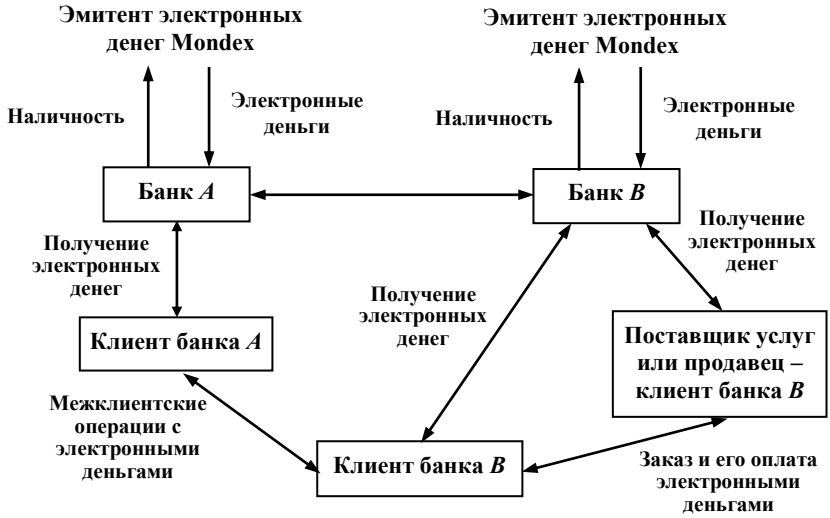


Рис.9. Архитектура платежной системы Mondex

В данной системе необходимо иметь организационный центр, обеспечивающий эмиссию электронных денег в валюте страны. Такой эмитент осуществляет функцию распространителя, снабжающего банки соответствующими электронными суммами в обмен на оборотные средства, имеющие себестоимость, или наличность.

Расчеты в системе Mondex производятся не по предоплатным схемам, а электронными эквивалентами наличных денег. Организационная структура данной системы может изменяться в зависимости от ее распространения.

Платежная система DigiCash является примером технологического решения для платежной системы цифровых денег (e-cash). Эта система демонстрирует все преимущества финансового обмена, совершаемого в электронной форме. Система основана на использовании электронных денег, передаваемых на рабочие станции пользователей–клиентов через Internet.

Организационная структура системы (рис. 10) предполагает, что все ее пользователи–клиенты должны быть зарегистрированы в Mark Twain Bank, осуществляющем ее обслуживание.

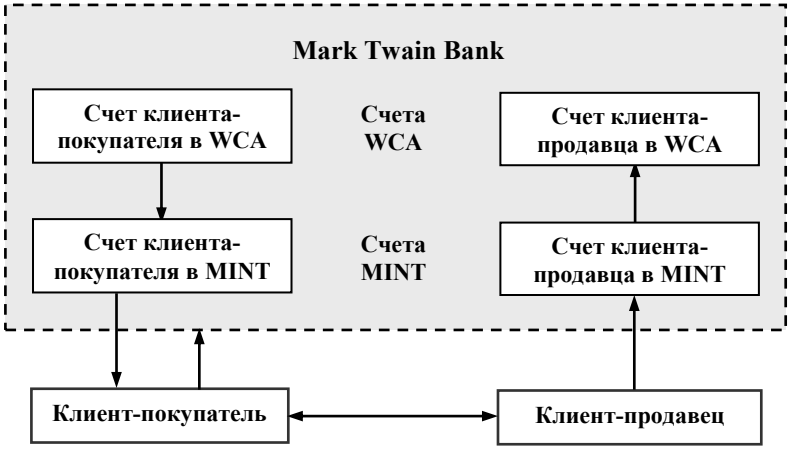


Рис.10. Архитектура платежной системы DigiCash

В системе предполагается использование двух типов счетов пользователей: WCA – счета для «реальных» денег и MINT – счета для электронных денег. Конвертация денег происходит путем их перевода со счета одного типа на счет другого типа.

В системе используются именно электронные деньги, а не данные предоплаты (как и в Mondex). Выпускаемые в данной системе электронные деньги (в отличие от системы Mondex) являются неразменными, что ограничивает ее возможности.

Как с использованием смарт-карт, так и с использованием Internet можно реализовать платежные системы на основе предоплатных схем. В подобных системах с использованием смарт-карт свободного обращения денежных средств между клиентами банков не происходит: каждая сделка должна быть зафиксирована в том или ином операционном центре финансового учреждения, обслуживающего данные системы оплаты. Такие системы являются по существу формами безналичных расчетов. Смарт-карта хранит данные о денежных суммах, которые загружаются на карты, списываясь со счетов клиента (или клиент кредитуется на указанную сумму). При осуществлении покупки или оплате услуги количество денежных средств, записанных на карте, уменьшается на величину требуемой суммы.

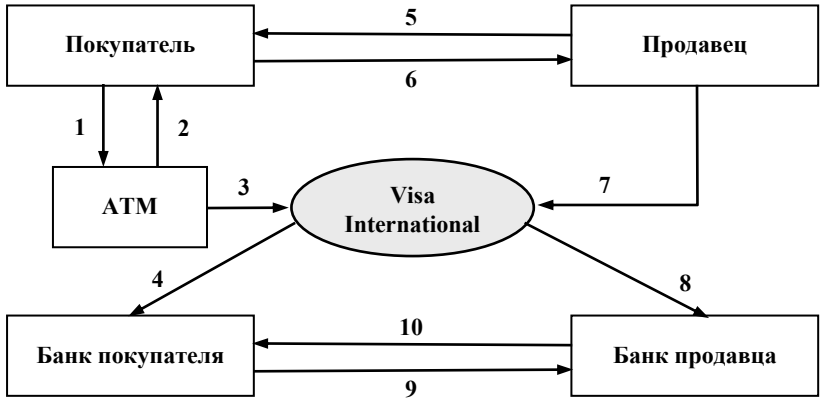


Рис.11. Архитектура платежной системы VisaCash

Примером подобной формы расчетов служит система VisaCash фирмы Visa International. Платеж в этой системе осуществляется по следующей схеме (рис. 11):

1. Использование кредитной карты покупателя для запроса данных об оплате.
2. Загрузка данных предоплаты на смарт-карту.
3. Передача информации об оплате в финансовую сеть Visa.

4. Поступление информации об оплате в банк покупателя и списывание с его счета необходимой суммы.
5. Поставка товара или оказание услуги.
6. Передача данных по оплате от покупателя к продавцу.
7. Передача предоплатных данных в финансовую сеть Visa.
8. Поступление данных в банк продавца.

9-10. Осуществление взаимозачета между банками покупателя и продавца, результатом которого является перевод денежных средств на счет продавца.

В среде Internet также могут быть реализованы предоплатные схемы. Примером такой системы является CyberCash, предлагающая интерактивную систему оплаты счетов. По своим функциональным возможностям она сходна с системой VisaCash. CyberCash предлагает платежные решения для кредитных карт, микроплатежей (CyberCoin Service) и интерактивную систему оплаты счетов (Interactive Billing).

CyberCoin предназначена для осуществления мелких платежей (включая оплату разменной монеты через Internet). В начале операции покупатель должен открыть счет CyberCash Account и перевести на него деньги со своего сберегательного счета (на этом счете деньги уже будут представлены как электронные деньги CyberCoin). Доступ к электронным деньгам открывается с помощью ПО CyberCash Consumer Wallet, деньги передаются на рабочую станцию пользователя через Internet.

Хотя в данной системе используются электронные деньги, расчеты фактически осуществляются переводом денежных средств со счета покупателя на счет продавца с применением банковской сети и предоплаты электронных денег путем резервирования денежных средств на счете клиента. Операции в CyberCoin не требуют открытия дополнительных специализированных счетов в других банках, так как выполняются через существующие банковские сети, что и отличает эту систему от DigiCash.

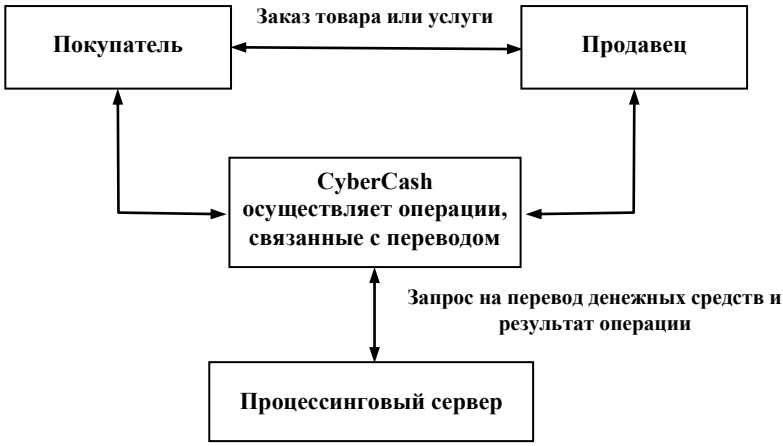


Рис.12. Архитектура платежной системы CyberCash

Покупка и оплата товара в данной системе (предварительно должна быть приобретена кредитная карта) осуществляется по следующей схеме (рис. 12):

1. Выбор предлагаемых на Web-сайте продавца товаров или услуг и активизация ПО CyberCash (с помощью специальной кнопки «Pay» («Оплатить»), доступной при работе с ПО электронного магазина).
2. ПО CyberCash осуществляет обработку и передачу электронных денег (если данное ПО недоступно покупателю, предлагается загрузить его из Internet):
   - шифрование финансовой информации, ее подпись и пересылка продавцу;
   - продавец проверяет целостность переданной информации, но при этом расшифровка информации, содержащей данные о кредитной карте покупателя, не осуществляется;
   - передача данных на сервер CyberCash с подписью продавца;
   - производятся необходимые проверки и в случае успешного их выполнения осуществляется расшифровка данных о кредитной карте покупателя;

- информация о кредитной карте покупателя отправляется на сервер процессинговой компании, обслуживающей данный тип кредитных карт;
- завершающие проверки данных процессинговым сервером (проверка номера кредитной карты, наличия на счете покупателя запрошенной суммы и т.д.);
- если результаты произведенных проверок оказались положительными, производятся переводы денежных средств со счета покупателя на счет поставщика и продавец информируется об успешном проведении платежа.

Перед владельцами банковских счетов и кредитных карт стоит проблема оперативного управления своими счетами. Существуют отечественные системы удаленного банковского обслуживания клиентов. Одна из таких систем – система, обладающая широким набором функциональных возможностей (сведения о движении денежных средств по счетам, о курсах валют, об управлении финансами и др.) и высоким уровнем обеспечения информационной безопасности, – Decart Home Bank (совместный проект компаний «АйТи», «Арсенал» и МО ПНИЭИ). Система позволяет проводить банковские операции с использованием Internet.

Система Decart Home Bank состоит из клиентской части (на рабочей станции клиента, подключенной к Internet, устанавливается ПО «Декарт») и банковской части (рис. 13).

Банковская часть выполняет следующие функции:

- регистрация пользователей системы – клиентов банка;
- обработка запросов зарегистрированных пользователей (клиентов банка);
- организация доступа к данным по счетам клиентов, хранящимся в банковской системе, и формирование данных для передачи по запросам клиентов (выписки по счетам клиентов, курсы валют, текущие условия обслуживания, текущее состояние счета и информация о подписках, уже оформленных клиентом и всех, предоставляемых банком);

- рассылка информации клиентам об операциях по их счетам;
- организация взаимодействия с клиентами через Internet;
- ведение журнала безопасности;
- обеспечение диагностики и возможности администрирования системы.

Клиентская часть системы предназначена для

- ведения финансов,
- планирования бюджета,
- выполнения операций с пластиковыми картами,
- персонального учета расходов,
- проведения анализа банковских операций.

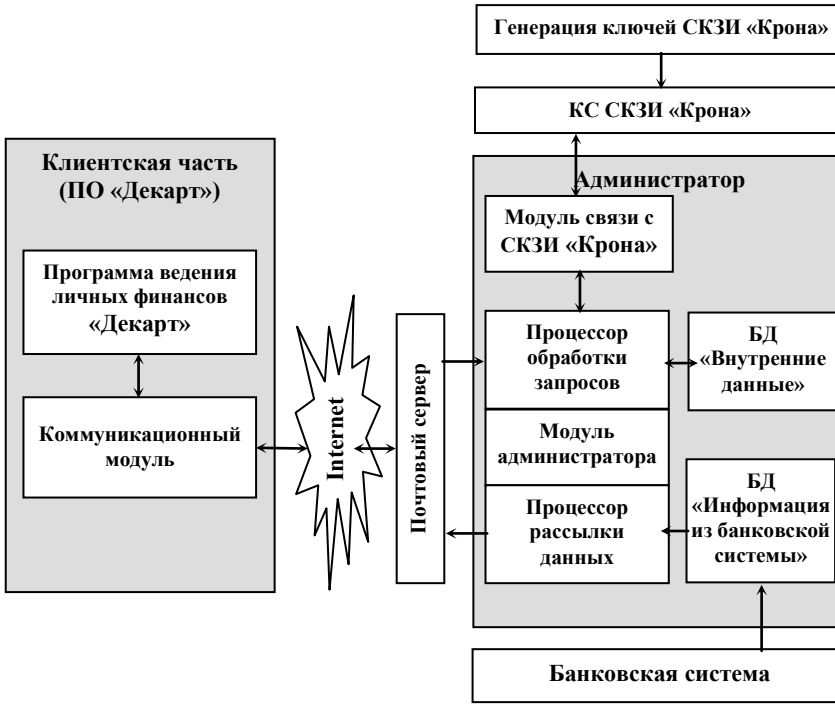


Рис.13. Архитектура системы Decart Home Bank

Схема работы системы включает следующие шаги, выполняемые клиентом и программным обеспечением (ПО) системы:

1. Запуск ПО «Декарт» и ввод пароля клиента (это ограничивает доступ к информации).
2. Вызов коммуникационного модуля, осуществляющего связь с банком, и выбор одной из следующих операций: получение информации от банка, изменение условий подписки на автоматическую рассылку информации или выполнение специального запроса.
3. Модуль связи шифрует запрос, связывается с почтовым сервером банка и передает запрос (криптографический ключ пользователь получает при регистрации в качестве клиента банка).
4. Передача зашифрованного запроса пользователя в процессор обработки запросов, установленный в банке, и расшифровка запроса (при этом проверяется целостность сообщения и право пользователя на получение запрашиваемой информации).
5. Обработка запроса и подготовка ответа.
6. Передача ответа на запрос процессору рассылки информации, который зашифровывает его для соответствующего абонента и передает на почтовый сервер, откуда его сможет получить клиент в удобное для него время.
7. Коммуникационный модуль клиента соединяется с сервером банка и проверяет наличие информации для клиента. При обнаружении нужной информации модуль связи снимает ее с сервера, расшифровывает ее, проверяя целостность и истинность отправителя.
8. Информация передается от коммуникационного модуля ПО «Декарт», где она представляется в удобном для пользователя виде. Нужная информация автоматически вводится в БД ПО «Декарт».

Программа «Декарт» ориентирована на пользователя, не имеющего специальных знаний в области бухгалтерского учета и финансов. Она позволяет вести любое количество счетов, операции по каждому из которых заносятся в отдельную таблицу.

Подсистема безопасности системы Decart Home Bank создана на основе отечественных средств криптографической защиты информации (СКЗИ «Крона»).

Алгоритм работы системы CyperPos приведен на рис. 14. Держатель пластиковой карты: Visa, EuroCard/MasterCard, Diners Club, JCB, American Express, Union Card (далее - Покупатель) может оплачивать покупки в Internet-магазинах, зарегистрированных на авторизационном сервере.

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

Магазин формирует заказ и переадресует Покупателя на авторизационный сервер CyberPOS.

Все информационное взаимодействие между Магазином и CyberPOS происходит по защищенному протоколу SSL и заверяется ЭЦП сторон.

Рис. 14. Алгоритм работы системы CyberPOS

CyberPOS устанавливает с Покупателем соединение по защищенному протоколу (SSL) и принимает от Покупателя параметры его кредитной карточки. Информация о карточке передается в защищенном виде только в CyberPOS и не предоставляется Магазину при операциях Покупателя.

CyberPOS проверяет наличие Магазина в Системе, контролирует соответствие операции установленным системным ограничениям. По результатам проверок формируется запрет или разрешение проведения авторизации транзакции в карточную платежную систему.

При запрете авторизации:

- CyberPOS передает Покупателю отказ с описанием причины,
- CyberPOS передает Магазину отказ с номером заказа.

При разрешении авторизации:

- CyberPOS передает ее в процессинговый центр Банка.

Запрос на авторизацию передается через закрытые банковские сети банку-эмитенту карточки Покупателя или процессинговому центру карточной платежной системы, уполномоченному банком-эмитентом.

При положительном результате авторизации, полученном от карточной платежной системы выполняются следующие шаги:

- Процессинговый центр Банка передает CyberPOS положительный результат авторизации;
- CyberPOS передает Покупателю положительный результат авторизации;
- CyberPOS передает Магазину положительный результат авторизации с номером заказа;
- Магазин оказывает услугу (отпускает товар);
- Банк зачисляет средства на счет Магазина в соответствии с существующими договорными отношениями между Банком и Магазином.

При отказе в авторизации:

- Процессинговый центр Банка передает авторизационному серверу отказ от проведения платежа;

– CyberPOS передает Покупателю отказ с описанием причины;
– CyberPOS передает Магазину отказ с номером заказа.

Вопросы для самопроверки

1. Определите понятие платежной системы.
2. Назовите известные Вам инструментальные средства, применяемые в электронных банковских системах.
3. Какие виды банковских карт Вы знаете? Какие технологии используются при их создании?
4. Что такое «электронные деньги»?
5. Приведите классификацию платежных систем.
6. Назовите примеры платежных систем различных типов. Охарактеризуйте их.
7. Охарактеризуйте особенности архитектуры и возможности каждой известной Вам платежной системы. Покажите схемы их функционирования.

Практические задания

1. Найдите в Internet информацию о платежных системах, используемых в настоящее время в системах розничной торговли и оказания услуг через Internet.
2. Сравните возможности существующих платежных систем.

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Как и любая информационная система, система электронной коммерции должна быть надежно защищена. Более того, к уровню защиты информации в системах электронной коммерции предъявляются повышенные требования, что связано с высокой степенью опасности попыток вторжений, обусловленной материальными интересами злоумышленников.

Система защиты должна быть комплексной, обеспеченной как правовыми средствами защиты и организационными мероприятиями, так и программно-аппаратными средствами. В данном пособии рассматриваются только специфические средства защиты, применяемые в системах электронной коммерции различного назначения.

Проблемы безопасности электронного бизнеса

Безопасность любой системы электронной коммерции в целом заключается в защите от различного рода вмешательств в ее данные. Все эти вмешательства (угрозы) можно разделить на несколько категорий:

- хищение данных;
- вмешательство в работу системы;
- искажение данных;
- разрушение данных;
- отказ от произведенных действий;
- неумышленное неправильное использование средств системы добросовестным пользователем;
- несанкционированный доступ к информации:
  - несанкционированное копирование, обновление или другое использование данных;
  - несанкционированные транзакции;
  - несанкционированный просмотр или передача данных.

Защита от вышеприведенных действий осложняется как правовыми факторами:

- технологии развиваются значительно быстрее законодательной базы;

– злоумышленника трудно поймать на месте преступления, а доказательства и следы преступлений легко могут быть бесследно уничтожены;

так и техническими:

– системы электронного бизнеса построены на базе множества готовых и сделанных на заказ программных приложений различных поставщиков и значительного количества внешних сервисов, предоставляемых провайдерами соответствующих услуг, в результате чего невозможно гарантировать полную совместимость и безопасность всей системы;
– каждый из отдельных компонентов системы может содержать дефекты защиты. Еще сложнее эти дефекты устранить, так как зачастую эти компоненты не прозрачны для IT-специалистов компании-заказчика.

Методологические рекомендации по обеспечению безопасности систем электронной коммерции

В проблеме защиты от внутренних угроз есть два аспекта: технический и организационный.

Технический аспект заключается в стремлении исключить любую вероятность несанкционированного доступа к информации. Для этого применяются такие известные средства, как:

– поддержка паролей и их регулярное изменение;
– предоставление минимума прав, необходимых для администрирования системы;
– наличие стандартных процедур своевременного изменения группы доступа при кадровых изменениях или немедленного уничтожения доступа при увольнении сотрудника.

Организационный аспект состоит в разработке рациональной политики внутренней защиты, превращающей в рутинные операции такие редко используемые компаниями способы защиты и предотвращения хакерских атак, как:

– введение общей культуры соблюдения безопасности в компании;

- тестирование программного обеспечения на предмет потенциальной уязвимости;
- отслеживание каждой попытки взлома (независимо от того, насколько успешно она завершилась) и ее тщательное исследование;
- ежегодные тренинги для персонала по вопросам безопасности и киберпреступности, включающие информацию о конкретных признаках хакерских атак, для того чтобы максимально расширить круг сотрудников, имеющих возможность выявить такие действия;
- введение четких процедур отработки случаев неумышленного изменения или разрушения информации.

Для защиты от внешнего вторжения сегодня существует множество систем, по сути являющихся разного рода фильтрами, помогающими выявить попытки взлома на ранних этапах и по возможности не допустить злоумышленника в систему через внешние сети. К таким средствам относятся:

- *маршрутизаторы* – устройства управления трафиком сети, расположенные между сетями второго порядка и управляющие входящим и исходящим трафиком присоединенных к нему сегментов сети;
- *брандмауэры* – средства изоляции частных сетей от сетей общего пользования, использующих программное обеспечение, отслеживающее и пресекающее внешние атаки на сайт с помощью определенного контроля типов запросов;
- *шлюзы приложений* – средства, с помощью которых администратор сети реализует политику защиты, которой руководствуются маршрутизаторы, осуществляющие пакетную фильтрацию;
- *системы отслеживания вторжений* (*Intrusion Detection Systems*, IDS) – системы, выявляющие умышленные атаки и неумышленное неправильное использование системных ресурсов пользователями;
- *средства оценки защищенности* (специальные сканеры и др.) – программы, регулярно сканирующие сеть на предмет наличия проблем и тестирующие эффективность реализованной политики безопасности.

Криптографические средства защиты информации

Шифрование – это наиболее широко используемый механизм защиты информации в вычислительных системах. Далее рассматриваются основные сведения о криптографических средствах защиты информации и их использовании в электронном бизнесе. Далее приведены основные понятия, используемые при описании средств защиты, в частности, криптографической защиты в системах e-commerce.

Основные понятия

Криптография («тайнопись») учит, как сохранить информацию в тайне, обозначает защиту информации с помощью шифрования. *Шифрование* – это преобразование «открытого текста» с целью сделать непонятным его смысл. В результате преобразования получается шифротекст. Процесс обратного преобразования – расшифровка (расшифрование, дешифрация) – восстановление исходного текста из шифротекста.

Шифрование используется для обеспечения защиты паролей, применяемых для аутентификации пользователей, защиты системной информации, а также информации, передаваемой по линиям связи, защиты данных в файлах и базах данных и т.д.

Криптографический алгоритм (*шифр* или *алгоритм шифрования*) – это математические функции, используемые для шифрования и расшифрования (используется две функции: одна – для шифрования, другая – для расшифрования).

В современной криптографии надежность криптографического алгоритма обеспечивается с помощью использования *ключей*. Зашифрованный текст всегда можно восстановить (расшифровать) в исходном виде, зная соответствующий ключ. Некоторые алгоритмы шифрования используют различные ключи для шифрования и расшифрования.

Под *криптосистемой* понимается алгоритм шифрования, а также множество всевозможных ключей, открытых и шифрованных текстов.

В общем случае порядок работы системы обмена сообщениями, секретность информации в которой обеспечивается с помощью шифрования, можно представить схемой, показанной на рис. 15.

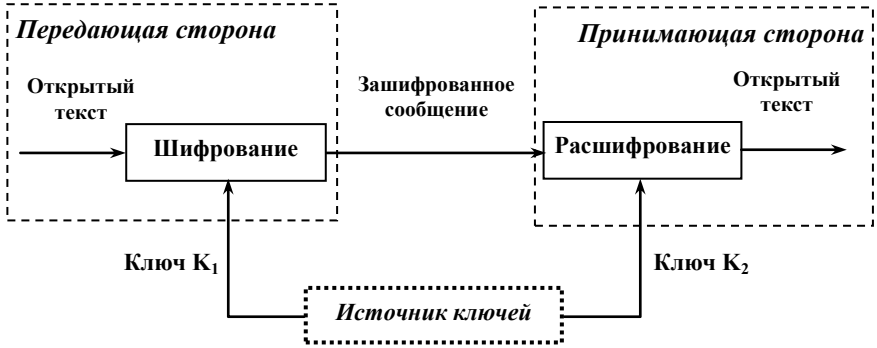


Рис. 15. Общая структура системы засекреченной связи

Существует две разновидности алгоритмов шифрования с использованием различных типов ключей: криптосистемы с открытым ключом и симметричные криптосистемы.

Симметричным называют криптографический алгоритм, в котором ключ, используемый для шифрования сообщения, может быть получен из ключа расшифрования и наоборот. В большинстве симметричных систем используется всего один ключ, который должен храниться в секрете. Такие алгоритмы называют одноключевыми, или алгоритмами *с секретным ключом*.

Алгоритмы шифрования с *открытым ключом* называют еще *асимметричными* алгоритмами шифрования. Они устроены так, что ключ, используемый для шифрования, отличается от ключа, применяемого для расшифровки сообщения, и ключ расшифрования не может быть за приемлемое время вычислен через ключ шифрования. Поэтому ключ шифрования не требуется держать в тайне и его называют *открытым*. Ключ же расшифрования является *тайным*, или *секретным*.

Симметричную криптосистему можно сравнить с сейфом, а ключ – с комбинацией, позволяющей открыть сейф каждому, кто

эту комбинацию знает. Алгоритм шифрования с открытым ключом можно сравнить с почтовым ящиком: в него просто опустить почту (зашифровать сообщение с помощью открытого ключа), но сложно сообщение извлечь – это может сделать только человек, имеющий специальный ключ (расшифровать сообщение может только тот, кто знает соответствующий тайный ключ).

Криптография ставит своей целью сохранение переписки в тайне от посторонних людей, которые захотели бы с ней ознакомиться. *Криптоанализ* же преследует цель получения доступа к тексту шифрованного сообщения в его исходном, незашифрованном (открытом) виде. Попытки криптоанализа называются *атаками*. Успешная криптоатака завершается взломом или вскрытием, в результате чего злоумышленникам становится известен не только текст зашифрованного сообщения, но и, зачастую, сами ключи, используемые для шифрования.

Наиболее известными компьютерными алгоритмами шифрования являются следующие алгоритмы:

- DES (Data Encryption Standard) – симметричный алгоритм шифрования, являющийся государственным стандартом в США. (В настоящее время разрабатывается новый стандарт AES – Advanced Encryption Standard.)
- RSA (Rivest, Shamir, Adleman) – алгоритм шифрования с открытым ключом, названный по первым буквам фамилий его создателей.
- ГОСТ 28147-89 – симметричный алгоритм шифрования, одобренный в СССР (и в России) для использования в качестве государственного стандарта.

Криптографические алгоритмы на практике в зависимости от области применения имеют несколько типов реализации: программную, аппаратную и программно-аппаратную.

Аппаратная реализация подразумевает, что алгоритмы шифрования реализуются в виде отдельных устройств. Такие устройства могут применяться для шифрования информации в различных системах передачи информации (телефон, радиосвязь и т.д.). Аппаратная реализация обладает лучшими скоростными

качествами, большей защищенностью от внешних воздействий, обеспечивает удобство эксплуатации.

Программная реализация является более гибкой, обеспечивает переносимость (программу можно модифицировать и настроить быстрее и с меньшими затратами). Недостатком программной реализации можно считать возможность вмешательства в действие алгоритмов шифрования, получения доступа к секретной ключевой информации, хранящейся в памяти компьютера.

Криптографические протоколы

Порядок работы систем, в которых используется криптографическая защита, определяется специальными протоколами.

В общем случае *протокол* – это совокупность правил, определяющих процедуру взаимодействия, т.е. последовательность шагов, которые предпринимаются двумя или большим количеством сторон для совместного решения какой-либо задачи. Все действия, заданные протоколом, выполняются в порядке строгой очередности, ни один шаг не должен быть пропущен, не может быть выполнен прежде, чем закончился предыдущий. Следовательно, каждый участник взаимодействия, направленного на решение некоторой задачи, заранее должен знать, какие шаги должны быть выполнены, и следовать предписанным правилам взаимодействия. Протокол допускает только однозначное толкование, он содержит описание реакции его участников на любые ситуации, возникающие в ходе взаимодействия.

Криптографическим протоколом называется протокол, в основе которого лежит криптографический алгоритм. Участники взаимодействия на основе криптографических протоколов используют их для совместной подписи договора или удостоверения личностей, например. В этих случаях криптография нужна, чтобы предотвратить или обнаружить вмешательство посторонних лиц, не являющихся участниками взаимодействия, не допустить мошенничество. Криптографический протокол гарантирует, что стороны, участвующие в решении определенной задачи, не могут сделать или узнать больше того, что определено соответствующим протоколом.

В *двусторонних* протоколах принимают участие два лица, две стороны, одна из которых начинает взаимодействие (т.е. выполнение шагов, предусмотренных протоколом), являясь его инициатором, а вторая осуществляет ответные действия.

Арбитр – это участник взаимодействия, которому в соответствии с протоколом полностью доверяют другие участники (т.е. доверенное лицо). Если протокол предусматривает участие во взаимодействии арбитра, он называется *протоколом с арбитражем*.

Реализация протоколов с арбитражем требует дополнительных накладных расходов на реализацию взаимодействия, поэтому для снижения расходов на арбитраж протокол, в котором участвует арбитр, делят на две части: первая часть полностью совпадает с обычным протоколом без арбитража, а вторая используется только тогда, когда между участниками возникают разногласия – для разрешения конфликтов используется особый арбитр – *судья*. Как и всякий арбитр, судья является незаинтересованным участником взаимодействия, которому все участники доверяют.

В компьютерных протоколах с судейством предусматривается наличие данных, на основании которых доверенное лицо может решить, не смошенничал ли кто-либо из участников взаимодействия. Хороший протокол позволяет определить, кто именно вел себя нечестно.

Самоутверждающийся протокол не требует присутствия арбитра для завершения каждого шага протокола или судьи для разрешения конфликта. Такие протоколы организованы так, что если один из участников взаимодействия мошенничает, то другие смогут распознать проявленную нечестность и прекратить выполнение дальнейших шагов.

На практике для каждого случая разрабатывается собственный протокол.

Атаки на протоколы бывают направлены против криптографических алгоритмов, которые в них используются, криптографических методов и самих протоколов.

При реализации пассивной атаки злоумышленник может подслушать информацию и использовать ее во вред взаимодействующим сторонам.

Активная атака на протокол предусматривает внесение злоумышленником изменений в сообщения, которыми обмениваются участники взаимодействия, или подмену информации, которая используется участниками взаимодействия для принятия решений.

Нечестно вести себя может и легальный пользователь информационной системы. Такого пользователя называют мошенником. Пассивный мошенник следует всем правилам, предписанным протоколом, но при этом еще и пытается узнать о других участниках взаимодействия больше, чем предусмотрено этим протоколом. Активный мошенник вносит изменения в протокол. Мошенничество направлено на извлечение нечестным путем наибольшей выгоды.

Чтобы избежать вторжений извне при передаче информации по не защищенному от подслушивания каналу связи, необходимо использовать шифрование. В простейшем случае последовательность действий, определяемая протоколом обмена сообщениями с использованием симметричного шифрования, показана на рис. 16.

Если злоумышленник имеет возможность перехватывать сообщения, которые передаются взаимодействующими сторонами, он может попытаться прочесть их, поэтому необходимо позаботиться о стойкости криптосистемы.

Кроме того, злоумышленники могут прервать взаимодействие, подменить сообщение.

Взаимодействующие стороны также могут навредить друг другу, отказавшись от обмена сообщениями или передав копии ключей третьему лицу. Поэтому такой протокол требует полного доверия сторон.

Симметричную криптосистему можно сравнить с сейфом, а ключ – с комбинацией, позволяющей открыть сейф каждому, кто эту комбинацию знает.

Рис. 16. Протокол обмена сообщениями с использованием симметричного шифрования

Алгоритм шифрования с открытым ключом можно сравнить с почтовым ящиком: в него просто опустить почту (зашифровать сообщение с помощью открытого ключа), но сложно сообщение извлечь – это может сделать только человек, имеющий специальный ключ (расшифровать сообщение может только тот, кто знает соответствующий тайный ключ). Порядок действий, определяемый протоколом шифрования с открытым ключом, показан на рис. 17.

Рис. 17. Протокол обмена сообщениями с использованием шифрования с открытым ключом

Применение систем с открытым ключом позволяет решить проблему передачи ключей. Для упрощения процедуры взаимодействия с использованием открытых ключей все открытые ключи абонентов системы можно поместить в базу данных, находящуюся в их общем пользовании.

На практике системы шифрования с открытым ключом используются для шифрования не сообщений, а ключей при их передаче по сети.

В криптографии распространенным приемом повышения надежности протоколов обмена информацией является шифрование каждого передаваемого сообщения с помощью отдельного ключа. Такой ключ называется *сеансовым*, так как используется только в течение одного сеанса связи. Секретные сеансовые ключи могут передаваться участникам взаимодействия доверенным лицом, наделенным правами арбитра. Для организации такого сеанса обмена сообщениями может быть использован протокол, последовательность действий для которого показана на рис. 18.

Рис. 18. Протокол с обменом ключами для симметричных криптосистем

При использовании этого протокола взаимодействующие пользователи целиком полагаются на честность доверенного лица (арбитра). Если арбитр поведет себя нечестно (злоумышленнику удастся его обмануть или подкупить), то ни о какой секретности отмена информацией не может быть и речи.

Кроме того, если доверенное лицо не сможет вовремя снабдить пользователей ключами для проведения сеанса взаимодействия, связь не состоится.

Для криптосистем с открытым ключом сеансовый ключ может генерироваться инициатором взаимодействия и шифроваться при пересылке с помощью открытого ключа получателя сообщения.

При обмене ключами злоумышленник может перехватывать передаваемые ключи и подменять их своими, выдавая себя за участников взаимодействия. При этом все сообщения, которые он перехватывает, могут быть расшифрованы, так как злоумышленник подменил ключи.

Для криптосистем с открытым ключом сеансовый ключ может генерироваться инициатором взаимодействия и шифроваться при пересылке с помощью открытого ключа получателя сообщения.

При обмене ключами злоумышленник может перехватывать передаваемые ключи и подменять их своими, выдавая себя за участников взаимодействия. При этом все сообщения, которые он перехватывает, могут быть расшифрованы, так как злоумышленник подменил ключи.

Атаки при обмене информацией по сети можно попробовать отразить с помощью цифровых подписей.

Криптографические протоколы, используемые в системах электронной коммерции

Электронные платежные системы, электронный документооборот и т.п. требуют использования специфических криптографических протоколов. К таким протоколам относятся следующие их виды:

- *безопасные выборы* – протокол, позволяющий решить проблему неотслеживаемости действий клиентов (клиент должен иметь возможность действовать анонимно, партнеры, конкуренты или банки не могут идентифицировать его действия);
- *совместная подпись контракта* – протокол, гарантирующий, что обе стороны подпишут контракт и не откажутся от подписей;
- *групповая подпись* – протокол, гарантирующий, что

только члены группы могут ставить подписи, причем получатель подписи может убедиться в ее правильности, но не может определить, кто именно из членов группы подписал документ, при споре подпись будет раскрыта;

- *доверенная подпись* – протокол, позволяющий передать полномочия подписания документа другому лицу;
- *неоспариваемая подпись* – протокол, гарантирующий, что получатель информации не сможет показать полученное сообщение третьей стороне без согласия лица, подписавшего сообщение;
- *слепая подпись* – протокол, гарантирующий, что лицо, подписывающее документ, не может ознакомиться с его содержанием, с помощью подписи можно только заверить факт и время отправки документа;
- *разделение знания секрета* – секретная информация разделяется на несколько частей, которые распределяются между группой лиц; каждая часть сама по себе не имеет смысла, сообщение полностью восстанавливается только при сложении всех частей.

Ведение электронного бизнеса требует использования средств криптографической защиты при оформлении документов и передаче сообщений. Конкретный тип протокола выбирается с учетом выполняемых в системе функций.

Вопросы для самопроверки

1. Определите понятие защищенной информационной системы.
2. Что такое криптография?
3. Определите понятие криптографического алгоритма.
4. Каково назначение ключей в системах шифрования?
5. Что понимается под криптосистемой?
6. В чем отличие систем с секретным и открытым ключом?
7. Дайте определение криптоанализа. Что такое атака?
8. Какие алгоритмы шифрования Вы знаете?
9. Сравните особенности аппаратной и программной реализации криптосистем.

10. Дайте определение протокола и криптографического протокола.
11. Чем различаются двусторонние протоколы и протоколы с арбитражем? Что такое самоутверждающийся протокол?
12. В чем отличие активных и пассивных атак?
13. Опишите протоколы с использованием симметричного шифрования.
14. Приведите общую схему протоколов с использованием открытых ключей.
15. Опишите схему протокола с обменом ключами.
16. Перечислите протоколы, используемые в системах электронной коммерции.

Практические задания

1. Разработайте презентации для демонстрации работы специфических криптографических протоколов электронной коммерции.

Электронно-цифровые подписи и открытые сделки

Для подтверждения подлинности документа люди издавна использовали личные подписи. Подписи служат доказательством того, что человек, подписавший документ, ознакомился с его содержанием и согласен с ним. Подпись вызывает доверие, так как ее сложно подделать и ее подлинность можно проверить. Подпись, стоящую под документом, нельзя использовать для того, чтобы заверить другой документ. Подписанный документ нельзя изменить. От подписи невозможно отказаться.

Таким образом, использование подписи должно гарантировать

- истинность письма, документа путем сличения подписи, стоящей под ним, с имеющимся образцом;
- авторство документа (с юридической точки зрения).

С переходом к безбумажным технологиям хранения и передачи информации, к электронному бизнесу (например, электронным переводам денежных средств, в основе которых лежат элек-

тронные аналоги бумажных платежных поручений) возникла проблема виртуального подтверждения аутентичности документов. Развитие подобных технологий требует существования электронных (электронно-цифровых, цифровых) подписей под электронными документами.

Для подтверждения подлинности файлов, электронных документов также можно использовать подписи. Но их использование сопряжено с большими трудностями: файл может быть скопирован вместе с подписью, после подписания в файл можно внести изменения. Поэтому подписание электронных документов требует реализации специальных протоколов.

Кроме того, применение цифровых подписей влечет целый ряд правовых проблем. Например, электронная подпись может применяться по договоренности внутри некоторой группы пользователей системы передачи информации, и в соответствии с этой договоренностью цифровая подпись в этой группе будет иметь юридическую силу. Но будет ли приниматься электронная подпись в качестве доказательства в суде, если это потребуется (например, при оспаривании факта передачи платежного поручения)?

Рассмотрим более подробно порядок использования цифровых подписей.

Предполагается, что при получении сообщения участник взаимодействия должен иметь возможность проверки его подлинности. Кроме того, часто возникают случаи, когда получатель информации должен доказать ее подлинность внешнему лицу. Чтобы иметь такую возможность, передаваемым сообщениям должны быть приписаны так называемые *цифровые сигнатуры* (электронные подписи).

Цифровая сигнатура (электронная, электронно-цифровая подпись) – это строка символов, зависящая как от идентификатора отправителя, так и от содержания сообщения. Никто (кроме самого отправителя информации) не может вычислить его цифровую подпись для конкретного передаваемого им сообщения. Никто (и даже сам отправитель!) не может изменить уже отправленного сообщения так, чтобы сигнатура (электронная подпись под сообщением) осталась неизменной. Получатель должен быть способен проверить, является ли электронно-цифровая подпись

(сигнатура), присвоенная сообщению, подлинной. В конфликтной ситуации внешнее лицо (арбитр, судья) должно быть способно проверить, действительно ли цифровая сигнатура, приписанная сообщению, выполнена его отправителем. Для верификации используется информация, предоставляемая арбитру отправителем и получателем.

Цифровые подписи могут быть реализованы на основе шифрования с секретными ключами (при симметричном шифровании), кроме того, допускается возможность подтверждения фактов передачи сообщений с помощью посредников, участвующих в процессе обмена информацией.

Классическим примером схемы электронно-цифровой подписи является алгоритм DSA (Digital Signature Algorithm), использованный как основа для опубликованного в 1991 г. в США стандарта на цифровые подписи DSS (Digital Signature Standard). Алгоритм DSA реализует схему на основе использования хэш-функций и асимметричного шифрования.

Отечественным стандартом на процедуры выработки и проверки электронно-цифровых подписей является ГОСТ Р 34.10-94. Схема, предложенная в данном стандарте, напоминает алгоритм DSA.

Используя цифровые подписи, можно организовать заключение сделок с использованием вычислительных сетей. Рассмотрим схему заключения сделок, в которой применяется модель цифровой сигнатуры на основе шифрования с открытым ключом.

В описании приведенной ниже схемы проведения сделки фигурные скобки {} определяют символьную строку (текст), составленную из содержащейся в этих скобках информации. Например: {ключ, номер} – строка символов, «склеенная» из символов, составляющих ключ, и символов в записи номера.

Банк, назовем его C, дает своему клиенту A чековую книжку, которая имеет следующим образом помеченные (пронумерованные) чеки:

ECF = {PKC, F({PCA, id(A), номер чека, время действия}, SKC)},

где:

PKC (Public Key of C) – открытый ключ банка C;

SKC (Secret Key of C) – соответствующий секретный ключ;

PKA (Public Key of A) – открытый ключ клиента A;

F – функция шифрования открытого ключа;
id(A) – идентификатор (идентификационный номер клиента A).

Чеки должны и могут быть выданы только банком C, так как только он знает секретный ключ SKC. При использовании открытого ключа банка при выдаче чека его можно в дальнейшем дешифровать или проверить права клиента A на использование чека.

Клиент A заполняет и подписывает чеки. Подписанный электронный чек представляется в виде

ECE = {PKA, F({ECF, id(B), номер сделки, размер, дата}, SKA)},

где:

B – получатель чека, предоставивший A услугу или товар;
SKA (Secret Key of A) – секретный ключ клиента A.

Протокол открытой сделки описывается схемой, которая включает семь фаз:

1. *Уведомление* (предложение) может быть передано от B в виде открытого текста.
2. *Запрос на сделку* должен подтверждать необходимость такой сделки для клиента A. Запрос представляет собой следующее сообщение, переданное от A к B:
   {PKA, F({запрос на сделку, вид изделия и т.п.}, SKA)}
3. *Сделка* (договор) оформляется так же, как и запрос.
4. *Разрешение* должно быть представлено банком C в связанной форме следующего вида:
   {PKC, F({ECF, id(B), номер сделки, размер=0, дата}, SKC)}
   Поскольку поле «размер» сделки равно 0, то подписанный чек нельзя использовать в виде реального чека, который будет оплачен банком.
5. Последующая *поставка* изделия может быть выполнена различными способами.
6. *Счет* оформляется так же, как и сделка, и посылается от B к A.
7. *Оплата* осуществляется с помощью подписанного электронного чека ECE, который передается от A к B.

В данной схеме используется модель цифровой сигнатуры, основанной на шифровании с открытыми ключами. В данном случае нет необходимости в посреднике, и только открытый

ключ получателя должен передаваться в защищенной форме перед фактическим обменом сообщениями.

Если ввести следующие обозначения:

M – сообщение, передаваемое отправителем S,

id(M) – приписанный ему идентификационный номер,

F – функция шифрования и

SKS – секретный ключ отправителя S,

то отправку подписанного сообщения от S к получателю R можно описать следующим образом:

1. S отправляет сообщение

   M' = {id(M), F({id(M), M}, SKS)}

   получателю R.
2. Получатель R дешифрует зашифрованную часть сообщения M' – строку F({id(M), M}, SKS), используя известный ему алгоритм шифрования и переданный ему заранее открытый ключ PKS отправителя S.
3. Если расшифрованный текст имеет смысл (он должен состоять из двух частей – id(M) и собственно сообщения M) и id(M) является верным (совпадает с id(M), переданным открытым текстом в M'), то сообщение M считается правильным, достоверным.

M' в данном случае может рассматриваться как цифровая сигнатура сообщения M.

В приведенной выше схеме открытой сделки отправителями поочередно выступают клиент банка A, банк C и сторона, предоставляющая за плату услугу или некоторое изделие (B). В сообщения включается вся необходимая для оформления сделки информация, которая шифруется с помощью секретных ключей. Открытые ключи передаются как часть сообщений. Идентифицирующая информация, которая может быть использована для проверки подлинности сообщения, также входит в сообщения.

Приведенная схема гарантирует достоверность полученной информации (зашифровать сообщение может только тот, кто владеет секретным ключом). Чтобы обеспечить секретность передаваемой информации, нужно открытые ключи, которые применяются для расшифровывания сообщений, передавать также в защищенной форме.

Вопросы для самопроверки

1. Дайте определение цифровой подписи.
2. Опишите схему действия протокола открытой сделки.

Вопросы для самопроверки

1. Разработайте распределенное приложение, реализующее протокол открытой сделки. Опишите его архитектуру и приведите обоснование использованных технологий. Разработайте руководство пользователей. Создайте презентацию, иллюстрирующую работу приложения.

Условия и ограничения использования криптографической защиты

Грамотно реализованная система криптографической защиты должна учитывать потребности и особенности поведения людей. К сожалению, пользователи готовы пожертвовать безопасностью, если средства ее обеспечения «мешают» им поскорее выполнить работу. Пользователей в первую очередь интересует простота и удобство использования программных продуктов, их совместимость с теми программами, с которыми они привыкли работать. Даже при использовании средств защиты пользователи зачастую выбирают пароли и ключи, которые проще запомнить, теряют ключевую информацию.

Таким образом, эффективность внедрения и использования криптографической защиты определяется реализацией комплекса организационных мероприятий.

Каждый владелец информации имеет право определять правила ее обработки и защиты. Базовым законом, определяющим права владельцев информации, является Закон Российской Федерации «Об информации, информатизации и защите информации», принятый 25 января 1995 г. В соответствии с ним любой российский гражданин имеет право на принятие мер по предотвращению утечки, хищения, утраты, искажения и подделки информации, но проблема состоит в том, как определить средства, обеспечивающие адекватную защиту, не противоречащие существующим ограничениям.

Следует помнить, что существуют законодательные ограничения на разработку, распространение и использование средств криптографической защиты.

В США они определяются специальным пунктом «Контроль за экспортом и импортом вооружений» в Своде законов. Программное обеспечение, предназначенное для целей эффективного шифрования данных, причисляется к военному снаряжению, поэтому его распространение строго лицензируется, а программные средства, легально экспортируемые за рубеж, обеспечивают лишь ослабленную криптографическую защиту.

В России также введены ограничения на экспорт, импорт и использование средств шифрования. При разработке криптографической системы она должна быть передана в ФАПСИ (Федеральное Агентство Правительственной Связи и Информации) для получения лицензии, дающей право на ее легальное использование на территории России. Единственным лицензированным ФАПСИ шифром в настоящий момент является ГОСТ 28147-89, разработанный еще в КГБ. Все остальные криптосистемы являются нелегальными. Распространению таких продуктов способствует нечеткость формулировки в президентском Указе № 334 термина «шифрование».

Кроме того, при разработке любой криптографической системы в ней обычно остаются «потайные ходы», которые обеспечивают контроль над шифруемой в этих системах информацией. Потайные ходы дают возможность спецслужбам, например, расшифровать информацию, не зная ключа пользователя.

Вопросы для самопроверки

1. Назовите условия и ограничения использования криптографических средств защиты в электронной коммерции в соответствии с действующим законодательством Российской Федерации. Перечислите документы, на основании которых подготовлен ответ.

ВВЕДЕНИЕ В МОБИЛЬНЫЙ БИЗНЕС

Одно из главных направлений современного этапа развития информационных и телекоммуникационных технологий – ориентация на поддержку *мобильных* пользователей, не привязанных к конкретным рабочим местам (компьютерам и вычислительным узлам). Информационные технологии разрабатываются с целью упрощения доступа и работы с информацией любого вида. Конечного пользователя не должны интересовать технические и организационные аспекты получения информации – он должен получать ее в удобном виде в приемлемое время и за приемлемую цену.

В ходе борьбы за конкурентное преимущество крупные корпорации (бизнес-системы) и любые другие достаточно сложно организованные структуры (в том числе и органы власти) вынуждены бороться за эффективность управления, взаимодействия своих структур, взаимодействия с партнерами и т.п. Для решения этой задачи необходимо оптимизировать процессы сбора, анализа, хранения и доставки актуальной оперативной информации.

Важный аспект развития современных корпоративных систем – работа с мобильными пользователями. В качестве такого пользователя может выступать руководитель предприятия, находящийся в поездках и оторванный от корпоративной сети и свежей новостной информации, необходимой для принятия обоснованных управленческих решений. Это может быть разъездной менеджер по продажам, которому необходимо постоянно обмениваться информацией с головным офисом фирмы.

В настоящее время происходит бурный рост в сфере мобильной коммерции и бизнеса. На рынке предлагаются различные услуги: начиная от мобильной торговли на биржевых рынках и услуг управления банковским счетом через мобильный телефон, заканчивая корпоративными системами, позволяющими пользователю в любое время в любом месте получать доступ к информационным ресурсам предприятия, включаться в его информационную среду.

Различные секторы рынка электронной коммерции получили широкое развитие благодаря возможности интегрировать раз-

личные источники данных и бизнес-процессы, делая их с помощью интегрированных Web-сайтов доступными потребителям, сотрудникам и партнерам.

Беспроводные технологии позволяют людям заниматься бизнесом, где бы они ни находились, в любое время. Уменьшение стоимости и возрастающая скорость работы беспроводных устройств стимулируют переход к их активному использованию. Начавшаяся конвергенция технологий позволит беспроводным устройствам выступать в качестве клиентов систем электронного бизнеса, которые таким образом превратятся в системы мобильного бизнеса.

Развитие мобильного бизнеса подразумевает реализацию следующих требований:

- обслуживание в любом месте (в офисе, дома, в дороге);
- использование любых сетей (проводных или беспроводных);
- использование любых устройств (телефонов, PDA, КПК и т.п.).

Указанные возможности становятся доступными в любой области (бизнес, досуг, образование). Вместе с тем, следует иметь в виду, что мобильный бизнес подразумевает не просто предоставление традиционных услуг электронного бизнеса через различные переносные устройства, но и реализацию принципиально новых сервисов (например, всевозможные уведомления и предупреждения, выдаваемые в зависимости от местонахождения клиента).

На рис. 19 приведены примеры некоторых возможностей приложений мобильного бизнеса.

Мобильный бизнес – это новый этап логического развития электронного бизнеса. Следовательно, для успешного применения новых технологий нужно учитывать опыт (в том числе и неудачный) реализации проектов электронной коммерции:

- Internet – это технология, помогающая более эффективно организовывать бизнес-процессы предприятия.
- Конкурентные преимущества обеспечивает не сам Internet, а успешная бизнес-стратегия предприятия, что, в частности, означает, что нельзя фокусироваться не на от-

дельно взятом процессе, необходима реорганизация всей деятельности предприятия на основе новых технологий.
- Решающее значение имеет предоставление именно тех Internet -услуг, которые приносят реальные преимущества (прибыль).
- Электронная коммерция невозможна без автоматизированных надлежащим образом и интегрированных бизнес-процессов, т.е. больший объем операций происходит за рамками видимой Web-страницы.
- Internet следует применять там, где это имеет смысл.

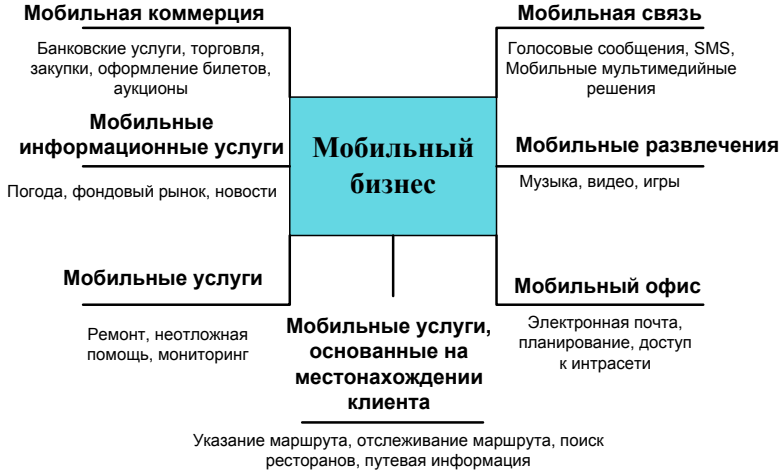


Рис.19. Примеры приложений мобильного бизнеса

Главная мотивация компаний в области продвижения мобильных приложений – это стремление сохранять конкурентоспособность в течение длительного времени и создавать источники новых доходов.

Рассмотрим два примера, демонстрирующих разные варианты эффекта от новой технологии. Первый – появление мобильных приложений само по себе вряд ли увеличит количество клиентов банка. Но банки, которые не будут иметь таких приложений, могут потерять своих клиентов завтра. Второй пример – открывающиеся новые возможности в области бизнеса могут при-

носить дополнительные доходы (это легко показать на примере услуг для путешествующих). Туристы будут готовы платить за услуги, которые постоянно «сопровождают» их во время поездки и оказывают помощь в соответствии с текущим местонахождением.

Возможности мобильной коммерции

Какие же возможности предлагает мобильная коммерция?

Одной из главных сильных сторон мобильной коммерции является персонализация, возможность выстраивания отношений с каждым отдельным клиентом. Предлагая брокерские услуги, компании в полной мере могут воспользоваться этими преимуществами. Специалисты аналитической компании IDC утверждают, что для обслуживающих частных инвесторов брокерских фирм предложение доступа к своим услугам через устройства мобильной связи является объективной необходимостью. В сфере инвестиций, по мнению аналитиков, мобильный Internet-доступ представляет основную ценность, скорее, как средство персонификации оказываемых клиенту услуг, нежели как средство привлечения новых клиентов и получения большой прибыли. В конечном итоге, беспроводные устройства могут стать основным каналом взаимоотношений с большей частью наиболее ценных для компании клиентов.

Особняком среди финансовых услуг стоят мобильные платежи. Они являются основой мобильной коммерции, и ситуация на этом рынке непосредственно зависит от степени их развития и распространения.

Удобство мобильных платежей – в сокращении времени на обслуживание клиента. Так, сеть ресторанов McDonald's, наибольшая привлекательность которых заключается именно в быстроте обслуживания, для уменьшения очередей приступила к тестированию систем беспроводной оплаты компаний Exxon Mobil и Freedom Pay. Комплект Speedpass – разработка компании Exxon Mobil, владеющей автозаправками, – состоит из электронного устройства, внешне очень напоминающего обычную шариковую ручку, и компактной системы считывания данных, заменяющей кассовый аппарат. Принцип действия заключается в том,

что в электронной «ручке» содержится вся информация о кредитных и дебетовых карточках владельца, откуда, после подтверждения оплаты в операционном центре, и переводятся деньги на счет заправки или McDonald's. Взаимодействие между «ручкой» и «кассой» происходит по инфракрасным портам. Достаточно только взмахнуть этой «волшебной палочкой» перед устройством для считывания данных, чтобы мгновенно получить свой оплаченный заказ.

Одним из направлений мобильных платежей является мобильная наличность. Однако разработки в этой области пока еще находятся на начальной стадии, поэтому сказать что-то определенное о будущем этого направления пока еще сложно, но многие аналитики считают его наиболее перспективным.

Не следует считать, что область применения мобильных устройств ограничивается сектором B2C. Корпоративный рынок является не менее важным сектором их использования. По данным IDC, в настоящее время корпоративный спрос на мобильные решения масштаба предприятия достиг достаточно высокого уровня. В отчете «Going Mobile: A Look at the End Users' Needs», составленном по результатам проведенного специалистами IDC опроса, аналитики приводят данные о том, что в настоящее время около 21% коммерческих предприятий в США самостоятельно внедряют у себя мобильные решения, а еще 56% намерены сделать это в ближайшем будущем. В Европе в процессе ввода в эксплуатацию мобильных решений масштаба предприятия находятся 35% компаний. Для поставщиков информационно-технологических услуг результаты опроса IDC представляются еще более обещающими: 75% компаний в Европе и 91% в США готовы внедрить у себя мобильные решения, пользуясь услугами сторонних поставщиков.

Одно из возможных применений мобильных приложений - это работа с клиентами, которая часто предполагает передачу данных в условиях, когда служащий находится вдали от офиса. Для того чтобы информация напрямую передавалась в информационную систему компании, чтобы сделать этот процесс простым и не зависящим от внешних условий, использование мобильных устройств подходит просто идеально. Так, компания Aviall Inc., дистрибутор авиационных запасных частей, постепенно разворачивает беспроводную SCM-систему (Supply Chain

Management) для инвентаризации запасов у своих потребителей. Потребность в точных и актуальных данных о состоянии запасов деталей подтолкнула Aviall, а также другие предприятия к тому, чтобы начать применение беспроводных устройств в сетях поставок. В настоящее время сотрудники отдела продаж Aviall должны при посещении потребителей определять количество необходимых деталей вручную, а затем каким-либо образом передавать эти данные в офис. С помощью же новой системы сотрудники Aviall смогут сканировать штриховой код на контейнере с деталями, а затем оперативно через Internet передавать информацию об остатках в центральную базу данных компании.

Еще один пример использования беспроводных технологий в снабжении демонстрирует компания Nicor Gas. Здесь мобильные устройства фирмы TS-Tek служат для того, чтобы гарантировать правильное выполнение определенных процедур сотрудниками. Рабочие применяют сканеры штрих-кодов для автоматизации создания заказов и подготовки необходимых документов для получения и отгрузки товара. Используемые устройства издают предупреждающий сигнал, если детали на складе идентифицированы неправильно или положены не в тот контейнер. Кроме того, сведения о перемещении товаров оперативно передаются в центральную базу данных, что гарантирует наличие актуальной и точной информации об уровне складских запасов. Если до применения беспроводных устройств всесторонняя инвентаризация занимала от трех до четырех рабочих дней, то теперь она делается за день.

Но есть приложения, в которых компании могут быть заинтересованы вне зависимости от вида своей деятельности. Это так называемый «мобильный офис». Фактически это набор тех основных приложений, которые в любой момент могут понадобиться деловому человеку и наличие которых позволяет полноценно продолжать работу и вне стен офиса. Для этого нужен мобильный телефон с доступом в Internet и карманный компьютер. Телефон в этой связке обеспечивает голосовой канал и подключение к Internet, а КПК (карманный персональный компьютер) позволяет работать со стандартными офисными приложениями, почтой, самим Internet, осуществлять прием и передачу факсовых сообщений.

Достоинства мобильного бизнеса

Среди наиболее важных достоинств мобильного бизнеса можно отметить следующие его характеристики:

- *Повсеместность*. Это самое очевидное преимущество мобильного устройства, позволяющего в режиме реального времени получать информацию и оставаться на связи независимо от местонахождения.
- *Достижимость*. Она важна для многих людей, которые желают постоянно оставаться «на связи».
- *Доступность*. Доступ к личным и деловым ресурсам обеспечивается любым устройством через любую сеть – кабельную или беспроводную.
- *Безопасность*. Обеспечение безопасности мобильных транзакций еще находится на стадии становления. Но более полное использование возможностей SIM-карты в будущем повысит уровень безопасности по сравнению с тем, что имеется в сегодняшних Internet-приложениях.
- *Удобство*. В мобильных устройствах хранятся личные данные, они всегда будут «под рукой», а использовать их становится все легче.
- *Локализация услуг и приложений*. Этот фактор также существенно повышает ценность мобильных устройств.
- *Мгновенное подключение к Internet* с мобильного телефона постепенно становится реальностью.
- *Персонализация*. Индивидуальные услуги доступны уже сегодня, хотя и в очень ограниченной степени.

Следующие факторы определяют возможности развития мобильного бизнеса:

- *Коммерческие факторы*. Бизнес нуждается в новых типах мобильных приложений, которые позволят уменьшить издержки в цепочке поставок товаров и услуг и одновременно удовлетворят потребность клиентов в обслуживании «везде и всегда».

- *Технические факторы*. Развитие технологий и снижение цен на мобильные устройства делают новые типы приложений экономически осуществимыми. Например, технологии, обеспечивающие точное определение местоположения абонента, откроют путь к внедрению новых типов приложений (например,

порталов поддержки торговли, находящих альтернативных поставщиков продуктов и услуг поблизости от покупателей).

– *Доступность*. Сотовой связью охвачено практически все экономически активное население. В результате открываются возможности для выполнения онлайновых транзакций, приложений электронной коммерции, в которой будет участвовать огромное число новых потребителей.

Вопросы для самопроверки

1. Определите понятие мобильного бизнеса.
2. Назовите примеры приложений мобильного бизнеса.
3. Перечислите преимущества использования мобильного бизнеса.
4. Назовите проблемы, вызванные развитием мобильного бизнеса.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. *Андреев А.А*. и др. Пластиковые карты. 3-е изд. / А.А. Андреев. М.: БДЦ-Пресс, 1999.
2. *Васкевич Д*. Стратегии клиент/сервер. Руководство по выживанию для специалистов по реорганизации бизнеса / Д. Васкевич. Киев: Диалектика, 1996.
3. *Вендров А.М*. Проектирование программного обеспечения экономических информационных систем: учебник /А.М. Вендров. М.: Финансы и статистика, 2000.
4. *Дубова Н*. Интегрированные системы управления распределенной корпорацией / Н. Дубова // Открытые системы. 1998. № 1. С. 69-75.
5. *Козье Д*. Электронная коммерция. Русская редакция / Д, Козье. М.: Издательский отдел «Русская редакция», 1999.
6. *Колесник А.П*. Компьютерные системы в управлении финансами / А.П. Колесник. М.: Финансы и статистика, 1994.
7. *Ойхман Е.Г., Попов Э.В*. Реинжиниринг бизнеса: реинжиниринг организаций и информационные технологии / Е.Г. Ойхман, Э.В. Попов. М.: Финансы и статистика, 1997.
8. *Пирогова Н*. Как создать виртуальную корпорацию? / Н. Пирогова // Открытые системы. 1998. № 1. С. 62-66.
9. *Петров А.А*. Компьютерная безопасность. Криптографические методы защиты / А.А. Петров. М.: ДМК, 2000.

Учебное издание

Юрков Кирилл Александрович

Лядова Людмила Николаевна

Хлызов Андрей Владимирович

Климов Григорий Валерьевич

Технологии создания систем электронной коммерции

Учебно-методическое пособие

Редактор *Н.И. Стрекаловская*

Корректор *А.В. Цветкова*

Подписано в печать 25.12.2007. Формат 60×84/16.

Усл. печ. л. 4,65. Уч.-изд. л. 4,5. Тираж 100 экз.

Заказ

Редакционно-издательский отдел Пермского государственного университета
614990. Пермь, ул. Букирева, 15

Типография Пермского государственного университета
614990. Пермь, ул. Букирева, 15