ПЕРМСКИЙ
ГОСУДАРСТВЕННЫЙ
НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ

О. Ю. Вологжанин, В. В. Ильин,
Л. С. Галкина

ЭЛЕКТРОННАЯ КОММЕРЦИЯ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное
образовательное учреждение высшего образования
«ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»

О. Ю. Вологжанин, В. В. Ильин, Л. С. Галкина

ЭЛЕКТРОННАЯ КОММЕРЦИЯ

Допущено методическим советом
Пермского государственного национального
исследовательского университета в качестве
учебного пособия для студентов, обучающихся
по направлению подготовки бакалавров
«Менеджмент»

Пермь 2024

УДК 339.376: 004.70(075.8)
ББК 65.290с51я73
В68

Вологжанин О. Ю.

В68 Электронная коммерция [Электронный ресурс] : учебное пособие / О. Ю. Вологжанин, В. В. Ильин, Л. С. Галкина ; Пермский государственный национальный исследовательский университет. – Электронные данные. – Пермь, 2024. – 2,40 Мб ; 198 с. – Режим доступа: http://www.psu.ru/files/docs/science/books/uchebnie-posobiya/elektronnaya-kommerciya.pdf. – Заглавие с экрана.

ISBN 978-5-7944-4095-9

В учебном пособии рассматриваются вопросы, связанные с функционированием рынка электронной коммерции в России и в мире. Издание адресовано обучающимся по направлениям «Экономика», «Менеджмент», «Торговое дело», слушателям курсов дополнительного профессионального образования, а также практикующим экономистам, финансовым аналитикам, осуществляющим специализированные виды профессиональной деятельности (коммерческую, торгово-технологическую, товароведческую).

УДК 339.376: 004.70(075.8)
ББК 65.290с51я73

Издается по решению ученого совета экономического факультета Пермского государственного национального исследовательского университета

Рецензенты: кафедра экономического анализа и статистики Пермского института (филиала) Российского экономического университета им. Г. В. Плеханова (зав. кафедрой, канд. экон. наук **О. И. Агеева**);

доцент отделения высшего образования Пермского филиала Волжского государственного университета водного транспорта, канд. техн. наук **А. Л. Погудин**.

ISBN 978-5-7944-4095-9

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Интернет как наиболее доступная и удобная система глобального обмена информацией между пользователями не только доказал свою жизнеспособность, но и начинает вытеснять иные способы и каналы коммуникаций, что происходит благодаря более низкой стоимости услуг, высокой скорости передачи данных, более широкому спектру представляемой и передаваемой информации.

Сегодня электронная коммерция позволяет бизнесменам сокращать расходы (например, такие как аренда помещений), значительно уменьшаются затраты на персонал, дополнительным преимуществом является освобождение от налоговых выплат, связанных с недвижимым имуществом, повышается конкурентоспособность, что не может не отразиться на повышении качества предоставляемых товаров и услуг. Электронная коммерция позволяет организации находить новые рынки сбыта, получать информацию о желаниях потребителей.

Электронной коммерцией могут заниматься не только крупные компании, здесь может начать свое дело обыкновенный человек, разбирающийся в механизмах ведения интернет-бизнеса.

Миллионы людей сейчас используют Интернет для заказа и оплаты товаров и услуг, при этом часто товары доставляются с другого конца света и оплачиваются с мобильных устройств.

Электронная коммерция – это копия привычного для нас рынка, только в сети Интернет. Интернет-маркетинг и связанные с ним сферы деятельности стали эффективным инструментом привлечения клиентов. Это новая среда распространения информации со своей спецификой.

Целью изучения дисциплины «Электронная коммерция» является формирование у студентов базовых знаний и представлений о стремительно развивающемся направлении – электронном бизнесе, развитие умений и навыков использования новых способов ведения коммерческой деятельности посредством информационных и телекоммуникационных технологий.

Данное пособие позволяет:

1. Изучить принципы информационного поиска информации в сети Интернет;

2. Подготовить студента к использованию в практической деятельности инструментария электронной коммерции;

3. Рассмотреть особенности работы на различных сегментах электронного рынка, продемонстрировать связь со смежными областями offline-коммерции;

4. Изучить основы практического использования электронных платежных систем;

5. Рассмотреть основы обеспечения безопасного функционирования систем электронной коммерции;

6. Выделить основные методы маркетинговых коммуникаций в сфере электронного бизнеса.

В результате изучения практических аспектов при помощи данного практикума студент должен

Знать:

• функциональные возможности интернет-магазинов, интернет-аукционов, интернет-бирж, электронные торговые ряды, витрины и каталоги для систем электронной коммерции;

• виды электронных платежей, используемых в Интернете, их возможности, преимущества и недостатки;

• основные законы, нормативно-правовые документы, федеральные и региональные целевые программы, касающиеся электронной коммерции.

Уметь:

• пользоваться поисковыми средствами Интернета;

• пользоваться информационными корпоративными порталами и корпоративными веб-сайтами для поиска потенциальных продавцов и покупателей при проведении коммерческих операций.

Владеть:

• методами и приемами работы с реально действующими интернет-магазинами и интернет-аукционами;

• простейшими методами оценки эффективности электронной коммерции на основе статистических данных.

1. ЭЛЕКТРОННАЯ КОММЕРЦИЯ В МИРОВОМ СООБЩЕСТВЕ

1.1. Основные этапы развития электронной коммерции

Мировая экономика приобретает все более виртуальный характер. Виртуальные банки, магазины, библиотеки, биржи – все это уже действительность дня. Интернет как наиболее яркое проявление новых информационных технологий стал сегодня символом нового мира, новых экономических решений.

Для изучения развития и возможностей электронной коммерции необходимо выполнить следующие задачи:

– дать понятие электронной коммерции;

– рассмотреть историю развития электронной коммерции;

– рассмотреть вопросы безопасности электронного бизнеса.

Предпосылкой для появления электронной коммерции стал переход США от индустриального к постиндустриальному этапу развития экономики, когда основным продуктом в экономике становится не товар, а услуга, а сам товар уже не рассматривается отдельно от организации его продажи и обслуживания. При этом подавляющее большинство принципиальных изменений электронный бизнес претерпел в последние двадцать лет, хотя начало электронной коммерции было положено еще в 1960 г. Именно тогда американские компании American Airlines и IBM приступили к разработке системы электронного бронирования авиабилетов, которая позволяла American Airlines оперативно управлять доходностью с помощью изменения цен на билеты с учетом наличия свободных мест.

Первым этапом развития электронной коммерции стало появление глобальной компьютерной сети Интернет. Начиная с начала 80-ых гг. XX в., сеть постоянно росла, увеличивая количество подключенных пользователей. За тридцатилетний период развития Интернета количество пользователей увеличилось от нескольких университетов и фирм, пересылающих электронную почту, до 1,966 млрд пользователей к 2010 г. Изначально Интернет использовался для передачи электронной почты, но, расширяясь, сеть приобретала все большие возможности пере-

дачи данных. Так, в 1994 г. был открыт первый Интернет-магазин. Это послужило началом развития электронной торговли (электронной коммерции) в мире. С этого момента крупный бизнес начал инвестировать средства в развитие электронной коммерции. Параллельно этому в октябре 1994 г. американский банк Stanford Federal Credit Union запустил первую в мире систему интернет-банкинга, позволяющую оплачивать счета за коммунальные услуги, Интернет, телефон, совершать платежи по кредитам и осуществлять переводы третьим лицам, не отходя от своего персонального компьютера. Появление интернет-магазинов и систем интернет-банкинга послужило переходом электронной коммерции к следующему этапу развития.

Вторым этапом развития электронной коммерции можно считать массовое дублицирование существующих в реальности хозяйствующих субъектов экономики (фирм, магазинов, торговых сетей, банков) в виртуальный мир. Основным процессом данного этапа развития является создание хозяйствующими субъектами электронных форм ведения бизнеса.

Электронная составляющая массово начинает появляться практически во всех крупных формах хозяйственной деятельности. Благодаря данному фактору и постоянному росту числа пользователей Интернета резко растет общий товарооборот электронной коммерции. За счет свободного доступа к технологии Интернет все новые и новые формы хозяйственной деятельности открывают свои online-представительства, получая тем самым дополнительный сбыт своей продукции, увеличивая при этом прибыль. Глобальное вовлечение новых форм хозяйственной деятельности в электронную коммерцию приводит к идеям создания уникальных технологий, работающих без физического присутствия. Появляются виртуальные банки, магазины, офисы. Все эти факторы послужили для перехода к третьему – современному – этапу развития электронной коммерции.

На данном этапе появляются виртуальные товары и электронные деньги. К виртуальным товарам относятся все виды товаров, которые не могут существовать вне виртуального мира. Это программное обеспечение, Интернет-сайты, компьютерные игры и т.д. Увеличение объемов продаж в электронной коммерции повлекло за собой появление электронных денег. Закон Рос-

сийской Федерации «О национальной платежной системе» содержит следующее определение электронных денежных средств: это денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа. Таким образом, электронная коммерция получила свою собственную, отличную от реальной экономики, денежную систему, что позволило резко ускорить темпы ее роста.

Виртуальные товары и электронные деньги являются уникальной особенностью электронной коммерции, поскольку они не могут существовать в реальной экономике. Они способны появляться только внутри виртуальной хозяйственной деятельности, тем самым создавая новую ступень для развития информационной экономики, внутри которой происходит глобальный переход от «движения атомов» к движению битов. Подтверждая мысль Николаса Негропонте, необходимо отметить, что полный переход от «движения атомов» к движению битов вряд ли полностью возможен. Ограничением может послужить физическая зависимость виртуального мира от компьютерной техники и средств телекоммуникации, так как именно они обеспечивают бесперебойную работу виртуального мира и электронной экономики.

1.2. Особенности развития электронной коммерции в России

В России электронная коммерция активно развивается с 1998 г. В 1999 г. Московская Межбанковская Валютная биржа начала прием электронных заявок на покупку и продажу валюты с помощью открытого мощного интернет-шлюза и электронный бизнес в России пополнился системой интернет-трейдинга. На сегодняшний день электронная коммерция – это многочислен-

ные интернет-магазины, системы электронных платежей, интернет-биржи, интернет-аукционы и прочее.

Рынок электронной коммерции в России развивается стремительными темпами, с каждым годом растет число покупателей, оценивших удобство покупок в интернете. Но, несмотря на радостную статистику, проблем в сфере электронной торговли достаточно много.

Особенности и сложности электронной коммерции в России:

1. Привлечение клиентов

Привлечение целевых посетителей на сайт – удовольствие дорогое. Особенно в высококонкурентном сегменте, где затраты на продвижение сайта и рекламу в интернете могут оказаться неподъемно высокими. Зачастую новый окупает затраты на его привлечение только со второй/третьей покупки. Поэтому важно работать над лояльностью, удержанием клиентов.

2. Удержание клиентов

Чтобы привлеченные дорогой ценой посетители сайта стали вашими покупателями, нужно постоянно работать над юзабилити сайта (удобство сайта для клиента), разрабатывать и внедрять новые online-сервисы.

Сегодня для успешной электронной торговли очень важен клиентский сервис: удобный процесс оформления заказа, возможность оплаты товара/услуг на сайте, своевременная и «вежливая» доставка, возможность выбора/примерки товара при доставке, возврат товара ненадлежащего качества и другие сервисы. Предстоит интеграция сайта с сервисами online-оплаты, службами доставки, сервисами общения клиентов с менеджерами компании online.

Поэтому еще на этапе создания сайта нужно включать данный сервис в техзадание программисту (если вы делаете индивидуальный сайт). Если сайт делается на одной из популярных cms-платформ, как правило, основные сервисы в нее уже включены. По мере развития бизнеса сайт будет нуждаться в новых модулях и сервисах. Индивидуальным сайтам дорабатывать функционал дороже, чем сайтам на популярных cms. На начальном этапе online-бизнеса нужно понимать, что затраты на доработку и техподдержку сайта будут постоянными.

3. Доставка товаров

Болезненный вопрос для всех интернет-магазинов с широкой географией продаж – доставка товаров. Если доставку нужно осуществлять в отдаленные регионы, конечная стоимость товара может значительно увеличиться и оказаться не конкурентной. В стоимость товара нужно закладывать риски возврата товара, и в первую очередь это затраты на доставку. Все это очень усложняет бизнес электронной коммерции в России.

4. Online-оплата

Проблемы российского менталитета и высоких процентов мешают развитию online-платежей в России. Покупатели еще опасаются мошенников и неохотно производят платежи на малознакомых сайтах. К тому же за каждый платеж на вашем сайте придется заплатить приличную комиссию банку и процессинговому центру (по банковским картам в среднем 3 %, по электронным деньгам 4–5 %); другой вариант оплаты товаров – наличными курьеру в момент доставки – есть высокий риск отказа от покупки на этапе доставки. Соответственно, в риски, а значит и в стоимость товара придется закладывать стоимость двойной доставки (туда-обратно). Все это мешает развитию рынка интернет-торговли в России.

Также затрудняют рост электронной коммерции в России такие факторы, как отсутствие единых стандартов, безопасность персональных данных, защита интеллектуальной собственности.

Во многом успех бизнеса электронной торговли в России зависит от бизнес-партнеров. Но, к сожалению, культура аутсорсинга в России еще слабо развита, и чтобы правильно выстроить работу с подрядчиками, самому владельцу магазина нужно разбираться в основах всех аспектов бизнеса электронной коммерции.

В Европе электронная коммерция развивалась другим путем. Еще до появления интернет-магазинов были созданы условия для их развития: отлажена система удаленных платежей, доставки, отслеживания посылок. Поэтому электронная торговля в Европе более развита и понятна, однако есть предел объема рынка и многие зарубежные интернет-магазины сейчас приходят к нам и учатся справляться со сложностями ведения online-бизнеса в России.

Основной тенденцией рынка электронной торговли в России является стремительный рост – более 20–25 % в год. Обороты продаж растут. Открываются новые интернет-магазины, большинство из которых закрываются в первый же год, в основном из-за проблем, перечисленных выше. Растут объемы трансграничных продаж. Российский рынок электронной коммерции является достаточно привлекательным и поэтому имеет большой потенциал для дальнейшего развития и роста.

Сегодня электронная коммерция предоставляет самые широкие возможности как поставщикам, так и клиентам. Среди этих возможностей:

1. Самостоятельная регистрация покупателя на сайте поставщика. Это создает дополнительные удобства в обслуживании для клиентов, а поставщикам позволяет осуществлять адресную рекламу своих товаров и услуг и маркетинговые исследования в процессе продаж.

2. Оформление заказов через Интернет с помощью электронных каталогов и прайс-листов. Данная возможность обеспечивает значительную экономию времени на поиске необходимого товара или услуги и сравнении цен различных поставщиков.

3. Электронная обработка заказа, включая проверку наличия товара на складе, расчет возможных сроков поставки. Данная возможность является неотъемлемой функциональной часть логистической системы предприятия.

4. Прием оплаты за покупку через Интернет. Оплата при этом может осуществляться посредством банковских карт через защищенные платежные терминалы, а также с помощью локальных или международных платежных интернет-систем.

Электронная коммерция имеет все возможности для дальнейшего развития. Экономия на затратах интернет-магазинов позволяет им снижать цены и покупать в интернет-магазинах сегодня порой гораздо выгоднее, нежели в обычных магазинах. Этот факт обеспечивает и постоянный приток покупателей, и появление новых игроков на рынке. Электронный бизнес становится более конкурентным, что в свою очередь положительным образом сказывается на уровне качества оказываемых услуг и предлагаемых товаров.

2. ЭЛЕКТРОННЫЙ БИЗНЕС И ЭЛЕКТРОННАЯ КОММЕРЦИЯ: ОСНОВНЫЕ ПОНЯТИЯ

2.1. Электронный бизнес

Развитие телекоммуникаций привело к тому, что в настоящее время частные лица и компании во всем мире связаны между собой посредством электронных каналов связи.

Интернет, являясь инструментом организации единого информационного пространства, позволил бизнесу выйти на новый виток развития. С одной стороны, он предоставил производителям доступ к максимальной аудитории потребителей со всеми их разнообразными предпочтениями. С другой стороны, дал клиентам возможность с помощью электронных интерфейсов самим вводить свои заказы в отлаженную систему управления производством. Таким образом, в последние годы электронный бизнес и электронная коммерция вошли в жизнь больших и малых фирм, а также частных лиц.

Чем же электронная коммерция отличается от электронного бизнеса?

Бизнес – это ***предпринимательская деятельность,*** направленная на ***систематическое получение прибыли*** от пользования имуществом, продажи товаров, выполнения работ или оказания услуг и осуществляемая субъектами на свой риск и под свою ответственность в соответствии с действующим законодательством.

Электронный бизнес *(e-business)* – это бизнес, использующий возможности глобальных информационных систем. Другими словами, это форма ведения бизнеса, при которой значительная его часть выполняется с применением информационных технологий. В качестве основных составляющих электронного бизнеса принято выделять внутреннюю организацию компании на базе единой информационной сети (интранет) и внешнее взаимодействие с партнерами, поставщиками и клиентами посредством сетей экстранет и Интернет. Основная цель создания сети интранет (локальной сети) – повышение эффективности взаимодействия сотрудников и оптимизации процессов управления компанией.

Элементы электронного бизнеса стали появляться в деятельности компаний с 60-х гг. XX в. Это автоматические системы ведения бизнеса, такие как:

– средства электронного обмена данными (Electronic Data Interchange, EDI);

– средства электронного перевода средств (Electronic Fund Transfer, EFT);

– средства планирования корпоративных ресурсов (Enterprise Resource Planning, ERP).

Таким образом, электронный бизнес представляет собой все формы электронной бизнес-деятельности производственных и организационных отношений между работниками одного предприятия, между различными предприятиями, государственными органами, учреждениями науки, культуры, образования, некоммерческими и общественными организациями.

Компания IBM зарегистрировала понятие «электронный бизнес» как торговую марку: «***The transformation of key business processes through the use of Internet technologies***», что означает «*преобразование основных бизнес-процессов при помощи интернет-технологий*».

Имеется в виду, что все стороны деловых отношений, включая внутреннее планирование работы и управления, маркетинг, продажи, финансовый анализ, платежи, поиск сотрудников, поддержку клиентов и партнеров, перенесены в Интернет.

К основным видам электронного бизнеса относятся:

– торговые площадки (интернет-биржи, аукционы, каталоги товаров и услуг);

– электронное управление закупками;

– порталы (корпоративные, информационные, коммерческие, персональные);

– организация, содержание и обслуживание общественных глобальных сетей (осуществляется операторами сетей);

– финансовые услуги (интернет-платежные системы, обменные пункты, интернет-банкинг, online-трейдинг);

– инвестиционные фонды (консолидированные инвестиционные фонды или буферные фонды и паевые инвестиционные фонды);

– интернет-магазины;

– контент-проекты (сайты с бесплатной и востребованной информацией для привлечения посетителей с целью ведение рекламного бизнеса);

– информационные посредники (каталоги, рейтинги, поисковые системы);

– информационный бизнес в Интернете (периодические интернет-издательства, новостные сайты и т.д.);

– интернет-маркетинг (продвижение сайта в поисковых системах);

– рекламный бизнес;

– услуги связи и средства общения;

– web-мастеринг (создание сайтов, веб-программирование, веб-дизайн, раскрутка сайтов);

– MLM, или сетевой маркетинг (форма ведения внемагазинной розничной торговли);

– разработка ПО и цифровых товаров;

– услуги сервис-провайдеров (поставщики сетевых услуг, поставщики хостинга, доменов);

– предоставление услуг (дистанционное обучение, сетевые библиотеки, электронное здравоохранение, интернет-консалтинг и т.д.);

– игорный бизнес в сети (виртуальные казино, букмекерские конторы, тотализаторы, лотереи);

– биржи труда (агентства по трудоустройству);

– партнёрские программы (аффилат-программы и др.);

– интернет-франчайзинг;

– интернет-лизинг.

2.2. Электронная коммерция

Первостепенной задачей, стоящей перед электронной коммерцией как отраслью экономической науки, является выработка научного определения понятия электронной коммерции и ее предметной области. Основной проблемой, с которой сталкиваются авторы при попытке решения данной задачи, является конфликт между эмпирическим и этимологическим подходами к ее решению.

Под **электронной коммерцией** следует понимать любую экономическую деятельность с использованием электронных информационных технологий. Предметной областью электронной коммерции как отрасли экономической науки являются экономические отношения, в процессе которых используются электронные информационные технологии.

Чтобы понять, что собой представляет ***электронная коммерция***, необходимо обратиться к этимологии слова «коммерция». Слово «commerce» в переводе с французского, откуда оно и попало в русский язык, означает «торговля».

Электронная коммерция, или ***электронная торговля*** *(e-commerce)* – это процесс покупки, продажи, передачи или обмена продуктами, услугами и информацией с помощью электронных средств коммуникации.

Существуют и другие определения ***электронной коммерции***, например, это коммерческая деятельность, имеющая целью получение прибыли и основанная на комплексной автоматизации коммерческого цикла за счет использования компьютерных сетей.

Экономисты определяют электронную коммерцию как «область народного хозяйства, которая охватывает все бизнес-процессы, связанные с проведением транзакций, финансовые и торговые сделки, осуществляемые при помощи компьютерных сетей».

В проекте Федерального закона «Об электронной торговле» она трактуется как «осуществление сторонами сделки предусмотренных законодательством действий и операций при оформлении и совершении сделок по продаже/поставке товаров, выполнению работ, оказанию услуг, а также совершение иных действий, направленных на извлечение прибыли, на основе исполнения электронных процедур».

Также следует заметить, что существуют две трактовки понятия «электронная коммерция» – узкая и широкая.

В узком смысле под электронной коммерцией понимается реклама и продажа товаров с помощью телекоммуникационных сетей.

В широком смысле, в соответствии с определением Комиссии ООН по праву международной торговли (ЮНСИТРАЛ),

посредством электронной коммерции могут выполняться сделки купли-продажи, поставки, а также факторинг, лизинг, консалтинг, инжиниринг и другие сделки в сфере промышленного и делового сотрудничества.

Таким образом, ***электронная коммерция – это важнейшая составная часть электронного бизнеса***, которая представляет собой новый способ организации, управления и осуществления бизнес-сделок с использованием компьютеров и коммуникационных сетей, т.е. любая форма бизнес-сделки, в которой стороны взаимодействуют электронным способом, а не посредством физических операций обмена или прямого физического контакта.

Системы электронного бизнеса, в отличие от систем электронной коммерции, могут иметь или не иметь коммерческой составляющей.

Торговля, или ***электронная коммерция***, дает возможность компаниям быть более эффективными и гибкими в их внутренней деятельности, работать более тесно с их поставщиками и оперативно реагировать на нужды и ожидания клиентов. Причем она позволяет компаниям выбрать самых лучших поставщиков независимо от их географического расположения и продавать на глобальном рынке.

К основным видам электронной коммерции относятся:

– электронный трейдинг (e-trade);

– электронные деньги (e-cash);

– электронный маркетинг (e-marketing);

– электронный банкинг (e-banking);

– электронное страхование (e-insurance).

Первый опыт создания системы электронной коммерции относится к 1960 г., когда компании American Airlines и IBM приступили к созданию системы автоматизации процедуры резервирования мест на авиарейсы – SABRE (Semi-Automatic Business Research Environment – полуавтоматическое оборудование для коммерческих исследований). Система SABRE сделала воздушные перелеты более доступными для рядовых граждан, помогая им ориентироваться в тарифах и рейсах, число которых постоянно росло. За счет автоматизации процесса расчета тарифов при резервировании мест снижалась стоимость услуг.

Один из лидеров электронной коммерции – компания Cisco Systems – в настоящее время автоматизировала свою сбытовую деятельность таким образом, что 90 % заказов от потребителей обрабатывается без участия сотрудников.

Электронная коммерция основана на структуре традиционной коммерции, а использование компьютерных сетей добавляет ей гибкость (рис. 1).

Интернет предоставляет обычным пользователям, бизнесу и государству различные возможности. При подключении к Интернету пользователь получает доступ к определенному набору услуг – как платным, так и бесплатным.

Рис. 1. Составляющие электронной коммерции

Примерный перечень набора услуг в Интернете:

– получение различной информации – платные и бесплатные веб-страницы. Доступ к государственной информации и взаимодействие с госаппаратом (например, оплата налогов, штрафов) – сектор Government-to-Customer – G2C;

– доступ к интернет-услугам – почта, хостинг, обмен моментальными сообщениями (IM) – ICQ;

– доступ к финансовым интернет-услугам – осуществление банковских операций (депонирование, получение денег в кредит, оплата счетов и пр.), брокеридж (получение данных с рынка и покупка/продажа ценных бумаг в режиме реального

времени), интернет-страхование (покупка полиса через Интернет);

– интернет-шопинг – покупка любых товаров через Сеть; в Интернете пользователь может распространять информацию, может влиять на общественное мнение (в том числе и на рыночные ожидания) – использование веб-досок, конференций;

– e-workforce (электронное рабочее место) – удаленные рабочие места, сотрудник может оперативно работать на компанию, которая находится в другом городе/стране, не посещая офиса самой компании.

2.3. Предпосылки возникновения электронной коммерции

Существуют экономические и технические предпосылки возникновения электронной коммерции.

Экономические предпосылки

XX в. характеризовался постоянным стремлением к снижению нормативного времени исполнения технологических операций на производстве за счет:

– в I-й четверти XX в. – внедрения принципов массового производства;

– во II-й четверти XX в. – расширенной механизации производства;

– в III-й четверти XX в. – автоматизации производства;

– в IV-й четверти XX в. – гибкого автоматизированного управления проектированием и производством продукции.

Таким образом, в течение последнего столетия произошло повышение производительности труда в сотни раз, что значительно снизило удельный вес затрат на оплату обобществленного труда в структуре себестоимости обобществленной продукции. Но конечный потребитель ощутил эти достижения не в полной мере. Из-за чего это произошло? Это произошло из-за того, что концентрация производства, объективно связанная с его автоматизацией и механизацией, привела к отдалению производителя от рынков потребления. Характер этого отдаления не только географический, но и структурный. Поэтому необходимы торговые структуры, которые и выполняют функции про-

движения товаров от производителя к потребителю. ***Следовательно, чем выше концентрация производства, тем сложнее торговые структуры и тем больше этапов имеет коммерческий цикл при движении товаров***.

Основные этапы коммерческого цикла:

– исследование рынка товаров и услуг;

– управление свойствами товаров и услуг;

– оповещение рынка о свойствах товаров и услуг;

– подготовка рынка к использованию заданных свойств товаров и услуг;

– прием, обработка и исполнение заказов на товары и услуги;

– оптимизация товарных потоков и складских запасов;

– взаиморасчеты с клиентами и поставщиками;

– послепродажное обслуживание.

В итоге к концу XX в. человечество имело и имеет сегодня удовлетворительную автоматизацию производственных циклов и не соответствующий ей низкий уровень автоматизации циклов коммерческих.

Таким образом, экономической предпосылкой явилась объективная необходимость снижения издержек, возникающих в коммерческих циклах, и приближение их к нормам, достигнутым в результате автоматизации циклов производственных.

Технические предпосылки

Можно назвать лишь одну фундаментальную техническую предпосылку электронной коммерции – это возникновение и развитие Интернета, так как благодаря этому, а также развитию сетей телекоммуникаций открылась возможность комплексной автоматизации коммерческой деятельности.

Часто при анализе взаимосвязи ЭК и Интернета электронную коммерцию представляют, как совокупность методов, предоставляемых всемирной паутиной для решения конкретных коммерческих задач: проведения маркетинговых исследований, рекламы, автоматизированный прием рекламы и др.

Необходимо заметить, что предпосылки возникновения электронной коммерции находятся не в Интернете – они лежат в объективных законах развития экономики и общества. Интернет

– это лишь средство реализации давно назревших объективных потребностей в автоматизации коммерческого цикла и инструмент для снижения доли издержек, приходящихся в них в структуре отпускной цены продукции. Наличие такого инструмента, как Интернет, это только техническая предпосылка к возникновению электронной коммерции, но не ее основа.

Преимущества электронной коммерции

Компании, занимающиеся электронной коммерцией, получают ряд преимуществ по сравнению с предприятиями «реальной» коммерции:

– расширение рынка сбыта с перспективой выхода на зарубежные рынки;

– круглосуточная доступность;

– автоматизация маркетинговой информации с использованием CRM-систем (Customer Relationship Management – управление отношениями с клиентами), позволяющая собирать информацию о посетителях сайта, которую они всегда оставляют о себе.

3. СИСТЕМЫ ЭЛЕКТРОННОЙ КОММЕРЦИИ

3.1. Бизнес-модели электронной коммерции

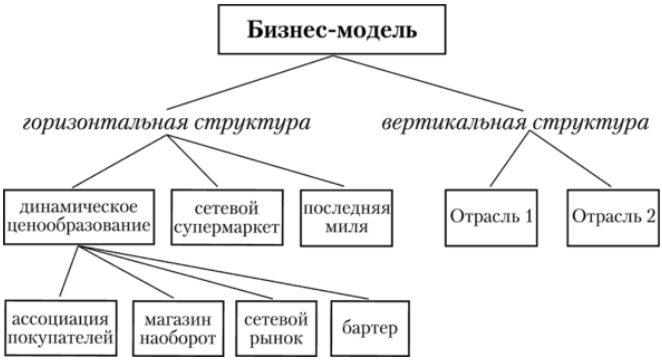

Рис. 2. Бизнес-модели, ориентированные на конечного пользователя

Данная классификация учитывает бизнес-модели, в основе которых лежит процесс продажи товара, и не учитывает возможности оказание бизнесом различных услуг с помощью Интернета. Финансовые услуги для конечного пользователя будут выделены в отдельную классификацию.

Горизонтальные бизнес-модели – модели, не ориентированные на конкретную отрасль или вид продукции.

Горизонтальные модели можно, в свою очередь, разделить на несколько типов:

1. *Сетевые супермаркеты* – наиболее многочисленная и развитая группа. Используют Интернет в качестве основного канала продвижения продукции.

2. *Последняя миля.* Такие компании осуществляют доставку до конечного покупателя.

3. *Динамическое ценообразование.* В эту группу попадают компании, продажная цена у которых не является фиксированной.

К данному типу бизнес-моделей относятся следующие:

• *сетевые рынки/аукционы;*

• *магазин наоборот.* Такая бизнес-модель подразумевает, что продавцы конкурируют между собой за конкретного покупателя, каждый из которых выставляет свои собственные условия (цена, условия доставки и т.п.);

• *ассоциации потребителей.* Такие компании позволяют потребителям объединять свои заказы и получить более низкую цену за счет экономии на масштабе;

• *бартер.* Компании создают инфраструктуру, способную эффективно сводить стороны, желающие обменяться тем или иным товаром.

Категории электронной коммерции: потребитель, компания, администрация, правительство. Их взаимосвязь представлена на рис. 3.

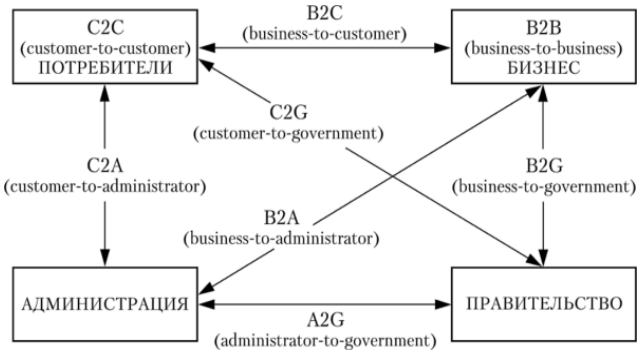

Рис. 3. Взаимосвязь категорий электронной коммерции

Данная схема представляет все восемь моделей отношений между категориями электронной коммерции:

• B2B (бизнес-бизнес) определяется как категория электронной коммерции, при которой участниками рынка являются две компании. Например, связи и отношения между дилерами и поставщиками, головными офисами компаний и их региональными представителями;

• B2C (бизнес-потребитель) регламентирует отношения между компаниями и потребителями, т.е. розничную электронную торговлю (интернет-магазины);

• B2A (бизнес-администрация) регламентирует отношения между бизнесом и администрацией, вопросы лицензирования, разрешения на деловую активность предприятия, поставки оборудования, таможня и т.п.;

• B2G (бизнес-правительство) – концепция построения бизнес-процессов предприятия, обеспечивающая повышение его «прозрачности» и облегчающая взаимодействие с государственными органами;

• C2C (потребитель-потребитель) регламентирует отношения между двумя потребителями, например, по обмену опытом по совершению коммерческих сделок. Классический пример – интернет-аукцион;

• C2A (потребитель-администрация) регламентирует отношения между потребителями и государственными структурами в различных областях и сферах экономики;

• C2G (потребитель-правительство) регламентирует отношения между потребителями и правительством. Увеличение общественного участия, в том числе и палат общественных экспертов, в политическом принятии решений и законодательной экспертизе;

• A2G (администрация-правительство) регламентирует отношения между администрацией и правительством в области политики и законодательства на макроуровне.

Система электронной коммерции B2B предназначена для осуществления торговых операций между предприятиями в Интернете. Это отношения между бизнес-партнерами, связанными единой цепочкой добавленной стоимости. Сюда включаются все торговые отношения между различными фирмами, организация поставок, продаж, согласование контрактов и планов.

Системы класса B2B – это системы интернет-торговли для партнеров и корпоративных заказчиков продукции и услуг крупных компаний, и корпораций. Организуется web-сайт, на котором корпоративные продавцы и покупатели (участники определенной индустрии) собираются вместе, чтобы продавать, покупать, рекламировать, участвовать в аукционах, совершать транзакции.

Отсутствие посредников позволяет участникам действовать напрямую и минимизирует издержки, также увеличивается

скорость принятия решения за счет быстрого обмена информацией. Электронный бизнес позволяет улучшить обслуживание клиентов при одновременном сокращении затрат, выявить новые каналы сбыта, обеспечить конкурентное преимущество.

Пока электронные биржи системы B2B работают в режиме, близком к информационному, в online проходят не все этапы заключения сделки. Подписание договора чаще всего происходит в offline. Это связано с тем, что тяжело наладить систему гарантий поставок для участников.

Для крупного бизнеса предлагаются следующие решения: создание торговых интернет-систем (ТИС), marketplace-систем, проведение аукционов.

ТИС – это специальное программное обеспечение электронной коммерции для службы сбыта и снабжения крупных торговых компаний, корпораций и холдингов. ТИС полностью интегрирована в уже сложившийся бизнес-процесс компании за счет подключения к автоматизированным торговой системе и системе управления ресурсами предприятия.

Посредством ТИС производитель может управлять своей региональной сетью дистрибьюторов и посредников, а дистрибьюторы – своей дилерской сетью. Специализированная ТИС позволяет организовать эффективную систему снабжения корпораций сырьем, материалами и комплектующими.

Аукционы – это специальное программное обеспечение электронной коммерции, установленное на сайте организатора торгов и предназначенное для создания системы сбыта или снабжения.

Marketplace-системы (отраслевые торговые интернет-площадки) предназначены для группы компаний, принадлежащих одной отрасли промышленности. Они представляют собой вертикальные (отраслевые) интернет-ресурсы, в которых объединены сервисные, электронно-коммерческие и маркетинговые составляющие. При их создании используется специальное программное обеспечение электронной коммерции, при этом создается единая служба сбыта и снабжения компаний, принадлежащих одной отрасли промышленности.

Система электронной коммерции C2C предназначена для осуществления торговых операций между самими потребителями в Интернете.

C2C – это интернет-аукционы, на которых происходит продажа товара (лота) без посредников. Популярность такой торговли очень быстро растет.

Особенности бизнес-модели интернет-аукциона: большое количество покупателей; большое количество товаров (нереализованных, б/у, уцененных); прямое интерактивное общение продавцов и покупателей; различные модели аукционов; круглосуточная работа; отсутствие территориальных границ; подробное описание и изображение товара.

Система электронной коммерции B2C предназначена для осуществления торговых операций между торговыми компаниями и потребителями, это система интернет-торговли для конечного покупателя продукции и услуг торговых компаний (розничная торговля).

Все системы розничной торговли через Интернет можно классифицировать как web-витрины, торговые площадки, интернет-магазины и торговые ряды.

Web-витрина реализована в виде простого web-сайта с web-каталогом и прайс-листом с кратким (или расширенным) описанием товаров и услуг, предлагаемых торговой компанией. На web-витрине организована система сбора заказов от покупателей. При этом возможно использование разных платежных систем и систем доставки. Предназначена для торговых компаний малого бизнеса.

Web-каталог легко расширяется/изменяется менеджером по продаже торговой компании (без обращения к программистам и web-дизайнерам) с использованием Excel-таблиц.

Web-витрины не имеют развитых средств управления интернет-торговлей, средств анализа статистики продаж и средств интеграции с торговыми системами продавца. Также отсутствуют функции автоматического оформления покупки и механизмы приема электронных платежей.

Торговая площадка – web-сайт, которому присущи черты как web-витрины, так и интернет-магазина. Она позволяет редактировать содержимое «корзины покупателя», ее стоимость,

стоимость доставки в зависимости от района проживания, выбирать форму оплаты. Обработку поступивших заказов, прием платежей и контроль за отгрузкой уже оплаченных покупок сотрудники фирмы-продавца производят вручную.

Интернет-магазин – это специальное программное обеспечение, которое упрощенно состоит из трех блоков.

Первый блок (фронт-офис) – это то, что видит покупатель в интернет-магазине: витрину, каталог, описание товаров, систему оформления заказов, информацию о торговой компании и о магазине и т.д.

Второй блок (бэк-офис) – это то, что видит только менеджер интернет-магазина. Через бэк-офис менеджер управляет интернет-магазином: удаляет или заносит новый товар в базу данных товаров; конфигурирует каталог товаров; устанавливает цены и скидки на товары; задает различные дисконтные схемы для своих дилеров и/или своих постоянных покупателей; управляет складом товаров интернет-магазина; формирует заказы на пополнение склада интернет-магазина; обрабатывает статистику о всех заказах, товарах и покупателях в интернет-магазине.

Третий блок – это база данных, в которой хранится вся информация о товарах, покупателях, заказах. В базе данных хранится также вся бизнес-логика обработки заказов и все настройки интернет-магазина.

В интернет-магазине могут быть реализованы практически любые торговые бизнес-схемы: торговля со склада и на заказ; торговля с частными лицами и с организациями; торговля вещественными и цифровыми товарами, услугами, информацией и т.д. При этом возможны различные сочетания схем оплаты и доставки товаров и услуг, предлагаемых покупателю на выбор.

Создание собственного интернет-магазина требует значительных затрат. Именно из-за этого в настоящее время наблюдается рост сервисных служб, предоставляющих готовые электронные магазины в аренду.

Торговые ряды – это специализированные порталы, позволяющие начать торговлю в Интернете без покупки дорогостоящего программного обеспечения. При аренде интернет-магазина компания-арендатор представляет данные по выстав-

ляемым товарам и передает эту информацию по электронной почте в администрацию портала. Администратор системы заносит товары в виртуальный каталог и отслеживает торговый процесс в каждом торговом магазине системы.

Возможна и иная ситуация: арендатору предоставляется лишь дисковое пространство и все необходимое программное обеспечение, настройку и сопровождение которого он должен выполнять самостоятельно.

3.2. Факторы снижения издержек при использовании электронной коммерции

Дальнейшее расширение сферы электронной торговли будет зависеть не только от улучшения инфраструктуры и более благоприятных условий доступа к Интернету во всем мире. В первую очередь оно будет связано с конкретными преимуществами, которые получит деловой сектор от использования инструментов электронной торговли в своей деятельности,

Можно привести следующие *факторы конкретной коммерческой выгоды от электронной коммерции*:

Первый фактор – снижение затрат на получение информации.

Интернет – наиболее быстрый и дешевый (по сравнению с другими способами сбора информации) источник получения информации. Для использования некоторых методов маркетингового исследования (опрос, анкетирование, сбор информации и т.д.) не требуется личный контакт с респондентами.

Второй фактор – снижение расходов на рекламу.

Себестоимость создания, распространения и обслуживания рекламы в сети Интернет гораздо ниже по сравнению с другими методами рекламы.

Третий фактор – снижение расходов на внутренние коммуникации.

Снижение расходов на оплату труда за счет уменьшения числа выездных мероприятий, телефонных переговоров. Экономия рабочего времени в части поиска необходимой информации.

Четвертый фактор – снижение расходов на внешние коммуникации.

Данное снижение происходит за счет автоматизации сбора, обработки заказов (быстрый доступ к информации о заказе, состоянии его исполнения и т.п.).

Пятый фактор – снижение расходов на аренду офисных помещений, организацию рабочих мест.

Работа сотрудников фирмы может осуществляться с удаленного компьютера (например, домашнего ПК).

Шестой фактор – снижение затрат на закупки товаров и услуг.

Использование системы электронной коммерции делает возможным проведение операций по продвижению товаров (предоставлении услуг) в полностью автоматизированном режиме.

3.3. Базовые технологии электронной коммерции

Электронная коммерция, или е-коммерция, состоит из технологий, предполагающих совершение покупок или продаж через различные платежные системы в Интернете и других компьютерных сетях.

К базовым технологиям электронной коммерции (технико-экономическим и правовым основам) относятся:

1. Аутентификация контрагентов в электронной коммерции.

Аутентификация – процесс идентификации, позволяющий удостовериться в личности стороны, желающей получить интерактивный доступ к информации (услугам). Данная процедура выполняется для обеспечения безопасности и гарантирования исполнения сделок между категориями электронной коммерции.

Аутентификация основывается на использовании паролей доступа к информации (услуге), специальных карточек, алгоритмах электронной цифровой подписи и т.д.

2. Международные стандарты и протоколы.

Стандарты представляют собой набор спецификаций, гарантирующих возможность взаимодействия между электронными коммерческими интернет-системами.

Стандарт OFX – стандарт электронного обмена финансовыми данными между предприятиями финансовой сферы, коммерческими предприятиями и потребителями через Интер-

нет. Основные функции стандарта – перевод денежных средств, потребительские платежи, платежи юридических лиц и т.д.

Протокол открытой торговли в Интернете (Internet Open Trading Protocol – IOTP) обеспечивает совместное функционирование различных систем электронной коммерции при проведении электронных торговых операций.

UDDI – общепринятая система стандартов, которая позволит системам электронной коммерции автоматизировать информационный обмен и осуществление транзакций.

3. Веб-службы.

Веб-служба – виртуальный агент, предоставляющий услуги через Интернет, постоянно присутствующий в сети робот, запрограммированный на сбор и фильтрацию необходимой информации, поиск контрагентов (ресурсов компьютерной сети, отвечающих заданным критериям), на осуществление определенных действий.

Данная технология позволяет снизить информационную нагрузку на субъекты электронной коммерции, повысить эффективность процедур установления контактов, проведения переговоров, осуществления взаиморасчетов и т.д.

4. Автоматизированные системы управления ресурсами предприятия.

Системы управления ресурсами предприятия в электронной коммерции служат основой эффективных бизнес-коммуникаций. Внедрение данных систем позволяет оптимизировать экономические процессы предприятия и сделать максимально полное использование преимуществ различных систем электронной коммерции. В свою очередь, успешный рост электронной коммерции делает особенно актуальным внедрение новых систем автоматизации управления ресурсами предприятия (MRP, MRP II, ERP, CSRP и т.п.).

5. Правовое обеспечение электронной коммерции.

Правовое обеспечение электронной коммерческой деятельности определено спецификой электронной среды телекоммуникаций. Все сделки, совершаемые в Интернете, должны отвечать действующему законодательству.

4. ПЛАТЕЖНЫЕ СИСТЕМЫ ИНТЕРНЕТА

4.1. Основные понятия и классификация платёжных систем

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

В системе электронной коммерции платежи совершаются при соблюдении ряда условий:

• ***Соблюдение конфиденциальности.*** При проведении платежей через Интернет, покупатель хочет, чтобы его данные (например, номер кредитной карты) были известны только организациям, имеющим на это законное право.

• ***Сохранение целостности информации.*** Информация о покупке никем не может быть изменена.

• ***Аутентификация.*** Покупатели и продавцы должны быть уверены, что все стороны, участвующие в сделке, являются теми, за кого они себя выдают.

• ***Средства оплаты.*** Возможность оплаты любыми доступными покупателю платежными средствами.

• ***Авторизация***. Процесс, в ходе которого требование на проведение транзакции одобряется или отклоняется платежной системой. Эта процедура позволяет определить наличие средств у покупателя.

• ***Гарантии рисков продавца.*** Осуществляя торговлю в Интернете, продавец подвержен множеству рисков, связанных с отказами от товара и недобросовестностью покупателя. Величина рисков должна быть согласована с провайдером платежной системы и другими организациями, включенными в торговые цепочки, посредством специальных соглашений.

• ***Минимизация платы за транзакцию.*** Плата за обработку транзакций заказа и оплаты товаров, естественно, входит

в их стоимость, поэтому снижение цены транзакции увеличивает конкурентоспособность. Важно отметить, что транзакция должна быть оплачена в любом случае, даже при отказе покупателя от товара.

Все платежные системы по имеющейся схеме платежей можно разделить на следующие виды:

• дебетовые (работающие с электронными чеками и цифровой наличностью);

• кредитные (работающие с кредитными карточками).

Дебетовые системы

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

Электронные чеки

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

Проведение платежей проходит в несколько этапов:

1. Плательщик выписывает электронный чек, подписывает электронной подписью и пересылает его получателю. В целях обеспечения большей надежности и безопасности номер чекового счета можно закодировать открытым ключом банка.

2. Чек предъявляется к оплате платежной системе. Далее (либо здесь, либо в банке, обслуживающем получателя) происходит проверка электронной подписи.

3. В случае подтверждения ее подлинности поставляется товар или оказывается услуга. Со счета плательщика деньги перечисляются на счет получателя.

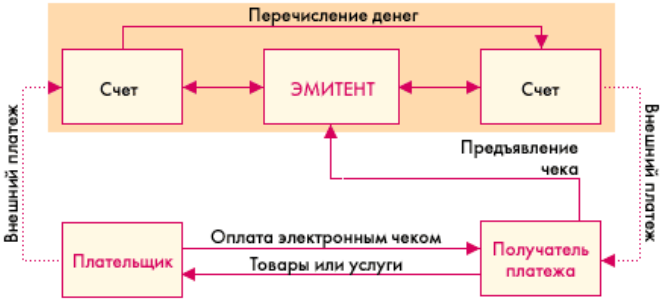

Рис. 4. Схема платежа с использованием электронных чеков

Подобные схемы платежей просты и давно применяются за рубежом (NetCash, NetChex, NetCheque), но для России они пока не слишком актуальны, т.к. прежде всего отсутствует широкая практика использования чеков даже при offline расчетах, а также отсутствуют сертификационные центры. Одной из первых ласточек в этой сфере электронных платежей в нашей стране является система PAYMER, в которой в качестве расчетного средства используются цифровые чеки.

Электронные деньги

В условиях интенсивного роста технологических и рыночных инноваций в сфере розничных платежей, приводящих к появлению новых средств платежа и платежных инструментов, все большее значение приобретает четкое определение новой экономической категории – электронных денег (e-money), а также выявление функционально-технологических особенностей их расчетных схем и организации систем электронных денег.

В экономическом смысле электронные деньги являются денежной стоимостью, представленной требованием на эмитента, выраженной в правительственных или частных денежных единицах и хранящейся в электронной форме на электронном устройстве. Согласно Директиве Европейского Парламента и

Совета № 2000/46/ЕС «О регулировании деятельности институтов – эмитентов электронных денег», публикациям Европейского Центрального банка и Банка международных расчетов, посвященным актуальным проблемам развития электронных денег, можно выделить следующие основные элементы, характеризующие электронные деньги в качестве нового средства платежа:

1) электронные деньги представляют собой денежную стоимость;

2) хранение стоимости основывается на электронном устройстве;

3) выпуск стоимости производится на основе предварительного внесения денежных средств;

4) прием стоимости осуществляется третьими лицами.

Денежная стоимость

Электронные деньги являются платежным продуктом, хранящим денежную стоимость, представленную требованием на эмитента. Термин «денежная стоимость» в контексте определения электронных денег означает хранилище покупательной способности или денежный актив, которые могут обращаться между экономическими агентами. Основное различие между денежной стоимостью и деньгами состоит в том, что денежная стоимость представляет собой средство платежа, которое может как обмениваться, так и не обмениваться на другие денежные формы. В отличие от наличных денег, которые являются универсальным, обязательным к приему средством платежа, которое выражено в правительственных счетных единицах, используемых для исчисления цен товаров и услуг, а также заключения контрактов на национальном и международном уровне, денежная стоимость не является обязательным к приему средством платежа и может быть выражена в частных денежных единицах. В отличие от традиционных денег, которые могут выпускаться либо центральным банком (в форме наличных денег), либо другими банковскими институтами (в форме депозитных денег), денежная стоимость (электронные деньги) может эмитироваться специализированными небанковскими кредитными института-

ми, предусматривающими особый порядок регулирования их деятельности.

Хранение стоимости на электронном устройстве

Электронные деньги представляют собой средство платежа, которое хранится на электронном устройстве. Такое определение подчеркивает, что электронные деньги являются исключительно электронным средством платежа. Стоимость хранится в электронном виде, а платежи с ее использованием осуществляются в электронной форме. В этой связи вместо термина «денежная стоимость» нередко используется термин «электронная стоимость». В экономическом смысле в контексте электронных денег речь идет не столько о стоимости, сколько о сумме покупательной способности, которой может распоряжаться ее владелец. Тот факт, что электронный носитель может быть магнитным, не ограничивает возможность его использования в качестве носителя электронных денег. Так, «стоимость, хранимая на персональном компьютере, не исключается из определения электронных денег только потому, что она хранится на магнитном (жестком) диске компьютера. Подобным образом, стоимость, которая хранится на пластиковой карточке, использующей технологию магнитной полосы, может также включаться в определение электронных денег, если расходуемая стоимость переводится с использованием электронной технологии».

Предоплата стоимости

Электронные деньги являются средством платежа, эмитируемым на основе предварительно полученных денежных средств. При этом величина внесенных в качестве предоплаты денежных средств эквивалентна величине выпускаемых электронных денег. В отличие от кредита, предоставляемого по кредитной карточке, а также прямых списаний, производящихся по дебетовой карточке, в случае электронных денег потребитель оплачивает свою покупательную способность заранее. Покупка электронных денег означает покупку денежной стоимости. Это не означает, что электронные деньги, оплаченные по кредитной карточке, не включаются в их определение. В данном случае имеют место две сделки: одна состоит в продаже электронных

денег, вторая – в предоставлении кредита. Тот факт, что средство хранения денежной стоимости сделано на основе пластиковой карточки, которая может также функционировать как дебетовая или кредитная карточка, не означает, что денежная стоимость не является электронными деньгами.

Многоцелевое использование стоимости

Электронные деньги являются средством платежа, которое принимается третьими лицами (институтами, предприятиями и индивидуумами), отличными от эмитента. Это означает, что держатель электронных денег должен иметь возможность использовать их для покупки товаров и услуг у широкого круга лиц. Например, электронная стоимость, которая выпущена работодателем для своих рабочих и может использоваться только для покупки обедов в столовой работодателя, не является электронными деньгами. Тот факт, что денежная стоимость может быть потрачена у третьих лиц, не означает, что она не может быть потрачена у эмитента.

Рассмотренные выше элементы определения электронных денег являются важными для понимания тех характеристик электронных денег как нового средства платежа, которые отличают их от других средств платежа или платежных инструментов, в том числе от пред авторизованных дебетовых карточек (pre-authorized debit cards) или так называемых зарплатных карточек (payroll cards). Тем не менее элементы определения электронных денег не позволяют предложить однозначную интерпретацию электронных денег в качестве новой экономической категории.

4.2. Подходы к интерпретации электронных денег

Одна из основных причин, по которым определение электронных денег и регулирующие подходы к деятельности в этой сфере отличаются в разных развитых странах, состоит в различном толковании вопроса о том, должна ли интерпретация электронных денег строиться на концепции логического владения (функциональный подход) или физического владения (подход физического владения) средством платежа.

Кочергин Д. А. кратко описал функциональный подход к интерпретации электронных денег следующим образом:

• «электронные деньги являются денежной стоимостью, хранящейся на электронном устройстве. Устройство (device) понимается здесь в широком смысле – это может быть физическое устройство (physical device), логическое устройство (logical device) или смешанная технология хранения и обработки стоимости;

• устройство для осуществления транзакций (платежный инструмент) с использованием электронных денег потребителя (карточка, мобильный телефон, персональный компьютер и др.) является технологически нейтральным в том смысле, что оно может либо содержать запись о сумме электронных денег непосредственно, либо предоставлять немедленный доступ к источнику, содержащему такую запись (например, удаленному компьютерному серверу эмитента);

• несмотря на то что удаленный компьютерный сервер не находится во владении держателя электронных денег, он выполняет те же функции, что и устройства для осуществления транзакций, находящиеся во владении держателя, поэтому он может рассматриваться в качестве электронного устройства, на котором хранятся электронные деньги и функциональное приложение электронных денег (функциональное приложение электронных денег представляет собой программную оболочку, позволяющую осуществлять операции по хранению и переводу электронных денег);

• системы электронных денег (модель с набором подсистем, которые позволяют электронной стоимости перемещаться под контролем системного оператора, отслеживающего безопасность создания, обращения и уничтожения электронной стоимости) могут работать как на основе индивидуальных счетов (individual accounts), так и на основе общеэмиссионных счетов (general liability accounts), также известных как теневые счета (shadow accounts), поскольку функционально и те, и другие не являются депозитами.

Подход физического владения к интерпретации электронных денег может быть кратко описан следующим образом:

• «электронные деньги» являются денежной стоимостью, хранящейся на электронном устройстве, которое находится в физическом владении потребителя;

• устройство для осуществления транзакций (платежный инструмент) с использованием электронных денег потребителя (карточка, мобильный телефон, персональный компьютер и др.) должно в то же самое время быть устройством, которое содержит электронные деньги (т.е. содержит запись о сумме электронных денег);

• удаленный компьютерный сервер не находится во владении держателя и поэтому не может рассматриваться как электронное устройство, на котором хранятся электронные деньги и функциональное приложение электронных денег;

• системы электронных денег не могут работать на основе индивидуальных счетов, поскольку фактически это делало бы электронные деньги одной из форм депозитов – предполагается, что в системах электронных денег допускается использование только общеэмиссионных счетов, которые выполняют не финансовую, а учетную функцию. Они используются (в целях безопасности осуществляемых платежей) для фиксирования информации об объемах эмиссии электронных денег и их уничтожении. Система на основе дистанционного доступа к серверам, имеющая возможность блокировать использование электронных денег, когда одно из устройств связи (например, мобильный телефон) потеряно, представляет собой систему на основе банковского счета, а не систему электронных денег.

В настоящее время функциональный подход к интерпретации электронных денег является более востребованным как среди исследователей, так и среди разработчиков новых электронных платежных систем, поскольку только технологически нейтральная интерпретация позволяет полностью реализовать потенциальные выгоды от внедрения электронных денег, таких как сокращение транзакционных издержек и снижение платежных/расчетных рисков, а также стимулировать внедрение технологических инноваций и способствовать созданию критической массы пользователей новых средств платежа.

4.3. Схема платежа с помощью цифровых денег

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

Одна из особенностей физических денег – их анонимность, то есть на них не указано, кто и когда их использовал. Некоторые системы по аналогии позволяют покупателю получать электронную наличность так, чтобы нельзя было определить связь между ним и деньгами. Это осуществляется с помощью схемы слепых подписей.

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

На рис. 5 приведена схема платежа с помощью цифровых денег.

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

• на жестком диске компьютера;

• на смарт-картах.

Разные системы предлагают разные схемы обмена. Некоторые открывают специальные счета, на которые перечисляются средства со счета покупателя в обмен на электронные купюры. Некоторые банки могут сами эмитировать электронную наличность. При этом она эмитируется только по запросу клиента с последующим ее перечислением на компьютер или карту этого клиента и снятием денежного эквивалента с его счета. При реализации же слепой подписи покупатель сам создает электронные купюры, пересылает их в банк, где при поступлении реаль-

ных денег на счет они заверяются печатью и отправляются обратно клиенту.

Наряду с удобствами такого хранения у него имеются и недостатки. Порча диска или смарт-карты оборачивается невозвратимой потерей электронных денег.

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

3. Деньги предъявляются эмитенту, который проверяет их подлинность.

4. В случае подлинности электронных купюр счет продавца увеличивается на сумму покупки, а покупателю отгружается товар или оказывается услуга.

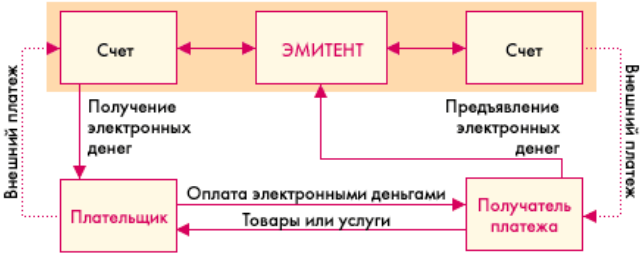

Рис. 5. Схема платежей с использованием электронных денег

Одной из важных отличительных черт электронных денег является возможность осуществлять микроплатежи. Это связано с тем, что номинал купюр может не соответствовать реальным монетам (например, 37 копеек).

Эмитировать электронные наличные могут как банки, так и небанковские организации. Однако до сих пор не выработана единая система конвертирования разных видов электронных денег. Поэтому только сами эмитенты могут гасить выпущенную ими электронную наличность. Кроме того, использование подобных денег от нефинансовых структур не обеспечено гарантиями со стороны государства. Однако малая стоимость транзакции делает электронную наличность привлекательным инструментом платежей в Интернете.

Наиболее известными платежными системами в России являются Webmoney, «Яндекс.Деньги», CyberPlat, Mondex и др.

4.4. Кредитные системы

Интернет-кредитные системы являются аналогами обычных систем, работающих с кредитными картами. Отличие состоит в проведении всех транзакций через Интернет и, как следствие, в необходимости дополнительных средств безопасности и аутентификации.

В проведении платежей через Интернет с помощью кредитных карт участвуют:

1. Покупатель. Клиент, имеющий компьютер с web-браузером и доступом к Интернету.

2. Банк-эмитент. Здесь находится расчетный счет покупателя. Банк-эмитент выпускает карточки и является гарантом выполнения финансовых обязательств клиента.

3. Продавцы. Под продавцами понимаются сервера Электронной Коммерции, на которых ведутся каталоги товаров и услуг и принимаются заказы клиентов на покупку.

4. Банки-эквайеры. Банки, обслуживающие продавцов. Каждый продавец имеет единственный банк, в котором он держит свой расчетный счет.

5. Платежная система Интернета. Электронные компоненты, являющиеся посредниками между остальными участниками.

6. Традиционная платежная система. Комплекс финансовых и технологических средств для обслуживания карт данного типа. Одной из основных задач, решаемых платежной системой, является обеспечение использования карт как средства платежа за товары и услуги, пользование банковскими услугами, проведение взаимозачетов и т.д. Участниками платежной системы являются физические и юридические лица, объединенные отношениями по использованию кредитных карт.

7. Процессинговый центр платежной системы. Организация, обеспечивающая информационное и технологическое взаимодействие между участниками традиционной платежной системы.

8. Расчетный банк платежной системы. Кредитная организация, осуществляющая взаиморасчеты между участниками платежной системы по поручению процессингового центра.

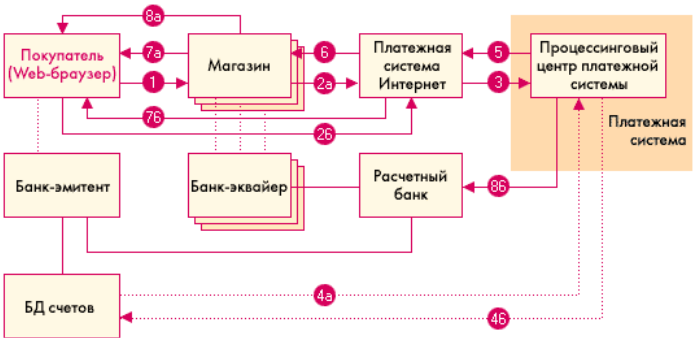

Рис. 6. Схема платежей в кредитной системе

Рассмотрим все этапы, представленные на данной схеме.

1. Покупатель в электронном магазине формирует корзину товаров и выбирает способ оплаты «кредитная карта».

2. Далее параметры кредитной карты (номер, имя владельца, дата окончания действия) должны быть переданы платежной системе Интернет для дальнейшей авторизации. Это может быть сделано двумя способами:

• через магазин, то есть параметры карты вводятся непосредственно на сайте магазина, после чего они передаются платежной системе Интернет (2а);

• на сервере платежной системы (2б).

Очевидны преимущества второго пути. В этом случае сведения о картах не остаются в магазине и, соответственно, снижается риск получения их третьими лицами или обмана продавцом. И в том, и в другом случае при передаче реквизитов кредитной карты все же существует возможность их перехвата злоумышленниками в сети. Для предотвращения этого данные при передаче шифруются.

1. Платежная система Интернета передает запрос на авторизацию традиционной платежной системе.

2. Последующий шаг зависит от того, ведет ли банк-эмитент online базу данных (БД) счетов. При наличии БД процессинговый центр передает банку-эмитенту запрос на авторизацию карты (4а) и затем (4б) получает ее результат. Если же такой базы нет, то процессинговый центр сам хранит сведения о состоянии счетов держателей карт, стоп-листы и выполняет за-

просы на авторизацию. Эти сведения регулярно обновляются банками-эмитентами.

1. Результат авторизации передается платежной системе.

2. Магазин получает результат авторизации.

3. Покупатель получает результат авторизации через магазин (7а) или непосредственно от платежной системы Интернет (7б).

4. При положительном результате авторизации:

• магазин оказывает услугу или отгружает товар (8а);

• процессинговый центр передает в расчетный банк сведения о совершенной транзакции (8б). Деньги со счета покупателя в банке-эмитенте перечисляются через расчетный банк на счет магазина в банке-эквайере.

Для проведения подобных платежей в большинстве случаев необходимо специальное программное обеспечение. Оно может поставляться покупателю, продавцу и его обслуживающему банку.

4.5. Примеры платежных систем

4.5.1. WebMoney Transfer

WebMoney Transfer представляет собой систему мгновенных расчетов электронными деньгами (WebMoney) через Интернет, которая позволяет производить платежи и переводы денежных средств в режиме реального времени. По своей сути WebMoney – «это цифровые титульные знаки, хранящиеся на информационном накопителе и дающие владельцу право оплачивать услуги и товары и производить денежные переводы в Сети». Проект принадлежит «ВМ Центру» – некоммерческой организации, учрежденной на основе добровольных взносов.

Общение пользователей системы (как владельцев магазинов, так и покупателей) друг с другом производится с помощью WebMoney Keeper.

WebMoney Keeper – программа, предназначенная для широкого применения пользователями системы WebMoney Transfer и позволяющая хранить, накапливать, принимать и переводить электронные деньги. Такие программы обычно называют **«электронными кошельками»** (но в данном случае это выра-

жение несколько некорректно, т.к. WebMoney Keeper позволяет пользователю создавать сразу несколько «кошельков»).

WebMoney Keeper можно получить бесплатно в виде самораспаковывающегося инсталляционного архива на сайте www.webmoney.ru. После инсталляции программы WebMoney Keeper автоматически регистрирует пользователя в системе WebMoney. После регистрации пользователю присваивается персональный идентификатор из 13 знаков, позволяющий использовать программу и работать в системе. Кроме того, пользователь самостоятельно назначает пароль для запуска программы.

После выполнения данных процедур WebMoney Keeper автоматически открывает клиенту «первый кошелек» (специальный счет) для хранения электронных денег. Пользователь может свободно распоряжаться своим кошельком или кошельками, т.е. создавать новые, удалять старые, менять свойства, просматривать историю транзакций и т.д. После получения кошелька клиент может взаимодействовать с другими пользователями системы WebMoney Transfer.

Типы платежей

В системе WebMoney Transfer возможны два типа платежей: обычный и двухфазовый.

Обычный платеж рекомендуется для оплаты информации или услуг, т.е. для товара, не требующего физической доставки. Покупатель оплачивает товар. При этом из его кошелька сумма, равная стоимости товара, переводится в кошелек продавца. Затем продавец производит поставку.

Двухфазовый платеж рекомендуется для оплаты товара, требующего доставки. Он состоит из двух фаз:

1. Покупатель оплачивает товар, резервируя в своем кошельке сумму, равную его стоимости, и самостоятельно определяя пароль транзакции.

После этого продавец получает уведомление от покупателя о том, что необходимая сумма зарезервирована на счете клиента, и информацию о доставке.

2. Далее возможны несколько сценариев развития ситуации:

• если покупатель доволен сроками доставки и качеством товара, он сообщает продавцу или его агенту пароль транзакции. Продавец или его агент в присутствии покупателя сверяет пароль транзакции через программу WebMoney Keeper. Затем зарезервированная сумма из кошелька покупателя поступает в кошелек продавца;

• если покупатель не удовлетворён заказом или выполнением условий поставки, он отказывается принять товар. Тогда по истечении срока доставки зарезервированная сумма разблокируется и становится доступна для нового использования покупателем.

Основные функции WebMoney Keeper:

1. Пользователь может принять (или отказаться принять) электронные деньги, переведенные другим пользователем системы.

2. Пользователь может перевести свои электронные деньги другому пользователю системы (частным лицам, компаниям, магазинам).

3. Пользователь может перевести электронные деньги на банковский счет, с последующим переводом в любую валюту.

4. Пользователь может перевести любую валюту в электронные деньги.

5. WebMoney Keeper поддерживает создание кошельков специально для одной валюты.

Например:

Если создать Z-кошелек и наполнить его долларами США, то с него можно отправить безналичный банковский перевод только в долларах США. На Z-кошельке 1WM=1USD.

Если же создать R-кошелек для хранения российских рублей, то с кошелька будет возможен безналичный банковский перевод только в российских рублях. На R-кошельке 1WM=1RUR.

В таких случаях перевод и получение денежных средств допустимы только между однотипными кошельками пользователей системы.

Для совершения сделок пользователю необходимо сообщить партнеру номер своего кошелька, после чего партнер сможет перевести ему на кошелек электронные деньги (пользова-

тель может отказаться их принять). При этом исключается возможность изъятия денег из кошелька пользователя по его номеру с удаленного компьютера. Более того, возможно создание кошелька для совершения отдельной сделки, после которой он удаляется.

Все номера кошельков пользователя хранятся в «общем файле». Этот файл можно спрятать в любом месте памяти компьютера или хранить на съемном накопителе (дискете, лазерном диске и т.д.). Поскольку при входе в WebMoney Keeper необходимо указать место расположения «общего файла», очевидно, что постороннему лицу будет очень затруднительно даже просто запустить программу.

WebMoney Keeper также предоставляет клиенту достаточную степень анонимности (если она необходима). Например, если пользователь нуждается в максимальной анонимности, то при открытии кошельков он может не указывать никаких данных о себе, а после проведения необходимых транзакций удалить инсталляцию WebMoney Keeper. Данные о транзакциях пользователя, зашифрованные его ключом, исключающим изменения, некоторое время хранятся в сертификационном центре системы.

WebMoney Keeper достаточно удобен и прост в эксплуатации. Интерфейс построен с использованием основных стандартов операционной системы Microsoft Windows. Удобной также является электронная оплата товара с помощью технологии Drag-and-drop.

Если настройки web-магазина допускают возможность операций по технологии Drag-and-Drop (например, в оформлении «витрины» присутствует значок «касса»), пользователь может произвести оплату простым перетаскиванием иконки из нижнего правого угла панели задач Microsoft Windows на соответствующий значок страницы («касса»). При этом программа WebMoney Keeper самостоятельно определяет сумму оплаты товара или услуги и переводит ее с активного кошелька пользователя на счет магазина.

Пополнение кошелька можно выполнить несколькими путями:

1. Перевести доллары США с любого банковского счета на расчетный счет IMTB Inc. (USA) с указанием номера кошелька, после чего доллары будут автоматически конвертированы в электронные деньги и зачислены на указанный кошелек.

2. Перевести российские рубли через любое отделение СБЕРБАНКА РФ на расчетный счет АНО «ВМ-ЦЕНТР» с указанием номера кошелька. После чего, как и в первом случае, рубли будут автоматически конвертированы в электронные деньги и зачислены на указанный кошелек.

3. С помощью программы WebMoney Keeper принять электронные деньги от других клиентов системы в качестве оплаты предоставленных услуг или товаров.

Таким образом, очевидно, что электронные деньги полностью конвертируемы с любыми валютами, используемыми в электронных расчетах.

4.5.2. «Яндекс.Деньги» / PayCash

В основе проекта «Яндекс.Деньги» лежит платежная система PayCash, высоко оцененная ведущими мировыми специалистами в области финансовой криптографии и поддержанная крупными российскими проектами электронной коммерции.

PayCash – проект банка «Таврический» и группы компании Алкор-Холдинг. Система PayCash позволяет множеству различных банков одновременно оперировать в одной электронной платежной системе, взаимодействуя на основе универсальных денежных единиц, принимаемых в оборот любым из этих банков. Кроме банков в системе существуют рядовые пользователи. Пользователями могут выступать юридические и физические лица или программные продукты, представляющие их (например, web-магазины). Все пользователи полностью равноправны с точки зрения банка.

Программное обеспечение

Все пользователи взаимодействуют друг с другом на основе специального программного обеспечения – «кошелька». Он обеспечивает хранение и накопление электронной наличности, а также пересылку электронных денег между пользователями системы.

Система PayCash предлагает своим пользователям два типа программного обеспечения «кошелек»: простой и полнофункциональный.

Простой кошелек предназначен для работ с одним банком системы и имеет две основные функции:

• при каждом запуске кошелек связывается с банком и получает все деньги, лежащие на счете;

• кошелек отдает и принимает электронные деньги с согласия владельца.

Полнофункциональный кошелек позволяет пользователю работать с неограниченным количеством банков системы PayCash. С его помощью кроме обычных функций можно осуществлять как управление деньгами на счетах системы PayCash, так и заводить множество платежных книжек для различных типов платежей.

Полнофункциональный кошелек системы PayCash способен одновременно управлять средствами, находящимися в нескольких банках. Для этого ему достаточно иметь некоторый набор сведений о новом банке (сетевой адрес банка, образцы цифровых подписей, сроки действия цифровых подписей и некоторые другие параметры), работающем в системе PayCash.

Управление счетом в банке возможно только при помощи того кошелька, с помощью которого он был создан. На счета с электронными деньгами распространяются те же правила, что и на обычные банковские счета.

Пользователь может самостоятельно изучить функциональные особенности кошелька PayCash, не рискуя потерять деньги. Для этого в системе предусмотрен «Демобанк», оперирующий демонстрационными деньгами («рублики», «долларики», «йенки» и т.д.). Для того чтобы положить «игрушечную наличность» на счет в «Демобанке», пользователь может обратиться к виртуальному банкомату. После этого клиент системы способен совершать покупки в демонстрационных магазинах.

Дополнительные технические характеристики системы PayCash:

1. Система поддерживает одновременное использование до 255 валют.

2. Сумма платежа может быть выражена практически любым числом с точностью до 0,001 копейки.

3. Применение особенностей построения системы PayCash позволяет пользователю кошелька получить денежные обязательства анонимно. Под анонимностью здесь предполагается, что ни банк, выпустивший обязательства, ни контрагент владельца кошелька, получивший их в качестве оплаты, не могут узнать владельца кошелька и номер счета, с которого были сняты деньги.

4. Для цифровых подписей используется алгоритм RSA с ключами в 1024 бит.

4.5.3. Система CyberPlat

Система CyberPlat была создана в 1997 г. как внутреннее подразделение банка «Платина». На сегодняшний день ОАО «CYBERPLAT.COM» – одна из ведущих российских интернет-компаний, предоставляющая инфраструктурные услуги для ведения электронной коммерции, приоритетными видами деятельности которой являются процессинг платежей и закрытый документооборот в режиме реального времени.

CyberPlat – это универсальная мультибанковская интегрированная система платежей в Интернете, которая обеспечивает весь спектр финансовых услуг – от микроплатежей до межбанковских расчетов.

Основные свойства системы CyberPlat:

Интегрированность – система объединяет различные инструменты для ведения бизнеса в сети Интернет:

• CyberCheck – подсистема обслуживания транзакций класса business-to-business с элементами электронного документооборота для клиентов, зарегистрированных в CyberPlat;

• CyberPOS – подсистема обслуживания платежей по пластиковым картам международных и российских платежных систем, ориентированная на услуги business-to-consumer и не требующая регистрации покупателя в системе CyberPlat;

• Internet-Banking – управление счетом в банке-участнике системы через Интернет.

Мультибанковость – система CyberPlat допускает участие в ней неограниченного количества банков, открыта для

взаимодействия с любыми другими платежными системами и в отличие от многих из них обеспечивает поддержку множества процессинговых центров.

Универсальность – система позволяет использовать различные платежные инструменты: пластиковые карты международных и российских платежных систем, в том числе Visa, Europay, Diners Club, JCB, American Express, Union Card, единые карты e-port, а также платежи непосредственно с банковских счетов плательщиков в банках-участниках системы на любой банковский счет, в том числе внешний.

CyberCheck – подсистема обслуживания транзакций клиентов-покупателей, зарегистрированных в системе интернет-платежей CyberPlat. CyberCheck обеспечивает конфиденциальность, надежность и юридическую чистоту взаимодействия сторон, а также полное отсутствие отказов от заявленных платежей. Это реализуется механизмами поддержки электронного документооборота с применением имеющей юридическую силу электронной цифровой подписью с длиной ключа 512 бит. Благодаря перечисленным свойствам, подсистема используется в схемах класса business-to-business.

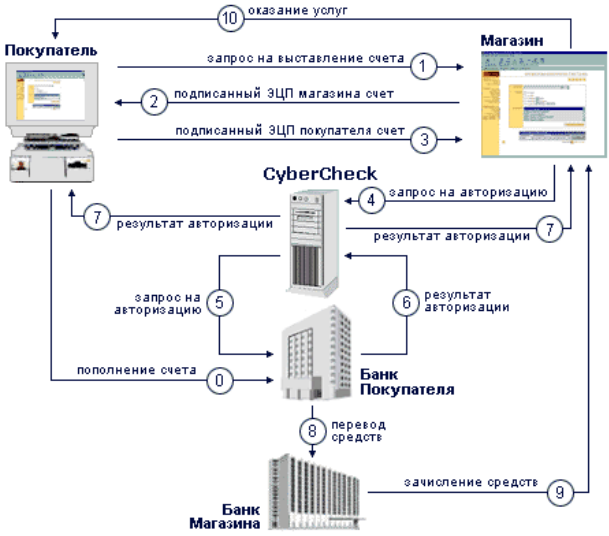

Рис. 7. Online покупка и проведение платежа

Технология CyberCheck с открытием счета в Банке-Участнике системы:

1. Покупатель через Интернет подключается к web-серверу Магазина, формирует корзину товаров и направляет Магазину запрос на выставление счета.

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

• наименование товара (услуги);

• стоимость товара (услуги);

• код магазина;

• время и дату совершения операции.

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

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

4. Подписанный двумя ЭЦП (Магазином и Покупателем) чек направляется Магазином на сервер CyberCheck для авторизации.

5. CyberCheck производит проверку подписанного чека:

• проверяет наличие в Системе Магазина и Покупателя;

• проверяет ЭЦП Покупателя и Магазина;

• сохраняет копию чека в базе данных CyberCheck.

В случае положительного результата проверки чек отправляется в Банк Покупателя (Банк-Участник системы, в которым ведутся счет клиента-Покупателя в системе CyberPlat®) для проведения платежа.

Банк Покупателя проверяет остаток и лимиты средств на счете Покупателя. В результате проверки формируется разрешение или запрет проведения платежа. Банк Покупателя передает результат авторизации CyberCheck.

6. При разрешении платежа:

• CyberCheck передает Магазину разрешение на оказание услуги (отпуск товара);

• Банк Покупателя переводит денежные средства со счета Покупателя в Банк Магазина;

• Банк Магазина зачисляет денежные средства на счет Магазина;

• Магазин оказывает услугу (отпускает товар).

7. При запрете платежа:

• CyberCheck передает Магазину отказ от проведения платежа;

• Покупатель получает отказ с описанием причины.

Покупатель полностью контролирует процесс совершения покупки.

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

Технология CyberCheck при обслуживании держателей банковских пластиковых карточек аналогична технологии CyberCheck с открытием счета в Банке-Участнике системы за исключением предварительной регистрации держателя пластиковой карточки:

1. Держатель пластиковой карты: VISA, Eurocard/MasterCard, Diners Club, JCB (Покупатель) регистрируется в платежной системе CyberPlat.

2. При регистрации Покупатель указывает:

• Свои персональные данные (Фамилия, имя, отчество, паспортные данные, адрес электронной почты, почтовый адрес, телефон)

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

Информация о карточке передается в защищенном виде только на сервер CyberCheck компании CYBERPLAT.COM при регистрации Покупателя и не предоставляется Магазину при операциях Покупателя.

Безопасность CyberCheck

Подсистема CyberCheck осуществляет контроль над каждым этапом проведения платежа в режиме online. Очень важно то, что CyberCheck полностью отвечает требованиям российского законодательства, легализуя осуществляемые платежи и сохраняя у каждого из участников комплект электронных доку-

ментов, которые заверяются электронными цифровыми подписями (ЭЦП) сторон, имеют юридическую силу (ст. 160, п. 2 Гражданского Кодекса РФ) и пригодны для разбирательства в обычном суде. Такая мера значительно облегчает разрешение конфликтов между продавцами и покупателями. В подсистеме CyberCheck используется асимметричный алгоритм шифрования RSA с использованием 512-битного ключа. Само это число ни о чем не говорит. Но если учесть, что существующие сейчас технические средства позволяют взламывать подпись, защищенную ключом, не более, чем из 48–52 разрядов, то многое прояснится. Еще долгие годы не удастся создать практического метода расшифровки.

Высокая безопасность и безусловная гарантия идентификации клиента при помощи CyberCheck позволяют проводить взаимные расчеты между корпоративными участниками системы CyberPlat, банками, фирмами и организациями любых размеров и форм собственности по схеме business-to-business. Появляется возможность разделения стадий оформления сделок и расчетов по ним. Клиенты могут использовать систему CyberPlat® для оперативного заключения договоров, расчеты по которым не обязательно пойдут через Интернет. Такой механизм позволяет обеспечить клиентам максимальный выбор схем взаиморасчетов, оптимальных с их точки зрения платежных инструментов.

CyberPOS – подсистема обслуживания платежей по пластиковым картам международных и российских платежных систем, в том числе Visa, EuroCard/MasterCard, Diners Club, JCB, Union Card, а также единых карт e-port.

Услугами CyberPOS может воспользоваться любой держатель пластиковой карты, причем данные о карточке и ее владельце становятся известными только CyberPOS и недоступны ни для интернет-магазина, в котором оплачивается покупка, ни, тем более, для третьих лиц, поскольку все данные передаются по каналу, защищенному с помощью протокола SSL.

В системе CyberPOS предусмотрены два варианта платежей по банковским картам: стандартный платеж и платеж подтвержденной картой (технология CyberPlatPay). Стандартный платеж не требует регистрации клиента в системе CyberPlat, в то время как для платежа подтвержденной картой необходимо за-

регистрироваться и получить код подтверждения. Регистрация в системе CyberPlat предоставляет клиенту-покупателю ряд преимуществ, в том числе возможность совершать покупки в интернет-магазинах, требующих платежа подтвержденной картой, а также отсутствие ограничений на суммы платежей при совершении покупок.

Безопасность CyberPOS

Опросы показали, что «90 % покупателей, оплачивающих покупки пластиковыми картами, опасаются, что номер карты попадет к посторонним». CyberPlat, благодаря подсистеме CyberPOS и используемому в ней протоколу SSL, полностью снимает эту проблему. Движение денежных средств через подсистему CyberPOS происходит только в закрытых межбанковских сетях, а реквизиты клиента известны только CyberPOS и никому более, что гарантирует недосягаемость Вашего банковского счета для злоумышленников и недобросовестных интернет-торговцев. Ваши деньги попадут именно к тому, кому Вы хотите их заплатить посредством CyberPlat. Запрос из магазина и ответ идет в шифрованном виде по стандарту выделенного сообщения (SSL) в Интернете, а сам номер карты вводится клиентом непосредственно в подсистему CyberPOS и, следовательно, становится известен только банку. Взлом же защиты банковской системы очень маловероятен – это гораздо сложнее, чем, например, совершить вооруженный налет на хранилище банка. Для магазина такое распределение ролей также выгодно, избавляя от необходимости создания собственной системы хранения номеров карт клиентов.

4.6. Правовая природа электронных денег

Многие разработчики систем электронных денег утверждают, что их системы аналогичны по свойствам наличным деньгам. Исходя из этого, можно сделать вывод, что данные системы могут использоваться аналогично наличным деньгам. Вместе с тем анализ действующего законодательства, в частности положений Конституции Российской Федерации, Гражданского кодекса Российской Федерации, Федерального закона

«О Центральном банке Российской Федерации (Банке России)», позволяет сделать несколько иные выводы.

В соответствии со ст. 75 Конституции Российской Федерации официальной денежной единицей (валютой) Российской Федерации является рубль. Аналогична норма содержится в ст. 27 Федерального закона «О Центральном банке Российской Федерации (Банке России)», которая прямо запрещает введение на территории Российской Федерации других денежных суррогатов. В соответствии со ст. 29 Федерального закона «О Центральном банке Российской Федерации (Банке России) банкноты (банковские билеты) и монета Банка России являются единственным законным средством платежа на территории Российской Федерации (аналогичная норма содержится в ст. 140 ГК РФ). Банк России монопольно осуществляет эмиссию денег и организует их обращение. Банкноты и монета являются безусловными обязательствами Банка России и обеспечиваются всеми его активами. Банкноты и монета Банка России обязательны к приему по нарицательной стоимости при всех видах платежей, для зачисления на счета, во вклады и для перевода на всей территории Российской Федерации.

Таким образом, законодательство Российской Федерации содержит четкий запрет эмиссии наличных денег любыми лицами и организациями, за исключением Банка России, что не позволяет рассматривать электронные деньги с точки зрения аналога наличных денег.

Вместе с тем возможен иной подход к правовой природе электронных денег, базирующийся на нормах обязательного права. Правовая конституция электронных денег отлична от конституции сходных правовых институтов, регулируемых Гражданским кодексом, что проявляется при их сопоставлении.

1. Электронные деньги и договор банковского вклада (Глава 44 ГК РФ). Электронные деньги не могут рассматриваться в качестве банковского вклада до востребования, поскольку существенным условием договора банковского вклада является выплата процентов (ст. 834 ГК РФ), которое в случае электронных денег не соблюдается.

2. Электронные деньги и формы расчетов (Глава 46 ГК РФ). К электронным деньгам представляется невозможным

применение комплекса норм, регулирующих безналичные расчеты, поскольку при эмиссии электронных денег клиенту не открывается банковский счет, что является существенным признаком безналичных расчетов в соответствии со ст. 861 (3) ГК РФ. Даже если рассматривать электронные деньги в качестве разновидности перевода денежных средств без открытия банковского счета, то в данном случае, во-первых, отсутствует платежный документ, служащий основанием перевода, а во-вторых – банковские реквизиты получателя денежных средств.

3. Электронные деньги и договор займа (Глава 42 ГК РФ). Наиболее близкой к электронным деньгам правовой конституцией является конституция договора беспроцентного займа, хотя она имеет два существенных недостатка применительно к особенностям эмиссии и обращения электронных денег:

• беспроцентный займ не может предоставляться кредитной организацией, поскольку ее кредитные операции регулируются кредитным договором, предусматривающим платность (ст. 819), тогда как наиболее активными эмитентами электронных денег за рубежом являются именно банки;

• поскольку срок обращения электронных денег является неограниченным, может использоваться только конституция беспроцентного займа со сроком возврата, определенным моментом востребования, а в соответствии со ст. 810 в этом случае сумма займа должна быть возвращена заемщиком в течение тридцати дней со дня предъявления заимодавцем требования об этом, если иное не предусмотрено договором (последнее осложнено технологическими особенностями электронных денег, в первую очередь в анонимных системах).

Необходимо учитывать, что механизм правового регулирования систем электронных денег имеет двоякий характер: с одной стороны, правоотношения, возникающие при эмиссии и обращении электронных денег в рамках частных систем, являются имущественными (денежными) и основанными на равенстве их участников, т.е. гражданско-правовыми, с другой стороны, данные отношения испытывают воздействие публично-правового характера, осуществляемое центральным банком в рамках банковского регулирования и надзора. Гражданско-

правовые аспекты эмиссии и обращения электронных денег основаны на следующих принципах:

• электронные деньги по своей правовой природе являются денежными обязательствами эмитента, выполняющими субститутивную функцию в отношении денежных обязательств держателя электронных денег перед третьими лицами, возникающих в результате совершаемых им сделок;

• размер денежных обязательств эмитента отражает в виде информации, хранимой на технических средствах (на микропроцессорных картах или картах памяти компьютера);

• при совершении платежа составляется электронный документ, содержащий сумму денежного обязательства эмитента;

• основанием возникновения денежных обязательств эмитента является договор, заключаемый между эмитентом и держателем электронных денег.

При описании обязательственно-правовой модели электроны денег будет использован именно данный термин, а не термин «предоплаченный финансовый продукт» (ПФП), который используется в Указании Банка России от 3 июля 1998 г. № 277-У «О порядке выдачи регистрационных свидетельств кредитным организациям-резидентам на осуществление эмиссии предоплаченных финансовых продуктов», имеющий скорее экономический характер, определяющий электронные деньги в отношении денежных обязательств эмитента.

Для удобства анализа представляется целесообразным разбить все правоотношения, касающиеся электронных денег, на три группы:

1) эмиссия электронных денег порождает денежные обязательства эмитента перед держателями электронных денег;

2) обращение электронных денег, в результате которого происходит переход прав требования к эмитенту по его денежным обязательствам от держателей электронных денег к третьим лицам;

3) погашение электронных денег – исполнение эмитентом денежных обязательств перед держателями электронных денег или третьими лицами в наличной или безналичной денежной форме.

4.6.1. Эмиссия электронных денег

Условиями эмиссии электронных денег являются:

1. Заключение договора между эмитентом и будущим держателем электронных денег – клиентом эмитента. Заключаемые договоры по своему характеру всегда являются договорами присоединения (ст. 428 ГК РФ) и, как правило, публичными договорами (ст. 426 ГК РФ). Заключение данных договоров может производиться как при физическом присутствии клиента (например, при получении микропроцессорной карты), так и электронным способом (например, с применением сети Интернет), в том числе в результате совершения клиентом определенных действий (например, путем использования программного обеспечения). Существенные условия договора с клиентом зависят от особенностей используемых технических средств и совершаемых клиентом сделок. Вместе с тем в качестве общей черты можно указать на необходимость отражения процедуры удостоверения прав сторон на использование технического средства и совершения сделок.

2. Перевод (взнос) клиентом денежных средств на счет эмитента в качестве предварительной оплаты (покрытия).

3. Предоставление технических средств. Применительно к системам электронных денег с использованием смарт-карт можно говорить о выдаче карты как о юридическом факте, порождающем эмиссию электронных денег в пользу клиента, а не об условии эмиссии. В случае же использования сетевых продуктов об эмиссии можно говорить только с момента физического перевода электронных денег в компьютер клиента, в связи с чем предоставление технического средства осуществляется до эмиссии, а юридическим фактом, порождающим эмиссию, является запрос клиента на определенную сумму. В данном случае рассматривается предоставление технического средства в качестве последнего условия эмиссии, хотя в случае использования сетевых продуктов оно может иметь место и до перевода (взноса) клиентом денежных средств на счет эмитента.

В том случае, если эмитентом является кредитная организация, эмиссия может производиться только после получения регистрационного свидетельства Банка России в соответствии с указанием № 277-У. Данное Указание не содержит норм, уста-

навливающих правила совершения сделок с использованием электронных денег, но вместе с тем определяет требования к документам, представляемым в Банк России для получения регистрационного свидетельства, основным из которых является положение о порядке эмиссии предоплаченного финансового продукта, включающее себя:

• проспект эмиссии предоплаченного финансового продукта;

• правила осуществления расчетов по операциям с применением предоплаченного финансового продукта, связанным с приобретением, отчуждением и хранением заключенной в предоплаченном финансовом продукте стоимости;

• проекты договоров между участниками расчетов по операциям с использованием предоплаченного финансового продукта.

Надлежащая обработка последних является особенно необходимой с точки зрения четкого распределения ответственности и рисков.

4.6.2. Обращение электронных денег

Юридически обращение электронных денег происходит путем уступки требования к эмитенту в соответствии со ст. 382 (1) ГК РФ. В данном случае уступка требования рассматривается в качестве основной формы обращения электронных денег, хотя для его юридического обоснования может использоваться также институт исполнения обязательств третьим лицом (ст. 313 ГК РФ). Предполагается, что обращение электронных денег осуществляется, как правило, без участия эмитента, хотя на практике реализуются и схемы, предусматривающие авторизацию (получение подтверждения эмитента на совершение сделки). При технической реализации систем необходимо учитывать, что в соответствии со ст. 382 (2) ГК РФ для перехода к другому лицу прав кредитора не требуется согласия должника, если иное не предусмотрено законом или договором. Соответственно, если условием перехода прав требования от владельца электронных денег к третьим лицам является авторизация, то данное условие должно отражаться в договоре между эмитентом и держателем электронных денег. В соответствии со ст. 385 ГК

РФ кредитор, уступивший требование другому лицу, обязан передать ему документы, удостоверяющие право требования, и сообщить сведения, имеющие значение для осуществления требований. Применительно к обращению электронных денег данное требование может считаться соблюденным, поскольку право требования к эмитенту на практике подтверждается путем проверки аналога собственноручной подписи эмитента под электронным документом, содержащим сумму обязательства, при предъявлении электронных денег к оплате.

Еще один вопрос, который возникает в связи с использованием электронных денег при совершении сделок приобретения товаров (услуг): влечет ли за собой передача электронных денег предприятию торговли (услуг) прекращение денежного обязательства по основному договору (купли-продажи и т.п.). В этой связи необходимо обратиться к ст. 407 (1) ГК РФ, предусматривающей то, что обязательство прекращается полностью или частично по основаниям, предусмотренным Гражданским кодексом, иными правовыми актами или договором. При отсутствии специальных регулирующих норм законодательства окончательность в случае использования электронных денег может быть достигнута только путем включения соответствующих условий в договор эмитента с держателем электронных денег и предприятием торговли (услуг). Таким образом, окончательность не является существенным условием систем электронных денег, но может использоваться для повышения привлекательности системы для клиентов.

Последний вопрос, имеющий отношение к обращению электронных денег: его связь с совершаемыми сделками (сделки купли-продажи в рамках систем электронной коммерции). Наиболее эффективной является следующая модель обращения электронных денег:

• «согласие продавца на использование электронных денег для исполнения денежного обязательства покупателя (при размещении на веб-сайте продавца соответствующей информации или логотипа системы электронных денег);

• совершение сделки и возникновение денежного обязательства клиента;

• составление электронного документа, содержащего денежное обязательство эмитента, и направление его продавцу (после авторизации эмитентом, если требуется);

• подтверждение продавцом получения электронного документа, содержащего денежное обязательство эмитента, следствием чего является прекращение денежного обязательства клиента, если это предусмотрено условиями сделки».

4.6.3. Погашение электронных денег

Погашение электронных денег означает исполнение эмитентом своего денежного обязательства перед держателем электронных денег. Юридическим фактом, порождающим обязанность эмитента по исполнению, является совершение держателем электронных денег действий, свидетельствующих о реализации своего требования. Содержание данных действий зависит от особенностей технического средства держателя электронных денег, но ключевым моментом является предъявление эмитенту электронного документа, содержащего его денежное обязательство, подписанного аналогом собственноручной подписи эмитента. В том случае, если эмитентом проводится авторизация при совершении сделки, обязанность эмитента исполнить денежное обязательство возникает не с момента предъявления им электронного документа, а с момента авторизации в отношении будущего предъявления.

Погашение электронных денег может производиться как в наличной, так и в безналичной форме в течение времени, определяемого договором с эмитентом. Денежное обязательство эмитента считается прекращенным полностью или частично, в зависимости от размера предъявленного клиентом денежного требования. В соответствии со ст. 408 ГК РФ кредитор, принимая исполнение, обязан по требованию должника выдать ему расписку в получении исполнения полностью или в соответствующей части. Данное требование реализуется в системах электронных денег через регистрацию совершаемых операций и их подтверждение путем обмена электронными документами.

4.7. Правовая природа «Яндекс.Деньги» и WebMoney

Правовую природу электронных денег удобнее всего изучать на примере наиболее успешных и распространенных в России систем – «Яндекс.Деньги» и WebMoney. Как упоминалось выше, законодательство РФ не признает за «электронной наличностью» статуса денег как таковых.

Таким образом, применение терминов «электронные деньги» и «электронная наличность» с юридической точки зрения является чисто условным, хотя с технической и экономической – вполне обоснованным. По этой же причине системы электронных денег используют разнообразные механизмы для того, чтобы реализуемые в них взаиморасчеты влекли за собой юридические последствия. Тем не менее существуют отдельные универсальные нормы, без которых юридически значимые денежные транзакции через Интернет были бы невозможны в принципе.

Основополагающими нормативными актами для электронных платежных систем является Гражданский Кодекс РФ. Ст. 160 ГК допускает при заключении сделок использование не собственноручной подписи, а ее аналога. В соответствии со ст. 434 письменный договор может быть заключен не только путем подписания сторонами одного документа, но и путем обмена документами посредством электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору.

Юридическая сила электронной подписи основывается на соглашении сторон, допускаемом Гражданским кодексом, а также законодательстве об электронной подписи.

Несмотря на то, что и «Яндекс.Деньги», и WebMoney были бы невозможны без признания законодательством электронной подписи в качестве средства заверения аутентичности документа, юридические механизмы, лежащие в их основе, различны.

WebMoney – достаточно «разносторонняя» в юридическом плане система. Она не привязана к национальному законодательству и позиционируется разработчиками как всемирная и универсальная. Поэтому для разных поддерживаемых

типов «виртуальной валюты»: WM-R (рубли), WM-Z (доллары) и так далее – WebMoney предлагает несколько различающиеся решения.

Для WM-R юридический «фундамент» системы сформулирован следующим образом. Некое юридическое лицо (в данном конкретном случае это АНО «ВМ-Центр») эмитирует векселя номиналом 1 рубль и большим сроком платежа (01.09.2011). Конкретный срок погашения особого значения не имеет – при его приближении «морально устаревшие» векселя легко заменить новыми, с более поздними сроками.

На сайте WebMoney выложено предложение приобрести данные векселя, в котором предусматривается, что выполнение определенных действий, а именно: установка ПО для ведения счета в векселях («кошелька» WebMoney Keeper) и введение клиентом в систему соответствующего количества денежных средств автоматически означает его согласие заключить договор на изложенных в оферте условиях.

Разумеется, никаких векселей пользователю не передается, поскольку на том же сайте есть еще одна оферта – на этот раз договора хранения векселей.

Далее специальными соглашениями аппаратно-программный комплекс WebMoney признается системой фиксации актов приема-передачи векселей.

Таким образом, все движения электронных денег в WebMoney, с юридической точки зрения, представляют собой передачу соответствующего количества векселей от одного участника системы к другому (либо их приобретение/выкуп при вводе/выводе денег). Векселя находятся у хранителя (АО «Гарантийное агентство»), а необходимости в физической передаче векселей нет – просто ведется учет, какое количество векселей какому участнику системы принадлежит.

Функция же программно-аппаратных средств системы WebMoney состоит в транслировании сообщений о передаче прав собственности на векселя таким образом, чтобы эти сообщения имели юридическое значение. В принципе, вместо векселей могут использоваться и другие ценные бумаги.

Эта юридическая «оболочка» предназначается, разумеется, в первую очередь, для интернет-магазинов, которым вирту-

альные деньги надо как-то проводить по бухгалтерии. Для покупателей же здесь наиболее важен тот момент, что WebMoney юридически не защищает плательщика от неисполнения обязательств со стороны продавца. Хотя в этой системе предусмотрено множество мероприятий для предотвращения подобных случаев: «идентификация личности», черные списки, арбитраж и т.п. Однако юридической «управы» на нерадивого контрагента в WebMoney не найти.

Вообще защитить плательщика от недобросовестного продавца или поставщика услуг является возможным. Правда, тут стоит оговориться, что защита эта может быть хороша настолько, насколько эффективно обращение в суд. То есть сама платежная система полностью защитить плательщика не может – она лишь дает ему инструменты для отстаивания своих интересов в суде.

Систему PayCash, на основе которой построены «Яндекс.Деньги», лет тридцать-сорок назад назвали бы «выдающимся достижением отечественной науки и техники». В принципе, она действительно заслуживает подобной характеристики, вот только такие эпитеты сейчас не в ходу. Разработчики существенно модифицировали и дополнили технологию online наличности, изначально разработанную известным криптографом Дэвидом Чаумом. Эти модификации придали системе такие, казалось бы, несовместимые качества, как высокая степень анонимности плательщика и взаимная защищенность участников сделки и банка от мошенничества. Чтобы разобраться, каким именно образом достигается такой результат, недостаточно лишь юридического аспекта, придется слегка затронуть и математику.

Чтобы изначально расставить точки над «i», следует оговориться, что система «Яндекс.Деньги» (она же PayCash) является, по всей видимости, единственной настоящей системой электронной наличности, действующей в нашей стране. Все прочие системы основаны на более традиционных механизмах, выросших из алгоритмов банковских и карточных транзакций. Принципиальное отличие электронной наличности от упомянутых схем заключается в применении электронных монет (купюр).

Разумеется, у любого, кто попытается представить себе электронные монеты, сразу же возникнет вопрос: как их можно использовать в экономическом обороте? Ведь фундаментальное свойство денег состоит в том, что их невозможно изготовлять «в домашних условиях», а файлы (которыми, по сути, и являются электронные монеты) можно легко копировать.

На самом деле, обойти эту проблему просто – достаточно сделать монеты одноразовыми, то есть использовать каждую монету лишь в одном платеже. Схема платежа тогда будет такой: банк-эмитент выдает (в смысле, пересылает по Интернету) плательщику некоторое количество монет – в момент платежа плательщик передает их (опять же по Интернету) продавцу – продавец передает монеты в банк. Банк проверяет, не были ли эти монеты уже использованы. Если были, банк отказывает в проведении платежа. Если не были, банк перечисляет продавцу на счет уплаченную сумму и считает монеты использованными.

Анонимность платежа в данной системе обеспечивается методом «слепой подписи» Чаума. Монеты генерируются самим плательщиком на основе его секретного ключа (разумеется, не вручную, а с помощью специальной программы-клиента), а затем «вслепую» подписываются банком. Подпись «вслепую» означает, что при окончательной генерации монеты банк не знает ее реквизитов (они известны только плательщику), ему известен лишь ее номинал, который он и подтверждает своей электронной подписью.

Кроме того, в отличие от обычной наличности, каждая «денежка» в «Яндекс.Деньгах» намертво привязывается к контракту, в силу которого она передается. Делается это примерно по той же технологии, что и обычная электронная подпись: хэш контракта (короткая уникальная информационная последовательность, получаемая на основе его содержания) подписывается ключом плательщика, на основе которого были сгенерированы монеты, а получившаяся подпись передается вместе с платежной книжкой на сумму контракта.

В отличие от оригинальной системы Чаума, в PayCash используются не монеты, а их модифицированные версии – так называемые «платежные книжки». Если в случае с монетой банк подтверждает своей подписью ее номинал, то в случае платеж-

ной книжки он подтверждает зачисляемую на нее сумму. Главным свойством платежной книжки является то, что ее владелец (то есть плательщик) самостоятельно (не зная секретного ключа банка) может легко генерировать книжки с такими же реквизитами, но с меньшей суммой. А вот увеличивать сумму плательщик может только с помощью слепой подписи банка.

Использование платежных книжек вместо монет имеет как положительные, так и отрицательные последствия. Положительным результатом является снижение стоимости транзакции. Действительно, платежная книжка является как бы «монетой переменного номинала». Это означает, что для платежа используется лишь одна такая «переменная монета» вместо нескольких в обычной схеме, плюс одна и та же книжка – «переменная монета» может использоваться множество раз. В результате сильно снижаются затраты машинных ресурсов как на стороне банка, так и на стороне плательщика (что ведет к повышению скорости транзакций), а сами транзакции кардинально дешевеют. Кроме того, появляется возможность проводить платежи даже с нецелыми долями самых мелких денежных единиц – номиналами виртуальной «мелочи» мы теперь не ограничены.

Отрицательным последствием введения платежных книжек является появление у каждой книжки платежной истории. У обычной монеты никакой истории быть не может – она используется лишь один раз. Книжка же может использоваться неограниченное количество раз (с учетом возможности ее пополнения), и все платежи, сделанные с ее помощью, могут быть увязаны друг с другом (но не с лицом, которому банк подписал книжку – его прямо установить нельзя). В принципе, с этим можно бороться, просто заводя в нужный момент новую книжку и прерывая таким образом платежную историю.

С юридической точки зрения, расчетные книжки (как и их предшественники – электронные монеты) – это обязательства банка выплатить соответствующие им суммы. Юридическая сила этих обязательств основывается на том, что они подписаны банком («слепая» подпись). В банковской практике такие платежные инструменты называются «предоплаченными финансовыми продуктами». Банк эмитирует обязательства в обмен на обычные денежные средства, передаваемые ему клиентом (бу-

дущим плательщиком). Размер обеспечения составляет 100 %, т.е. банк выпускает электронных денег ровно столько, сколько ему поступает обычных денег.

Итак, благодаря «слепой подписи», «Яндекс.Деньги» обеспечивают высокую степень анонимности платежей. Используя механизма платежных книжек и виртуальных счетов, обеспечивается юридическая сторона платежной системы. Из-за привязки каждого платежа к соответствующему контракту и рассылке электронных квитанций участникам сделки у плательщика всегда есть возможность подтвердить, что деньги за товар или услугу были им уплачены, и требовать надлежащего исполнения продавцом своих обязательств.

Без адекватного правового регулирования на государственном уровне нельзя говорить о едином электронном бизнес-пространстве, которое в настоящее время становится реальностью во многих странах.

4.8. Преимущества и недостатки электронных денег

Неоспоримыми преимуществами электронных денег являются:

– удобство, быстрота расчетов (операции в них происходят практически в режиме реального времени);

– легкий обмен и сопряженность с другими платежными системами;

– анонимность;

– долговечность (все деньги хранятся на нескольких независимых серверах, которые дублируют друг друга, храниться, таким образом, они могут бесконечно долго) и т.д.

Однако данная валюта имеет и недостатки:

– отсутствие устоявшегося правового регулирования (во многих странах по сегодняшний день отсутствует стабильное правовое регулирование безналичных средств);

– электронные деньги нуждаются в специальных инструментах хранения и обращения (терминалы, банкоматы, пластиковые карточки, сами платёжные системы);

– невозможность восстановить денежную стоимость средств владельца в случае уничтожения носителя электронных денег;

– недостаточная зрелость технологий защиты, что ведет к хищению электронных денег посредством инновационных методов.

Одной из существенных проблем, сдерживающих более активное развитие электронной коммерции, является несовершенство платежных online систем, число которых сегодня составляет несколько десятков. Несмотря на разнообразие, их можно разделить на четыре основные группы: кредитные карты, дебетовые схемы, цифровая наличность и интернет-банкинг.

Первые две группы систем хорошо известны в традиционной коммерции. Новинкой подобного рода является смарт-карта, представляющая собой миникомпьютер с процессором, памятью, программным обеспечением и системой ввода/вывода информации. Наличные цифровые деньги на базе смарткарт обеспечивают необходимый уровень конфиденциальности и анонимности, кроме того, не нужна связь с центром для подтверждения оплаты.

Цифровые наличные – это электронная платежная система, в которой роль денежных знаков выполняют специальные цифровые файлы очень больших чисел. В отличие от других платежных систем, эти файлы и есть сами деньги, а не записи о них. Они обеспечивают полную анонимность, так как не несут никакой информации о потратившем их клиенте. Наиболее известными компаниями, развивающими эту платежную систему, являются NetCash, Citibank, DigiCash, Mondex.

Главным тормозом на пути применения подобных систем является неопределенный юридический статус такого вида денег, существующие барьеры по применению необходимых в данном случае криптографических средств, сложности контроля за эмиссией цифровых наличных. Экономисты опасаются, что именно из-за этого может быть разрушено мировое денежно-финансовое равновесие.

Для совершения платежей исключительно через Интернет используется платежная система интернет-банкинга, основанная на виртуальных банковских картах. Владелец такой карты знает

ее номер, реквизиты и PIN-код, но в физической форме она не присутствует, поэтому расплатиться с ее помощью в обычном магазине, ресторане и т.п. нельзя. В остальном она обладает характеристиками обычных кредитных или дебетовых карт.

Виды доставки товаров и услуг в Интернете: собственная служба доставки интернет-магазина; почта; электронная почта (информационные услуги); предоставление доступа к информационным услугам или каналам связи; импорт («скачивание») информации (программное обеспечение, информационные ресурсы).

Программные продукты, информация, доклады и отчеты, консультации и материалы исследований, электронные версии книг – вся эта продукция может быть доставлена через Интернет.

Электронные магазины в России пока применяют любые возможности доставки (используя даже проводников поезда). Есть магазины, у которых налажена собственная инфраструктура доставки. К этой категории относятся некоторые электронные торговые представительства фирм, имеющих сервис доставки в своей offline сети магазинов, а также единичные интернет-магазины, которые одновременно с торговой системой организовали систему доставки. В основном же сервис доставки большинства интернет-магазинов ограничивается пределами Москвы.

Ввиду того, что многие интернет-магазины отказываются от услуг почты из-за некачественного сервиса (несоблюдение сроков доставки, отсутствие гарантий), в России начали создаваться независимые специализированные службы доставки: «Ассиана», «Скороход», «Апорт», «Сити Экспресс».

Многие книжные интернет-магазины практикуют доставку «книга – почтой» наложенным платежом или с предоплатой.

5. ПОИСКОВЫЕ СИСТЕМЫ В ЭЛЕКТРОННОЙ КОММЕРЦИИ

5.1. Информационно-поисковая система

В общем случае *информационно-поисковая система* – это прикладная компьютерная среда для обработки, хранения, сортировки, фильтрации и поиска больших массивов структурированной информации.

Информационно-поисковая система (ИПС) – это система, обеспечивающая поиск и отбор необходимых данных в специальной базе с описаниями источников информации (индексе) на основе информационно-поискового языка и соответствующих правил поиска.

Главной задачей любой ИПС является поиск информации, ***релевантной*** информационным потребностям пользователя.

По глубине охвата различают следующие типы ИПС:

– локальные;

– глобальные.

Локальные предназначены для поиска информации по какой-либо части всемирной сети, например, по одному либо нескольким сайтам, или же по локальной сети.

Глобальные предназначены для поиска информации по всей сети Интернет. Представителем глобальных ИПС является поисковая система Google.

По принципу организации и пополнения БД о документах в сети выделяют следующие типы ИПС:

– поисковые машины;

– каталоги.

Информационно-поисковая система состоит из поисковой машины, базы данных и системы выдачи результатов поиска пользователям.

База данных представляет собой хранилище всех данных, которые поисковая машина загружает и анализирует, и требует огромных ресурсов для их хранения и обработки. Базу данных ИПС называют «индекс».

Поисковая машина – это комплекс программ, предназначенный для поиска информации. Поисковая машина являются

ключевым инструментом поиска информации для пользователя, поскольку содержит индексы большинства web-серверов Интернета. Однако именно это достоинство оборачивается их главным недостатком. На любой запрос они выдают обычно чрезмерно большое количество информации, среди которой только незначительная часть является полезной, после чего требуется значительный объем времени для ее извлечения и обработки.

Зарубежные поисковые машины:

– Google – www.google.com;

– Altavista – www.altavista.com;

– Excite – www.excite.com;

– HotBot – www.hotbot.com.

Российские поисковые машины:

– Yandex – www.yandex.ru;

– Рамблер – www.rambler.ru.

В комплекс программ ***поисковой машины*** входят «программа-паук» («программа-червяк») и индексатор. Первые две программы по-другому называют «поисковым роботом».

«Программа-червяк» (Crawler) («Программа-паук» (Spider)) – это программа, которая в автоматическом режиме просматривает web-страницы, отыскивая на них нужную информацию, т.е.:

– загружает в поисковую машину web-страницы;

– работает аналогично браузеру, установленному на компьютере пользователя, однако ничего ни на каком экране не отображает;

– передает в поисковую машину HTML-код документа;

– способна найти на web-странице все ссылки на другие страницы;

– определить направление, куда дальше должен идти «паук», руководствуясь найденными ссылками либо заранее заданным списком адресов.

Индексатор (Indexer) – это программа, которая разбирает web-страницу на составные части и анализирует их, т.е.:

– вычленяет и анализирует заголовки, ссылки, текст документов;

– отдельно анализирует выделенный текст, который набран полужирным шрифтом или курсивом.

Процесс анализа web-страницы называется «индексацией».

Система выдачи результатов поиска (Search Results Engine) – это программа, с которой «общается» пользователь и которая решает, какие web-страницы удовлетворяют запросу пользователя и в какой степени.

Каталог – это информационно-поисковая система с классифицированным по темам списком аннотаций, содержащим ссылки на web-ресурсы. В каталогах обычно используют многоуровневую группировку ссылок (дерево). В каждой группе («Новости», «Наука», «Образование» и т.п.) есть разделы, в разделах – подразделы и т.д. Классификация, как правило, производится людьми.

Поиск в каталоге очень удобен и проводится посредством уточнения тем. Тем не менее каталоги поддерживают возможность быстрого поиска определенной категории или web-страницы по ключевым словам с помощью локальной информационно-поисковой машины. База данных ссылок (индекс) каталога обычно имеет ограниченный объем, заполняется вручную персоналом каталога. Некоторые каталоги используют автоматическое обновление индекса.

Результаты поиска в каталоге представляются в виде списка, который состоит из краткого описания (аннотации) документов с гипертекстовой ссылкой на первоисточник.

Зарубежные популярные каталоги:

– Yahoo – www.yahoo.com;

– Magellan – www.mckinley.com.

Российские популярные каталоги:

– «Апорт» – www.aport.ru;

– Weblist – www.weblist.ru;

– «Улитка» – www/ulitka.ru.

Информационно-поисковые системы выполняют следующие функции:

– хранение больших объемов информации;

– быстрый поиск требуемой информации;

– добавление, удаление и изменение хранимой информации;

– вывод информации в удобном для человека виде.

В настоящее время использование информационно-поисковых систем является одним из основных методов при проведении предварительного поиска. Его применение основано на ключевых словах, которые передаются системе в качестве аргумента поиска. Результатом является список ресурсов Интернета.

После получения запроса ИПС анализирует информацию, которая была собрана ранее и находится в индексе, т.е. в базе данных ИПС.

Плюсы – многократно повышается скорость обработки запроса.

Минусы – область поиска ограничена внутренними ресурсами ИПС, а информация в базе данных быстро устаревает.

Ссылки на документы в результате поиска (поисковой выдачи) сортируются (ранжируются) по мере соответствия запросу. Для ранжирования страниц в поисковой выдаче поисковыми системами используются следующие критерии:

– текстовые;

– ссылочные;

– критерии пользовательской оценки.

Текстовые критерии определяют ***релевантность*** документа по совпадению слов и их сочетаний:

– с одной стороны – в запросе;

– с другой стороны – в тексте и заголовке web-страницы.

Релевантность документа – показатель, отражающий, насколько полно соответствует содержание документа конкретному запросу поисковой системы. По каждому слову или словосочетанию запроса поисковая система находит в индексах все веб-страницы, которые их содержат. Таких страниц могут быть десятки тысяч, и поэтому следующая задача системы – отображение их в порядке убывания релевантности. Необходимо добиться того, чтобы независимо от построения запроса веб-страница попадала в первые ряды результатов поиска, а спектр слов и словосочетаний, по которым ее можно найти, был доста-

точно широк. Поисковые системы, как правило, отображают найденные по запросу страницы частями по 10–20 ссылок.

Также можно сказать, что ***релевантность*** – это соответствие результатов поиска сформулированному запросу.

Запрос представляет собой набор слов в определенной последовательности. Если в запросе есть междометия и предлоги (так называемые стоп-слова), то они не рассматриваются ИПС. В результатах поиска, выдаваемых ИПС, слова из запроса будут встречаться в различной последовательности. Кроме того, при поиске ИПС использует все словоформы введенных слов, т.е. существительное в различных падежах, прилагательные на основе существительного и т.п.

Согласно данным маркетинговых исследований, около 60 % пользователей ограничиваются первой страницей результатов поиска и почти 90 % – первыми тремя страницами. Отсюда следует задача – добиться того, чтобы страницы веб-сайта стояли в первых 10–20 результатах поиска. Для ее решения необходимо знать принципы отображения результатов поиска в поисковых системах.

5.2. Поисковая оптимизация

Поисковая оптимизация – процесс увеличения релевантности документа и увеличения его индекса цитирования. Для достижения обозначенной цели используется ряд методов, которые исходят из предположения, что существуют поисковые, или ключевые слова и словосочетания, характерные для определенных групп потенциальных клиентов. Ключевые слова с наиболее удачным соотношением запросов со стороны целевой аудитории и конкуренции со стороны аналогичных веб-ресурсов образуют семантическое ядро сайта. Для оптимизации сайта необходимо досконально изучить язык посетителей, понять, какими способами пользуются они при поиске информации, каковы их интересы, что можно предложить им дополнительно. Наиболее высокая релевантность документа запросу возникает, когда совпадают не отдельные слова, а целые фразы. При этом желательно, чтобы в ключевые фразы входили только ключевые слова.

Один из важных шагов оптимизации – это составление семантического ядра сайта. ***Семантическое ядро сайта*** – это список целевых запросов, вводимых пользователями в строку поиска поисковых систем. Эти запросы, по сути, и определяют тематику сайта. Именно с создания семантического ядра начинается любая раскрутка сайта, ведь при его отсутствии продвижение в поисковых системах окажется просто неэффективным.

Причины отказа индексации сайта поисковыми системами

Для сайта на WordPress отключена видимость для ПС

Нередко при создании сайта с системой управления WordPress владельцы не обращают внимания на приватные настройки, в которых указывается возможность индексации ресурса ПС. Одна галочка может стать причиной отсутствия индексации, и ее достаточно просто убрать.

Наличие тега noindex для содержимого страницы

Возможно, страница Вашего ресурса не индексируется из-за наличия на странице мета-тега < meta name = «robots» content = «noindex, nofollow» > или блоки текста заключены в обычный тег <noindex>, который закрывает его от индексации.

Запрет на индексацию посредством robots.txt

Разработчики нередко не обращают внимания на содержимое данного файла, и весь сайт оказывается закрыт для индексации.

Поисковый робот в первую очередь обращается именно к данному файлу и с его помощью намного эффективнее сканирует содержимое сайта, поэтому стоит тщательно проверить его содержимое на наличие соответствующих запретов и разрешений на индексацию разделов ресурса.

Наличие ошибок и проблем с работой сайта

Сервис Webmaster может показывать перечень проблем сканирования ресурса, которые также могут повлиять на индексацию посредством поискового робота. Все критические ошибки подлежат исправлению.

Возможные проблемы с работой сервера

Если ресурс недоступен в нужный момент времени, то, соответственно, содержимое не индексируется.

6. ИНТЕРНЕТ-МАРКЕТИНГ И WEB-АНАЛИТИКА

6.1. Понятие интернет-маркетинга

По определению Американской маркетинговой ассоциации (AMA) 2004 г., «*маркетинг является организационной функцией и набором процессов для создания ценности, распространения коммуникаций о ценности и доставки ценности потребителям и для управления отношениями с потребителем таким образом, чтобы обеспечивать выгоды организации…»* [4].

Существует множество других определений, понятий и концепций маркетинга, в которых их авторы выражают свое видение маркетинга и как одной из функций предприятия, и как философии бизнеса.

Представление маркетинга как вида деятельности по выявлению и удовлетворению потребностей покупателей и успешность предприятий, уделяющих пристальное внимание своей маркетинговой деятельности, привели к тому, что маркетинг в последние десятилетия все больше рассматривается как направляющая сила деятельности всего предприятия в целом.

Виды маркетинга

Существуют различные подходы к дифференциации маркетинга.

Один из подходов базируется на принципиальных различиях в продукции и ее назначении.

По первому критерию маркетинг можно разделить на:

– маркетинг услуг;

– маркетинг товаров.

По второму критерию:

– маркетинг продукции производственного назначения (промышленный маркетинг);

– маркетинг продукции (товаров) народного потребления.

Второй подход основывается на стадиях воспроизводственного цикла: производство – обращение – потребление. В соответствии с этим подходом маркетинг можно разделить на:

– производственный маркетинг;

– маркетинг оптовой торговли;

– маркетинг розничной торговли.

Третий подход базируется на «виде» покупателя (люди и предприятия) и цели покупки:

– потребительский маркетинг, если покупатель розничный и целью покупки является личное потребление;

– промышленный маркетинг, если покупатель оптовый и целью покупки является производственное потребление или перепродажа.

Более глубокая дифференциация маркетинга может быть осуществлена по отраслям. Отрасль – это совокупность производителей одного блага, которые продают его на одном рынке.

Примеры отраслей – добывающая промышленность, обрабатывающая промышленность, сельское хозяйство и т.п.

В соответствии с названиями отраслей и сфер деятельности или результатом этом деятельности называют и прикладные направления маркетинга:

– банковский маркетинг (маркетинг банка и банковской деятельности);

– маркетинг в сельском хозяйстве;

– маркетинг образовательных услуг;

– промышленный маркетинг (маркетинг товаров производственного назначения);

– маркетинг в строительстве;

– маркетинг предприятий розничной и оптовой торговли и др.

6.2. Инструменты интернет-маркетинга

Контекстная реклама – вид интернет-рекламы, при котором объявление показывается в зависимости от запросов пользователей в поисковой выдаче (Google, Yandex, Mail и т.д.). Всегда обозначается словом «реклама».

SEO-продвижение – совокупность мер по внутренней и внешней оптимизации сайта для поднятия его позиций в результатах выдачи поисковых систем по определенным запросам пользователей.

Таргетированная реклама в социальных сетях – рекламные объявления, которые показываются определенной

группе пользователей, выделенной на основании их предшествующего поведения или анкетных данных.

Платные посты в популярных пабликах. Название говорит само за себя. Под популярными понимаются паблики в соцсетях, у которых не менее 100 000 подписчиков и высокая посещаемость.

Медийная реклама – анимированные или статичные баннеры, тизеры, видеоролики, размещаемые на сайтах в качестве рекламы.

Количественное тестирование (A/B) – способ тестирования, который позволяет оценивать количественные показатели работы двух вариантов веб-страницы, а также сравнивать их между собой. Практический смысл этого метода заключается в поиске и внедрении компонентов страницы, увеличивающих ее результативность.

Ретаргетинг (перенацеливание) – это повторяющийся показ интернет-рекламы ранее посещённой веб-страницы.

E-mail–marketing – способ индивидуальной коммуникации с клиентом, характеризующийся построением долгих доверительных взаимоотношений при помощи рассылки писем на электронные адреса пользователей.

Партнерские программы – форма делового сотрудничества, которую предлагают раскрученные в Интернете проекты для увеличения количества продаж товаров и услуг. Суть партнерской программы в том, что за привлечение клиентов проект платит вам часть прибыли, которую получает от продаж. Это позволяет продавцу сократить расходы на привлечение конечного покупателя. Важное условие для успешной работы с партнерскими программами – это большая посещаемость вашего сайта: как минимум, несколько сотен уникальных посетителей в день.

SMM-продвижение (Social Media Marketing) – комплекс мероприятий по привлечению внимания к продукту/услуги и трафика на сайт через социальные сети.

Работа с лидерами мнений – выстраивание дружеских отношений с человеком, который оказывает влияние на мнение других людей. Лидер мнений имеет активную жизненную позицию, у него много друзей, большое количество контактов в Интернете. Это долгая кропотливая работа на результат. Необхо-

димо показать лидеру все преимущества вашего товара/услуги, дать полную информацию, создать у него благоприятное впечатление и поддерживать его всевозможными способами: дарить новинки, проводить эксклюзивные тесты и т.д.

Вирусный маркетинг – различные методы распространения рекламы в геометрической прогрессии и с высокой скоростью (как вирус), где главным распространителем информации являются сами получатели информации.

Контент-маркетинг – подготовка и распространение качественной, актуальной и ценной информации, которая не является рекламой, но которая косвенно убеждает аудиторию принять необходимое решение, выбрать определенный товар/услугу.

Многочисленные исследования показывают, что социальные медиа являются самыми популярными платформами в Интернете: многие пользователи имеют аккаунт по крайней мере в одной социальной сети.

Социальные медиа (англ. *social media*) – это основанные на интернет-технологиях каналы и площадки для общения и обмена контентом между пользователями: социальные сети, форумы, блоги, сервисы видеохостинга.

Активность в социальных медиа, также известная под аббревиатурой SMM (*social media marketing*), быстро развилась и получила статус одного из важных инструментов взаимодействия с аудиторией. Интернет-маркетинг в социальных медиа имеет много преимуществ:

– более широкий охват целевой аудитории. Социальные медиа по своей популярности превосходят все традиционные ресурсы, не превышая разве только актуальности поисковых систем;

– достаточно точная информация о клиентах, их вкусах и предпочтениях;

– невысокая стоимость рекламной кампании (цена за один контакт стоит минимум в два раза дешевле традиционной рекламы, при этом каждый контакт представляет собой реальную ценность);

– возможность получать быструю обратную связь и оперативно реагировать на нее;

– повышение лояльности покупателей вследствие «очеловечивания» бренда компании. Реклама в социальных медиа не столь явная, она не рассматривается пользователями как навязываемая, скорее сообщение воспринимается как рекомендации знакомых, как мнение интересных людей лидеров сообществ (и это вызывает большее доверие).

6.3. Показатели эффективности для интернет-магазина

1. Посещаемость сайта

Измеряйте посещаемость вашего сайта в разрезе дневной аудитории, недельной и месячной. Это позволит оценивать падения и всплески посещаемости сайта и выявлять их причины.

Установите для себя цель по среднему количеству посещений, которое хотите достигнуть, и работайте над стратегией привлечения посетителей на сайт, отталкиваясь от этой цифры

Чтобы определить цель по посещаемости, проанализируйте конкурентов, у них могут быть установлены открытые счетчики статистики, которые покажут посещаемость их сайта. Вы сможете проанализировать каналы, которые используют конкуренты для привлечения трафика, и использовать эти данные для увеличения посещаемости своего сайта.

2. Просмотры товарных страниц

Какие страницы на вашем сайте посетители просматривают больше всего, а какие меньше? Анализируя посещаемость продуктовых страниц, вы сможете понять товарные предпочтения посетителей и как они взаимодействуют с сайтом. Возможно, у вас есть отличные товары, но потенциальные покупатели не могут найти их на из-за плохой навигации сайта.

Пример: вы предлагаете хорошие товары со скидкой, но они доступны лишь в общем разделе сайта. Создайте отдельный каталог («Распродажа», «Товары со скидкой», «Лучшие предложения»), таким образом привлекая внимание к нужным товарам.

3. Среднее время пребывания на сайте и среднее количество просмотренных страниц

Многие владельцы интернет-магазинов и маркетологи пренебрегают оценками этих двух метрик, считая их не показательными. Но они позволяют сделать определенные полезные

выводы о работе вашего интернет-магазина. Если эти показатели низкие, то стоит оценить качество трафика вашего сайта. Насколько быстро загружается ваш сайт? Помните, пользователи нетерпеливы и ждут быстрой работы сайта. Проверьте скорость загрузки с помощью GTmetrix, чтобы понять, нужна ли вам оптимизация в этой области работы сайта.

Важно понимать, что для целевых страниц или интернет-магазинов с небольшим ассортиментом эти показатели могут быть сравнительно небольшими, а у крупных магазинов среднее количество просмотренных страниц может быть более 20.

Кроме того, если в вашем интернет-магазине среднее количество товаров в заказе невелико, например 1–2, то и среднее время, проведенное посетителем на сайте, будет небольшим, так как на выбор товара не нужно тратить много времени.

4. Страницы выхода

Когда посетители покидают ваш сайт? Тогда, когда они понимают, что необходимо зарегистрироваться для завершения покупки? Или, может быть, когда они видят стоимость ваших товаров? Анализируя точки выхода посетителей сайта, вы сможете лучше понимать причины низкой конверсии и оптимизировать сайт таким образом, чтобы пользователи оставались на сайте и завершали покупки.

О проблемах в оформлении заказа могут свидетельствовать выходы со страниц:

– регистрация;

– корзина;

– оформление заказа.

Это значит, что пользователи начинают оформлять покупку на сайте, но сталкиваются с проблемами и не завершают процесс заказа.

5. Каналы привлечения посетителей

Отслеживание источников привлечения посетителей на сайт – важная метрика для оценки эффективности работы интернет-магазина, т.к. каналов для привлечения может быть очень много, и экономическая эффективность тоже разная. Используете ли вы поисковую оптимизацию в «Яндексе» и Google для привлечения посетителей, а контекстную рекламу в «Ян-

декс.Директ» и Google Adwords? Активны ли вы в социальных сетях и на отраслевых площадках?

Необходимо отслеживать не просто источники привлечения посетителей, а их отдачу. Если один из каналов показывает хорошую вовлеченность посетителей на сайте и рост продаж, тогда необходимо увеличивать бюджет на этот канал. А если канал не эффективен, необходимо подумать о том, как минимизировать затраты или же оптимизировать работу, например, удалив неэффективные ключевые слова из рекламной кампании в «Яндекс.Директ» или пересмотреть SEO-ядро, по которому продвигается сайт.

6. Показатель конверсии

Ваш интернет-магазине устроен так, чтобы довести посетителя до покупки? Оценка конверсии сайта позволяет облегчить путь посетителя от выбора товара до покупки. Наверняка у вас есть идеи по улучшению вашего сайта и процесса оформления заказа. A/B-тестирование таких идей позволит точно узнать, что повысит конверсию, а что нет.

Необходимо начинать с оптимизации наиболее важных страниц сайта:

– товарная карточка;

– регистрация;

– корзина;

– оформление заказа.

Тестируйте кнопку «добавить в корзину», форму регистрации на сайте, форматы описания товара, варианты оформления заказа (с регистраций или без нее, в 1 клик или из нескольких шагов).

7. Количество брошенных корзин

Очень важно оценивать показатель брошенных корзин. По исследованиям института Baymard, средний показатель составляет 67,75 %. Почему это происходит?

Причин может быть очень много:

– стоимость товаров в заказе не соответствует стоимости, указанной в карточке товара. Или, например, в корзине появляется дополнительная строка стоимости доставки, которая увеличивает стоимость товара и отталкивает заказчика;

– промо-код на скидку не работает;

– посетитель не видит, есть ли доставка товара в его страну или регион;

– на странице оформления заказа появляются дополнительные расходы, например, налоги;

– недостаточное количество вариантов оплаты заказа;

– технические проблемы с заполнением платежных данных.

Необходимо постоянно проверять работу корзины товаров в вашем интернет-магазине. Необходимо тестировать новые идеи по оптимизации процесса оформления заказа.

Рекомендации. Работайте с брошенными корзинами: отправляйте письма с уведомлением о том, что оформление заказа не завершено и товары ждут покупателя в корзине. Старайтесь получить обратную связь, почему покупка не была совершена.

7. СТАНДАРТЫ В ЭЛЕКТРОННОЙ КОММЕРЦИИ

7.1. Система электронного обмена данными (EDIFACT)

Первые системы электронной коммерции возникли в 1960-х гг. в США. Первоначально электронная коммерция велась по сетям, использующим собственные протоколы обмена данными, что объективно сдерживало электронную коммерцию. Для развития электронной коммерции были созданы стандарты электронного обмена данными между организациями (Electronic Data Interchange, EDI) – наборы правил электронного оформления типовых деловых документов: заказов, накладных, таможенных деклараций, страховых форм, счетов и т.д.

К концу 1960-х гг. в США уже существовали четыре индустриальных стандарта для обмена данными в системах управления авиационным, железнодорожным и автомобильным транспортом.

Примерно в те же годы аналогичные события произошли и в Англии. Выработанный здесь набор спецификаций Tradacoms был принят Европейской экономической комиссией ООН (United Nations Economic Commission for Europe, UNECE) в качестве стандарта обмена данными в международных торговых организациях. Этот набор форматов и протоколов получил название GTDI (General-purpose Trade Data Interchange).

В 1980-х гг. начались работы по объединению европейских и американских спецификаций. На базе GTDI международная организация по стандартизации ISO сформировала новый стандарт Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT, ISO 9735), использующий в качестве транспортного протокол электронной почты X400, что дало новый толчок для увеличения оборотов электронной коммерции и числа, вовлеченных в нее компаний. В 1996 г., когда торговля через Интернет была еще в зачаточном состоянии, посредством EDI-трансакций было совершено операций на $300 млрд, а в 1999 г. – уже на $1,1 трлн. В 2003 г., по оценкам компании IDC, этот показатель достиг $2,3 трлн.

Главным положительным свойством EDI, привнесенным в мир электронной коммерции, является стандартизация всех процедур документооборота между компаниями.

Еще один немаловажный фактор состоит в том, что EDI является удобным и безопасным интерфейсом, надежность которого была проверена в течение многих лет эксплуатации.

В качестве основных недостатков EDI можно назвать следующие:

– необходимость доработки программного обеспечения информационных систем компаний для отображения данных из внутрикорпоративного представления в EDI-совместимый формат;

– необходимость согласования способа формирования EDI-пакетов;

– большой объем трансакций.

Перечисленные недостатки показывают, что внедрение EDI является достаточно сложным и дорогостоящим мероприятием, а потому доступным только крупным компаниям.

Привлекательность Интернета для электронной коммерции обусловлена прежде всего низкой себестоимостью передачи данных. Однако проблема заключалась в том, чтобы сделать EDI-системы доступными для массового потребителя глобальной сети. В результате в середине 1990-х гг. был разработан еще один стандарт – EDIFACT over Internet (EDIINT), описывающий, как передавать EDI-трансакции посредством протоколов безопасной электронной почты SMTP/S-MIME.

Тем не менее и этот стандарт не стал исчерпывающим, в связи с чем не прекращаются попытки связать воедино форматы электронных документов – HTML в Интернете и EDIFACT в глобальных вычислительных сетях (ГВС).

Существенным недостатком HTML можно назвать ограниченность набора его тегов для отображения специализированной информации (например, мультимедийной, математических, химических формул и т.д.). На смену HTML предложен XML (Extensible Markup Language) – язык разметки, описывающий целый класс объектов данных, называемых XML-документами. Этот язык используется в качестве средства для описания грамматики других языков и контроля правильности

составления документов. То есть сам по себе XML не содержит никаких тегов, предназначенных для разметки, он просто определяет порядок их создания.

Еще одним из очевидных достоинств XML является возможность использования его в качестве универсального языка запросов к хранилищам информации.

XML позволяет также осуществлять контроль корректности данных, хранящихся в документах, производить проверки иерархических соотношений внутри документа и устанавливать единый стандарт на структуру документов, содержимым которых могут быть различные данные.

Для упрощения процессов взаимодействия между информационными системами предприятий и тем самым привлечения компаний среднего и малого размера в мир электронной коммерции разработан стандарт XML/EDI, который устраняет главный недостаток EDI: сложность отображения корпоративных данных из внутреннего представления в EDI-формат.

Все эти разработки должны обеспечить дальнейшее снижение себестоимости систем электронной коммерции.

Появление Интернета привело к возникновению качественно новых форм электронной коммерции, в которых EDI-технологии не используются или их применение носит вторичный характер.

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

Не являясь единой технологией, электронная коммерция в Интернете характеризуется разносторонностью. Она объединяет широкий спектр бизнес-операций, которые включают в себя:

– обмен информацией;

– установление контактов;

– пред- и послепродажную поддержку;

– продажу товаров и услуг;

– электронную оплату, в том числе с использованием электронных платежных систем;

– распространение продуктов;

– возможность организации виртуальных предприятий;

– осуществление бизнес-процессов, совместно управляемых компанией и ее торговыми партнерами.

Возможности электронной коммерций в Интернете привносят следующие новые элементы в современный бизнес:

– рост конкуренции;

– глобализация сфер деятельности;

– персонализация взаимодействия;

– сокращение каналов распространения товаров;

– экономия затрат.

Технологии, применяемые для реализации решений по электронной коммерции

Здесь мы кратко рассмотрим преимущества EDI-технологий и требования, связанные с решением сложных проблем и задач безопасности.

EDI – взаимообмен электронными данными.

Технология EDI – это очень быстрый способ обмена деловой документацией, используя компьютерные соединения между различными компаниями. Проще говоря, EDI – это стандарт, который конвертирует формат передаваемого документа в формат получающего компьютера.

Преимущества, которые дает использование EDI:

• сокращаются всякого рода затраты, связанные с подготовкой документации на бумажных носителях;

• улучшается решение проблемных ситуаций;

• улучшается обслуживание клиентов;

• расширяется база клиентов/поставщиков.

Первоначально EDI-технология использовалась, чтобы улучшить проведение отдельных процессов, таких как автоматизация платежных расчетов или процесс перевода средств со счетов. В настоящее время EDI используется в е- коммерции при соединении внешних и внутренних бизнес-процессов, которые позволяют компаниям улучшить свою производительность в таких масштабах, как никогда ранее.

Компании теперь могут делать заказы, осуществлять покупки, оплачивать счета, переводить средства, связываться с

поставщиками, дистрибьюторами, клиентами, банками, транспортными организациями посредством новых электронных технологий.

Используя Интернет как коммуникационный канал EDI, можно значительно снизить издержки и расширить круг торговых партнеров. Множество компаний по всему миру используют Интернет в своем бизнесе.

Между тем вследствие того, что EDI является дорогостоящей системой, требует больших затрат по установке и подключению, только крупнейшие компании могли позволить себе использовать ее в качестве системы обмена данными.

Интернет-технологии могут существенно облегчить эту ситуацию. Кроме сокращения издержек, открытый или интерактивный обмен данными позволяет покупателям и поставщикам полностью осуществить сделку от начала и до конца.

Вместе с тем все еще существуют проблемы хостинга, которые, правда, связаны с бизнесом, а не с технологией. Необходимы стандарты и более открытые системы, которые воспринимаются продавцами как угроза собственным решениям и созданию добавочной стоимости.

7.2. Штриховое кодирование

Штрих-код – это набор геометрических символов, расположенных по определенному стандарту. Как правило, представляет собой вертикальные прямоугольники различной ширины. Набор таких прямоугольников представляет данные в машинном коде.

Штрих-код чем-то напоминает заводской номер. Числа и/или знаки, закодированные штрих-кодом, это уникальный идентификатор, который после считывания может быть использован компьютером для поиска дополнительной информации о продукте. Например, штрих-код на плитке шоколада – идентификатор продукта, который используется системой продаж для определения цены, текущей скидки и других коммерческих данных по базе данных.

Штриховое кодирование эффективно используется в системах, в которых участие человека минимально или отсутству-

ет совсем. Применение технологий штрихового кодирования максимально возможно устраняет ошибки, которые возникают при вводе данных вручную. Штрих-код имеет множество сфер применения, в их числе идентификация товаров, инвентаризация, маркировка грузов и т.д.

Поскольку штрих-код печатается и считывается машинами, их обработка занимает гораздо меньше времени, а также с более высокой точностью, чем ввод данных вручную.

Например, ввод 12-ти позиций займет у оператора около 6 секунд. В то время как считывание штрих-кода 12-ти позиций займет только 300 миллисекунд. При ручном вводе в среднем возникает одна ошибка на 300 позиций. При работе с контрастным штрих-кодом нормой является менее одной ошибки в каждом миллионе считанных позиций. Ошибки при вводе данных приводят к дополнительным затратам – от стоимости повторного ввода данных до отгрузки не того товара не тому клиенту.

Штрих-код чрезвычайно точен. В то время как оператор может допускать ошибку каждые 300 позиций, штрих-коды имеют нормы, допускающие менее одной ошибки на каждый миллион считанных штрих-кодов. К тому же некоторые стандарты кодирования имеют алгоритмы корректирования ошибок, что ведет к уменьшению этой нормы.

На данные момент существует более 300 стандартов штрихкодирования. Различные стандарты используют разнообразные алгоритмы кодирования. У каждого алгоритма существуют свои особенности, такие как минимальная и максимальная длинна данных, ограничения на размер штрих-кода и т.д. Стандарты имеют свои достоинства и недостатки и часто разрабатываются с учетом конкретной области применения. Однако есть небольшое количество стандартов, которые подходят для большинства приложений.

Разные стандарты используются для множества целей. Ниже приведен список наиболее популярных стандартов штрих-кода и указана сфера применения каждого стандарта.

Code 128: штрих-код переменной длины. Обычно кодируются буквенно-цифровые данные. Данный стандарт подходит для общего применения, например для маркировки DVD-дисков, удостоверений личности и многих других целей.

EAN.UCC-128: штрих-код переменной длины. Обычно кодируются буквенно-цифровые данные. Этот международный стандарт разрабатывался для обмена данными между различными компаниями. Стандарт UCC.EAN-128, помимо данных, кодирует идентификатор (AIs), который позволяет определить тип закодированных данных и формат кодирования. UCC.EAN-128 кодирует данные, используя алгоритмы стандарта Code 128.

Code 39: штрих-код переменной длины. Обычно кодируются буквенно-цифровые данные. Данный стандарт широко используется уже много лет и является самым популярным в мире для общих задач. Однако Code 39 уже начинает уступать лидерство более новым форматам, таким как Code 128.

UPC-A: 12-значный штрих-код фиксированной длины для кодирования числовых данных. Используется в американских розничных магазинах для идентификации товаров. Уникальные штриховые коды UPC-A разработаны UC-советом. Если Вы собираетесь продавать свои товары в американских розничных магазинах, то, скорее всего, вам придется позаботиться о наличии штрих-кода UPC-A на вашей продукции.

UPC-E: 6-значный штрих-код фиксированной длины для кодирования числовых данных. UPC-E – сокращенный вариант штрих-кода UPC-A. Данный стандарт используется для идентификации мелких розничных товаров, размеры которых не позволяют разместить на них полный штрих-код UPC-A.

EAN-8 (JAN-8): 8-значный штрих-код фиксированной длины для кодирования числовых данных. EAN-8 – сокращенный вариант штрих-кода EAN-13. Используется для маркировки мелких товаров, размеры которых не позволяют разместить полный штрих-код EAN-13.

Standart 2 of 5: штрих-код переменной длины для кодирования числовых данных. Данный стандарт используется с 60-х гг. для маркировки авиабилетов и других целей. Также известен как Industrial 2 of 5.

Interleaved 2 of 5: штрих-код переменной длины для кодирования числовых данных. Обновленная версия Standart 2 of 5 и во многих случаях заменившая его. Широко распространен на складах и в сфере дистрибуции.

MSI Plessy обычно используется для контроля за наличием товара на розничных складах.

Codabar: штрих-код переменной длины для кодирования числовых данных. В основном используется библиотеками, банками крови и плазмы, а также курьерской службой FedEx.

PostNet: штрих-код фиксированной длины для кодирования числовых данных. Используется американской почтовой службой для сортировки почты. С помощью PostNet кодируются 5- или 9-значные почтовые индексы, а также 11-значные коды доставки.

PDF417: двумерный штрих-код переменной длины для кодирования буквенно-числовых данных. PDF417 очень похож на DataMatrix и предоставляет немного больше возможностей, требуя, соответственно, больше места. Используется для общего применения, включая ярлыки на багаже, маркировку различных частей и удостоверения личности.

8. КОММЕРЧЕСКИЙ ЦИКЛ ЭЛЕКТРОННОЙ КОММЕРЦИИ

8.1. Стратегии интернет-бизнеса

Изменение направления бизнес-деятельности с переходом к электронной коммерции.

Электронная коммерция облегчает реинжиниринг бизнеса – процесс, который широко распространен в настоящее время среди наиболее крупных компаний экономически развитых стран Запада. Цели электронной коммерции схожи с целями, которые решаются в процессе реинжиниринга:

– сокращение издержек;

– уменьшение времени производственного цикла;

– ускорение выполнения запросов клиентов;

– улучшение качества обслуживания.

Однако усилия фирм, связанные с реинжинирингом, как правило, игнорируют социальные издержки, возникающие при радикальных организационных изменениях в деятельности фирмы. В то время как ценность изменений, связанных с внедрением интернет-технологий, е-коммерции, предполагает, что если такие изменения сделаны грамотно, то это стимулирует создание положительной рабочей обстановки.

В условиях ведения бизнеса по традиционному пути предприятия отвечали за все. Развитие товара, его производство, продажа, доставка, материально-техническая поддержка требовали громадных затрат ресурсов, в чем организации не всегда были полностью компетентны.

Электронная коммерция начала трансформацию деятельности предприятий в сеть виртуальных сообществ организаций, каждое из которых может сконцентрировать свою деятельность на тех направлениях, в которых наиболее компетентно, с тем чтобы поставлять законченное производственное решение своим клиентам.

Электронная коммерция является инструментом в создании ряда новых возможностей ведения бизнеса.

Сюда входят:

1. Системы информационной/деловой среды бизнеса.
2. Видеоконференции.
3. Многообразная информация.
4. Обучение.
5. Финансовое взаимодействие.
6. Новые отношения между компаниями, основанные на электронных технологиях.
7. Новая экономика производить и покупать товары/услуги.
8. Новые модели маркетинга.
9. Сотрудничество.
10. Новые и более дешевые каналы.
11. Новые бизнес-комбинации.
12. Поддержка альтернативных работ.
13. Новые отношения с клиентами.

Наиболее важным в том, как е-коммерция изменяет бизнес, является то, как происходит построение новых взаимоотношений с клиентами. Сюда входят:

– online реклама и маркетинг;

– возможность оформления заказа online;

– online обслуживание клиентов;

– максимальное соответствие продуктов и услуг запросам клиентов.

Управление цепочкой поставок

Электронная коммерция также уменьшает расходы, связанные с приобретением товаров и управлением запасами, за счет прямого эффективного взаимодействия с широким кругом поставщиков и торговых партнеров. Различные виды бизнеса создают заново услуги по дистрибуции на основе приложений business-to-business, создающих добавочную стоимость.

Многие печатные издания размещают свои материалы в сети Интернет, которые становятся доступными читателям повсюду. Новички, входящие в этот бизнес, имеют возможность получить неограниченную аудиторию благодаря размещению своих материалов в сети.

Ряд компаний занимается поставкой продуктов, основу которых также составляет информация; это интерактивные игры, аудио и видеоматериалы, что пользуется широким спросом у разных слоев населения.

Причины необходимости электронной коммерции для offline-бизнеса

Можно назвать, по крайней мере, три причины:

1. Размер и рост рынка.

2. Быстрая адаптация к е-коммерции конкурентов.

3. Быстрый рост числа конкурентов вследствие понижения входных барьеров на рынок.

Модели, в основе которых лежит использование web- технологий, могут включать все фазы совершения сделки, включая:

– запрос информации клиентом у поставщика;

– система подтверждения наличия товара у поставщика;

– клиентская система, позволяющая производить покупку товара;

– система поставщика, признающая/одобряющая покупку;

– система поставщика, подтверждающая покупку;

– система поставщика, размещающая заказ.

Несмотря на все вышеперечисленное, процесс проведения трансакций через web создает некоторые серьезные проблемы для бизнеса. В чем состоят эти проблемы, рассмотрим далее.

Главная особенность стратегии интернет-бизнеса – ориентация на потребителя. Используя Интернет, бизнес может более «близко» подойти к потребителю, более качественно организовать индивидуальное обслуживание покупателей и клиентов.

Новая стратегия развития компании

Новая стратегия развития компании заключается в том, что интернет-проект начинает развиваться в сторону корпоративного offline-бизнеса. Возможны два варианта стратегии:

1. Интернет-проект создает свой собственный offline-бизнес по образцу традиционных бизнес-схем компаний аналогичного профиля деятельности. Например, книжный магазин арендует склад, организует курьерскую и транспортную службу и нанимает квалифицированный персонала. Но «с нуля» создавать свой offline-бизнес очень сложно, потому что, например,

рост объемов продаж для раскрученного интернет-проекта чаще всего оказывается больше, чем темпы наращивания мощности обслуживающих ресурсов для соответствующей offline-деятельности. Кроме того, offline-конкуренты не допускают нового конкурента в offline-сегмент рынка. Поэтому наиболее правильной стратегией является второй вариант.

2. Покупка некой offline-компании для интернет-проекта, соответствующей профилю деятельности интернет-проекта.

Но необходимо отметить, что создание собственного offline-бизнеса для Интернет-проекта целесообразно на втором этапе развития, т.е. только тогда, когда Интернет-проект уже раскручен и приносит прибыль.

Стратегии развития корпоративных проектов в Интернете

Для корпоративного бизнеса в Интернет возможно использовать одну из трех нижеследующих стратегий:

1) трансформация традиционного offline-бизнеса компании в online с учетом новых возможностей, появляющихся в online мире. При этом компания по-прежнему остается и в offline-бизнесе, таким образом создается компания «смешанного» типа;

2) образование дочерней компании, которая находится в эксклюзивных отношениях с материнской и реализует функции перевода бизнеса материнской компании в электронные формы;

3) покупка существующего интернет-проекта для развития бизнеса предприятия в online среду. Например, есть интернет-магазин, торгующий компьютерами, и есть компания, производящая компьютеры, тогда компания покупает интернет-магазин, чтобы затем интегрировать его в свой бизнес.

Стратегии развития интернет-проектов

В отличие от корпоративных проектов, интернет-проекты не имеют своей целью «выход в Интернет», они изначально являются частью интернет-экономики. При этом проекты, которые приступили ко второму этапу развития (этапу движения к offline-бизнесу), могут выбрать те же самые 3 стратегии, но со своей спецификой:

1) трансформация своего online-бизнеса в «смешанный» вариант, объединяющий online- и offline-процессы в единый бизнес;

2) образования дочерних компаний из интернет-проектов обычно не происходит, но инвесторы решают вопросы диверсификации с помощью образования интернет-холдингов, т.е. путем создания нескольких интернет-проектов. В России такими холдингами являются Runet, Netbridge, «Рамблер», Port.ru, Golden Telecom и именно они определяют инвестиционный климат в Рунете;

3) покупка offline-компании, бизнес которой дополняет online-бизнес интернет-проекта. Это очень распространенная стратегия для Интернет-проектов с серьезной инвестиционной поддержкой.

Стратегии развития и для корпоративных проектов, и для интернет-проектов вполне сопоставимы. И важной особенностью интернет-бизнеса является возможность для корпоративных и интернет-проектов взаимодействовать между собой.

8.2. Преимущества внедрения стратегий электронной коммерции

Преимущества внедрения стратегий электронной коммерции

Существует целый ряд преимуществ и возможностей, которые открываются с внедрением технологии электронной коммерции, обеспечивая устойчивое конкурентное превосходство бизнеса.

1. Конвергенция – сближение технологий, информационных средств и даже отраслей промышленности.

2. Возможности – удобство и возможность контролировать деятельность для повышения благосостояния и повышения степени удовлетворенности от выполняемой работы.

3. Интеграция – оптимизация и осуществление производственных процессов на предприятии и альянсов с другими организациями с помощью цифровых технологий для роста эффективности производства и расширения рынков.

4. Устранение посредников – трансформация составляющих бизнес-цепочки, чтобы приблизить потребителей к производителям, минуя многочисленных посредников.

5. Инновации – сохранять конкурентоспособность в условиях, когда на рынке появляются все новые и новые товары и услуги, возникают новые формы конкуренции.

6. Заинтересованность – вовлечение клиентов в производственный цикл. Потребители должны быть вовлечены в процесс создания продукта, чтобы в результате они получили именно то, что хотели.

7. Немедленный отклик на запрос

8. Глобализация – представление своего бизнеса на глобальном рынке.

Электронная коммерция устраняет географические границы и барьеры. С одной стороны, это открывает огромные возможности, а с другой – означает необходимость решения сложных проблем.

9. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ

9.1. Виды и источники угроз

Психологический фактор, связанный с осознанием угрозы потенциального мошенничества, остается основным препятствием для использования Интернета в качестве средства проведения коммерческих операций. Опросы показывают, что более всего люди боятся потенциальной угрозы получения кем-либо их персональных данных при работе через Интернет. По данным платежной системы VISA, около 23 % транзакций электронной коммерции не производится из-за боязни клиента ввести запрашиваемую электронным магазином персональную информацию о клиенте.

Масштабы мошенничества

Примерно 25 % всех сообщений chargeback (отказ от платежа), генерируемых в платежных системах, приходится на транзакции Cardholder Not Present. Транзакции электронной коммерции занимают второе место среди всех видов мошенничества по кредитным картам, уступая лишь мошенничествам, совершенным по украденным или потерянным картам (Lost/Stolen) – 40 %, и сравнявшись с мошенничествами по подделанным картам (Counterfeit) – 25 %. Полезно также отметить, что создание и отправка одного сообщения chargeback обходится банку-эмитенту в среднем в $10–15, а во многих случаях, связанных с электронной коммерцией, эта сумма может быть в несколько раз больше.

По данным консалтинговой компании Meridien Research, только в 2010 г. сумма похищенных через Интернет средств достигла $1,6 млрд. Больше всего от электронных краж пострадали Соединенные Штаты.

Некоторые интернет-продавцы утверждают, что каждая четвертая попытка провести транзакцию через Интернет является мошеннической. Большинство таких транзакций завершаются отказом от авторизации из-за неправильного номера карты и/или срока действия карты.

Приведем классификацию возможных типов мошенничества через Интернет, приводимую международными платежными системами:

– транзакции, выполненные мошенниками с использованием правильных реквизитов карточки (номер карточки, срок ее действия и т.п.);

– компрометация данных (получение данных о клиенте через взлом БД торговых предприятий или путем перехвата сообщений покупателя, содержащих его персональные данные) с целью их использования в мошеннических целях;

– магазины-бабочки, возникающие, как правило, на непродолжительное время для того, чтобы исчезнуть после получения от покупателей средств за несуществующие услуги или товары;

– злоупотребления торговых предприятий, связанные с увеличением стоимости товара по отношению к предлагавшейся покупателю цене или повтором списаний со счета клиента;

– магазины и торговые агенты (Acquiring Agent), предназначенные для сбора информации о реквизитах карт и других персональных данных покупателей.

Рассмотрим некоторые из перечисленных выше типов мошенничества. Так, первый тип мошенничества является наиболее массовым. Для совершения транзакции электронной коммерции мошеннику достаточно знать только номер карты и срок ее действия. Такая информация попадает в руки мошенников различными путями. Наиболее распространенный способ получения мошенниками реквизитов карт – сговор с сотрудниками торговых предприятий, через которые проходят сотни и тысячи транзакций по пластиковым картам, зачастую хранящим информацию о реквизитах карт в своих базах данных. Результатом сговора становится передача информации о реквизитах карт в руки криминальных структур.

Другой способ получения информации о реквизитах карт, ставший популярным в последнее время, это кража баз данных карточек в торговом предприятии.

Достаточно распространенным является способ, когда криминальные структуры организуют свои магазины, и торговые агенты с главной целью получить в свое распоряжение зна-

чительные наборы реквизитов карт. Часто такие магазины представляют собой различного рода порно-сайты.

Второй тип мошенничества – компрометация персональных данных владельцев пластиковых карт – связан со взломом баз данных. Так, только в последние несколько лет наиболее громкими «делами» стали кража в Уэльсе двумя подростками 26000 реквизитов карт из баз данных одного из электронных магазинов, российским хакером была вскрыта база данных объемом 300000 записей, кража реквизитов 485000 карт, выставленных в сети National Aeronautic & Space Administration.

По данным компании Meridien Research, уязвимость интернет-магазинов усугубляется еще и тем, что лишь 30 % online продавцов используют надежные системы защиты для борьбы с компьютерными мошенниками.

Третий тип мошенничества – магазины-бабочки, которые открываются с целью «отмывания» украденных реквизитов карточек. После того, как у мошенников появляются украденные реквизиты карточек, они организуют виртуальный магазин, торгующий всякими безделушками. При этом в обслуживающий банк регулярно направляются авторизационные запросы, использующие украденные номера карточек, а, следовательно, магазин регулярно получает от обслуживающего банка возмещения за совершенные в нем «покупки».

Магазины-бабочки обычно выбирают две крайние стратегии своей работы. Выбор стратегии определяется размером украденной базы данных карточек. Если размер украденной БД достаточно большой, то выбирается стратегия, в соответствии с которой транзакции делаются на небольшие суммы. В этом случае владелец карты заметит небольшую потерю средств на своем счете не сразу. Когда же база данных о карточках незначительная, то транзакции выполняются на крупные суммы.

9.2. Вопросы правового регулирования безопасности электронной коммерции

Интернет подвергается правовому регулированию, но либо оно недостаточно, либо несвоевременно, либо не совсем корректно.

Развитие сети Интернет в ближайшем будущем превратит ее в стандартный канал социальных коммуникаций, по которому будут осуществляться подавляющее число розничных торговых операций, перевод денежных средств, все функции связи и вещание средств массовой информации. Возникнут новые социальные группы, новая идеология, сформируется новый психологический образ жителя планеты XXI в. Тем самым природа открывшихся возможностей позволит успешно дублировать классические социальные связи материального мира, привязанного к географии планеты, и в некоторых случаях заменять их.

Указанный канал социальных коммуникаций сейчас можно использовать и как благо для развития общества, и как средство для осуществления антисоциальных действий. При отсутствии норм, регулирующих действия пользователей, организаций и государств в Интернете, возникает и прочно укрепляется в сознании двойной стандарт: законы должны соблюдаться, но только не в Сети.

Причины данной опасной тенденции многогранны, и их можно условно разделить на технические, социально-психологические и правовые.

К первым можно отнести влияние природы информации на электронных носителях (электронные данные в нашем материальном мире являются чрезвычайно изменчивыми и нестабильными), колоссальные массивы данных и «текучесть» информации в сети Интернет, а также незащищенность протоколов обмена информацией.

Социально-психологическими причинами процесса становления двойного стандарта являются отсутствие понимания места и роли сети Интернет в человеческом обществе и эфемерный статус автономности личности, дающий возможность наслаждаться анонимностью и кажущимся могуществом.

К правовым причинам относятся известная недостаточность правового регулирования и концептуальная сложность обеспечения доказательств в сети.

На настоящий момент, например, с точки зрения российского уголовного закона, любой российский сегмент сети Интернет представляет собой конгломерат уголовно наказуемых деяний в форме клеветы и оскорблений, встречающихся повсе-

местно на просторах Интернета, заведомо ложной рекламы в виде распространения порнографических материалов, нарушения прав на объекты интеллектуальной собственности.

Текущая ситуация таит в себе колоссальную опасность. Если тенденции раздвоения реального и виртуального мира сохранятся, то любые усилия международного сообщества, государств по регулированию ряда общественных отношений будут пропадать даром: например, Россия борется с распространением наркотиков, а в Сети уже сейчас существуют русскоязычные сайты, детально описывающие все тонкости изготовления, покупки и применения наркотических средств.

При анализе механизмов действия сети Интернет и способов представления и распространения информации в ней также возникают уникальные и не имеющие аналогов в реальном мире специальные юридические проблемы.

Во-первых, это проблемы регулирования электронной коммерции. К ним относятся вопросы заключения контрактов посредством Интернета, вопросы недобросовестной рекламы, спама, проблема налогообложения предпринимательства в Сети.

Тематикой следующей группы юридических проблем является соблюдение авторских прав в Интернете. Здесь возникают неразрешенные и неоднозначно трактуемые по законодательству зарубежных стран и Российской Федерации вопросы использования фреймов, ссылок, метатэгов.

Очередная чрезвычайно полемическая проблема Сети – использование товарных знаков в ней, включая известную дилемму: товарный знак – доменное имя, а также вопрос злоупотреблений при регистрации доменов (cybersquatting). Именно по этой сетевой проблеме на Западе уже сейчас имеется большое количество судебных решений.

Торговля доменными именами стала прибыльным, хотя и неофициальным бизнесом в Интернете. Такие «коммерсанты» (их называют хаперами, или скваттерами) регистрируют на свое имя звучные и привлекательные домены, а затем перепродают их. Например, компания Multimedia Publishing заплатила за домен http://www.business.com $150 тыс., а чуть позже он был выставлен на аукцион по цене уже в $7,5 млн.

Очень важной проблемой сети Интернет является определение ответственности провайдеров и владельцев сайтов за содержание находящихся на их серверах информации клиентов и пользователей. В ряде стран уже принято несколько специфических нормативно-правовых актов, регулирующих указанные отношения, и правоприменительная практика приобретает ярко выраженную национальную дифференциацию, что вступает в противоречие с всемирным характером сети Интернет.

Пятой группой правоотношений, отражающей специфичность регулирования сети Интернет, являются многогранные вопросы информационной безопасности, включающие в себя криптографию, шифрование (эти аспекты детально регламентированы в России), обеспечение безопасности доступа к данным, охрану интересов частной жизни.

К данной группе примыкают вопросы нравственности и цензуры (как частной, так и сетевых социальных групп, а также государств и организаций).

Вопросы защиты информации и безопасности корпоративных компьютерных сетей во всех развитых странах мира достаточно жестко регулируются законодательством. Как правило, это регулирование касается трех сторон применения средств защиты информации (СЗИ):

– сертификация СЗИ;

– лицензирование деятельности в области защиты информации и работ, связанных с созданием СЗИ;

– экспортно-импортные ограничения на СЗИ.

Цель такого регулирования очевидна: для обеспечения собственной безопасности любому государству необходим максимальный контроль за стратегическими информационными ресурсами.

В этом смысле российское законодательство не является исключением и имеет ряд законодательных актов и инициатив, призванных регулировать использование СЗИ на территории России. Например, в рамках серии руководящих документов Гостехкомиссии при Президенте РФ подготовлен ряд документов, регламентирующих вопросы деятельности в области защиты информации. Среди этих документов наибольший интерес для корпоративных пользователей представляют следующие:

«Защита от несанкционированного доступа к информации. Термины и определения» (М., 1992); «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», (М., 1992); «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации» (М., 1997).

Однако специфика интернет/интранет-технологий заключается в том, что они развиваются весьма быстро. Поэтому нормативно-правовая, а, следовательно, и техническая база компьютерной безопасности любого государства практически всегда отстает от потребностей рынка корпоративных заказчиков, что и подтверждается следующими фактами.

По данным Института компьютерной безопасности США (CSI – Computer Security Institute, San Francisco; http://www.gocsi.com) и группы компьютерного вторжения (Computer Intrusion Squard) Федерального бюро расследований (ФБР – FBI, San Francisco; http://www.fbi.gov), 90 % всех опрошенных в США корпоративных респондентов обнаружили атаки на свои сети, 273 корпорации понесли финансовые убытки на общую сумму $265 589 940. Полный совместный отчет CSI/FBI «2000. Компьютерные преступления. Обзор безопасности» содержит по-настоящему сенсационные статистические данные:

– 90 % опрошенных представителей крупных корпораций и правительственных организаций сообщили о незаконном проникновении в свои компьютерные сети;

– 70% сообщили о хищении информации и финансовом мошенничестве;

– 74% понесли значительные финансовые убытки в результате взлома их сети;

– 27% обнаружили атаки типа «отказ в обслуживании» (deneal of service);

– 79% сообщили о несанкционированном доступе или других нарушениях безопасности;

– 35% были не в состоянии ответить, подвергались ли они компьютерным атакам за отчетный период;

– 85% обнаружили компьютерные вирусы.

В целом статистические данные текущих отчетов по компьютерной безопасности показывают, что за последние три года соотношение между атаками из Интернета (59 %) и внутренними атаками (38 %) изменилось в пользу внешних атак. Поэтому не случайно проблема интернет-преступности впервые за время существования компьютерных технологий удостоилась внимания ООН. На проходившем недавно в Вене X Конгрессе ООН тема компьютерных преступлений в Интернете стала темой номер один.

Для локализации этой проблемы страны «большой восьмерки» активировали свою деятельность в области защиты информации и в настоящее время вырабатывают общую стратегию борьбы с компьютерными преступлениями, обсуждают проекты разработки новых технологий слежения за нарушениями и быстрого реагирования на них служб безопасности компьютерных сетей.

В России для борьбы с компьютерными преступлениями в 1998 г. было создано специальное управление МВД РФ под литерой «Р». В целом вопросами защиты информации корпоративных сетей на территории РФ занимаются следующие государственные организации: ФСБ, ФАПСИ и Гостехкомиссия.

В России большая часть отношений между участниками электронной коммерции до сих пор не регулируется специальными, адресованными им законами или иными источниками права. В настоящее время электронная торговля представлена терминами «электронный документ», «электронная форма сделки», «электронная подпись», «электронные расчеты», которые в основном используются в подзаконных актах.

Общепризнанный и важнейший правовой принцип электронной торговли – не ставить под сомнение действительность и обязательность сделки только на том основании, что она заключена электронным способом.

На практике создаются и постоянно модифицируются разного рода соглашения об электронном обмене данными или об электронном документообороте, в большей или меньшей степени соответствующие действующему законодательству. Однако такие соглашения в случаях судебного разбирательства могут быть непризнанными или не принимаемыми в качестве

доказательств. Многие сделки действующим законодательством разрешается заключать только традиционным способом на бумаге и заверенными собственноручными подписями. Единственный документ, хоть как-то регулирующий сделки, это временное положение ЦБ РФ № 17-п «О порядке приема к исполнению поручений владельцев счетов, подписанных аналогами собственноручной подписи, при проведении расчетов кредитными организациями». Это положение позволяет осуществлять на территории России денежные переводы в Интернете с использованием систем «банк – клиент».

В целом же сохраняется общая неразвитость и фрагментарность правовых норм, затрагивающих названную форму бизнеса, что является юридическим барьером для электронной коммерции в России и интеграции ее в глобальный электронный рынок.

В настоящее время законодательство в сфере информации и информатизации представлено следующими действующими федеральными законами: «О средствах массовой информации», «Об информации, информатизации и защите информации», «О связи», «Об архивном фонде Российской Федерации и архивах (основы законодательства)», «О библиотечном деле», «О статистической деятельности в Российской Федерации», «Об обязательном экземпляре документов», «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», «Об освещении деятельности органов государственной власти в государственных средствах массовой информации», «О государственной поддержке, районных газет», «О почтовой связи», «О фельдъегерской связи», «Об участии в международном информационном обмене», «Патентный закон», «Об авторском праве и смежных правах», «О правовой охране программ для электронно-вычислительных машин и баз данных», «О правовой охране топологий интегральных микросхем», «О государственной тайне», «О рекламе», «О федеральных органах правительственной связи и информации», «Гражданский кодекс Российской Федерации» (соответствующие статьи), «Уголовный кодекс Российской Федерации» (соответствующие статьи). Недавно принят закон «Об электронной цифровой подписи».

Закон об электронно-цифровой подписи (ЭЦП) решает несколько важнейших юридических задач.

Во-первых, это принципиальное признание ЭЦП в качестве аналога собственноручной подписи для значительно более широкого круга юридических действий, чем предусмотрено в ГК РФ, который формально признает ЭЦП только в связи с заключением сделок. Закон также дает возможность легального использования ЭЦП в качестве функционального эквивалента собственноручной подписи в случаях, когда это прямо не запрещено законодательством.

Во-вторых, закон устанавливает требования, при соблюдении которых электронная цифровая подпись считается равнозначной собственноручной подписи лица.

В-третьих, данный закон снимает противоречия и неопределенности в отношении ЭЦП, которые есть в иных законах.

Кроме этого, деятельность в данной сфере регулируется указами Президента, а также нормативно-правовыми актами органов связи, ФАПСИ, Гостехкомиссии, а также других органов исполнительной ветви власти. Существует также ряд международных соглашений, подписанных Россией, регламентирующих смежные с сетью Интернет правоотношения (в первую очередь связанные с использованием объектов интеллектуальной собственности).

Вышеприведенные особенности правового регулирования использования информационного пространства порождают ряд предложений, раскрывающих возможные пути решения проблем взаимодействия реального и информационного мира. Среди них необходимо выделить следующие: правовые – создание рамочного акта, содержащего основные юридические определения и принципы использования норм права; технические – разработка и внедрение общедоступных государственных систем поиска с индексацией информации, а также систем депонирования информации; организационные – свободный доступ в сегменты Сети с условием соблюдения законов; политические – обеспечение участия России в создании протоколов и стандартов Интернета.

9.3. Принципы создания системы информационной безопасности электронной коммерции

Принципы создания и функционирования системы обеспечения безопасности можно разбить на три основные блока:

– общие принципы обеспечения безопасности;

– организационные принципы;

– принципы реализации системы безопасности.

Общие принципы обеспечения безопасности:

– *принцип неопределенности* обусловлен тем, что при обеспечении защиты неизвестно, кто, когда, где и каким образом попытается нарушить безопасность объекта защиты;

– *принцип невозможности создания идеальной системы защиты* следует из принципа неопределенности и ограниченности ресурсов, которыми, как правило, располагает система безопасности;

– *принцип минимального риска* заключается в том, что при создании системы защиты необходимо выбирать минимальную степень риска, исходя из особенностей угроз безопасности доступных ресурсов и конкретных условий, в которых находится объект защиты в любой момент времени;

– *принцип защиты всех от всех* предполагает необходимость защиты всех субъектов отношений против всех видов угроз.

Организационные принципы:

– *принцип законности,* важность которого трудно переоценить в условиях возникновения новых правоотношений в российском законодательстве – «частная собственность», «интеллектуальная собственность», «коммерческая тайна» и др. Однако нормативная правовая база, регламентирующая вопросы обеспечения безопасности, пока несовершенна;

– *принцип персональной ответственности* предполагает ответственность каждого сотрудника фирмы за обеспечение режима безопасности в рамках своих полномочий. Ответственность за нарушение режима безопасности должна быть заранее конкретизирована и персонифицирована;

– *принцип разграничения полномочий* позволяет снизить вероятность нарушения коммерческой тайны или нормального

функционирования предприятия, так как она прямо пропорциональна количеству осведомленных лиц, обладающих информацией. Поэтому никого не следует знакомить с конфиденциальной информацией, если этого не требуется для выполнения его должностных обязанностей;

– *принцип взаимодействия и сотрудничества* предполагает наличия на предприятии доверительных отношений между сотрудниками на основе понимания всеми необходимости выполнения мероприятий обеспечения безопасности информации в своих же собственных интересах.

Принципы реализации системы защиты:

– *принцип комплексности и индивидуальности* предполагает обеспечение безопасности совокупностью комплексных, взаимосвязанных и дублирующих друг друга мероприятий, реализуемых с индивидуальной привязкой к конкретным условиям;

– *принцип последовательности рубежей* позволяет своевременно обнаружить и посягательство на безопасность и организовать последовательное противодействие угрозе в соответствии со степенью опасности;

– *принцип защиты средств защиты* является логическим продолжением принципа защиты всех от всех. Иначе говоря, любое мероприятие по защите само должно быть соответственно защищено. Например, средство защиты от попыток внести изменения в БД должно быть защищено программным обеспечением, реализующим разграничение прав доступа.

Реализация названных принципов и построение комплексной системы защиты объектов является в общем случае индивидуальной задачей, что обусловлено экономическими соображениями и состоянием, в котором находится объект защиты, а также многими другими обстоятельствами.

9.4. Международный стандарт ISO 27001

Международный стандарт ISO 27001 является стандартом де-факто в области менеджмента информационной безопасности (ИБ) [6]. Требования данного стандарта могут быть применены

любыми организациями, независимо от их отрасли и сферы деятельности, используемых технологий.

Система управления ИБ, соответствующая требованиям ISO 27001, обеспечивает взаимосвязь между уровнем принятия бизнес-решений и операционным уровнем обеспечения ИБ, что делает обеспечение информационной безопасности эффективным, соответствующим требованиям бизнеса и адекватным возникающим угрозам.

Внедрение комплексной системы управления информационной безопасностью, соответствующей требованиям ISO, позволяет:

– оптимизировать расходы на информационную безопасность;

– снизить риски, связанные с возможными ущербами для активов организации при реализации угроз ИБ;

– снизить операционные затраты на ИБ за счет повышения прозрачности процессов ИБ;

– обеспечить уровень ИБ законодательным, отраслевым, контрактным, внутрикорпоративным требованиям и целям бизнеса.

В стандарте ISO 27001 указаны три группы факторов, которые необходимо учитывать при формировании требований в области информационной безопасности:

– оценка рисков организации. Посредством оценки рисков происходит выявление угроз активам организации, оценка уязвимости соответствующих активов и вероятности возникновения угроз, а также оценка возможных последствий;

– юридические, законодательные, регулирующие и договорные требования, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг;

– специфический набор принципов, целей и требований, разработанных организацией в отношении обработки информации.

Полный российский аналог международного стандарта ISO/IEC 27001:2005 – «ГОСТ Р ИСО/МЭК 27001-2006 – Информационная технология – Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности – Требования». По сути, данные стандарты – это набор

лучших практик по управлению информационной безопасностью в различных организациях.

В стандарте приводится перечень мероприятий по управлению информационной безопасностью, однако этот перечень может быть изменен, исходя из потребностей организации. В связи с тем, что ISO 27001 является стандартом универсальным, то есть применимым к любой организации, а значит, не учитывающим специфику отрасли, этот перечень может быть изменен, исходя из потребностей организации.

Выбор мероприятий по управлению информационной безопасностью должен основываться на соотношении стоимости их реализации, эффекта от снижения рисков и возможных убытков в случае нарушения безопасности. Также следует принимать во внимание факторы, которые не могут быть представлены в денежном выражении, например, потерю репутации. В соответствии со стандартом рекомендуется на первом этапе разрабатывать политику безопасности организации, которая должна быть утверждена руководством и доведена до сведения всех сотрудников организации. Разработкой политики безопасности должны заниматься управляющие советы. За соблюдение политики безопасности должны нести персональную ответственность назначенные приказом лица. Также политика безопасности требует учета всех информационных активов организации и их закрепления за соответствующими ответственными лицами. Для учета информационных активов может быть использована следующая классификация:

– информационные активы (базы данных и файлы данных, системная документация и т.д.);

– активы программного обеспечения (прикладное программное обеспечение, системное программное обеспечение, инструментальные средства разработки и утилиты);

– физические активы (компьютерное оборудование, оборудование связи, носители информации, другое техническое оборудование, мебель, помещения);

– услуги (вычислительные услуги и услуги связи, основные коммунальные услуги).

Для определения необходимости и степени защиты информации нужно провести ее анализ на приоритетность и кри-

тичность для организации, например, с точки зрения ее целостности и доступности.

В политике безопасности необходимо четко прописывать права каждого пользователя и правила контроля доступа. При использовании парольной идентификации должен быть прописан порядок осуществления контроля в отношении паролей пользователей. Требуется обеспечить безопасность процесса получения пароля пользователем и, если это используется, управления пользователями своими паролями (принудительная смена пароля после первого входа в систему и т.д.).

Также в отношении каждого пользователя должен быть прописан порядок доступа к сетевым сервисам – внутренним и внешним. Доступ должен обеспечиваться только к разрешенным для конкретного пользователя сервисам. Особое внимание должно уделяться проверке подлинности удаленных пользователей.

В политике безопасности должны быть указаны применяемые средства обеспечения информационной безопасности как на уровне операционной системы, так и на уровне приложений. Также в политике безопасности должен быть определен регламент проведения мониторинга для обнаружения отклонений от прописанных в ней требований безопасности. Результаты мониторинга следует регулярно анализировать, а журнал аудита может использоваться для расследования инцидентов.

В разделе «Разработка и обслуживание систем» стандарта ISO 27001 указывается на необходимость учета требований информационной безопасности на этапе разработки ИС и предотвращения потерь, модификации или неправильного использования пользовательских данных на этапе эксплуатации ИС. Для обеспечения конфиденциальности, целостности и аутентификации данных могут быть использованы криптографические средства защиты.

Важную роль в процессе защиты информации играет обеспечение целостности программного обеспечения. Чтобы свести к минимуму повреждения информационных систем, следует строго контролировать внедрение изменений. В этих случаях необходимо проводить анализ и тестировать прикладные системы с целью обеспечения уверенности в том, что не

будет оказано никакого неблагоприятного воздействия на их функционирование и безопасность. Насколько возможно, готовые пакеты программ рекомендуется использовать без внесения изменений.

Одним из методов противодействия «троянским» программам и использованию скрытых каналов утечки является использование программного обеспечения, полученного от доверенных поставщиков, и контроль целостности системы. В случаях, когда для разработки программного обеспечения привлекается сторонняя организация, необходимо предусмотреть меры по контролю качества и правильности выполненных работ.

Заключительный раздел стандарта посвящен вопросам соответствия ИС требованиям. В первую очередь, это касается соответствия ИС и порядка ее эксплуатации требованиям законодательства:

– соблюдения авторского права (в том числе, на программное обеспечение);

– защиты персональной информации (сотрудников, клиентов);

– предотвращения нецелевого использования средств обработки информации.

При использовании криптографических средств защиты информации они должны соответствовать действующему законодательству. Также должна быть досконально проработана процедура сбора доказательств на случай судебных разбирательств, связанных с инцидентами в области безопасности ИС.

Сами информационные системы должны соответствовать политике безопасности организации и используемым стандартам. Безопасность информационных систем необходимо регулярно анализировать и оценивать.

В то же время требуется соблюдать меры безопасности и при проведении аудита безопасности, чтобы это не привело к нежелательным последствиям (например, сбой критически важного сервера из-за проведения проверки).

Стандарт ISO 27001 затрагивает широкий круг вопросов, связанных с обеспечением безопасности информационных си-

стем, и представляет собой набор лучших практических рекомендаций по информационной безопасности.

С этой точки зрения и необходимо рассматривать данный документ специалистам по информационной безопасности большинства российских предприятий. Прохождение аудита на соответствие международным требованиям безопасности целесообразно лишь предприятиям и организациям, которые планируют выход на международную арену.

9.5. Способы оценки эффективности системы безопасности электронной коммерции

Угрозы безопасности обычно связаны с действиями факторов, значение и влияние которых практически всегда неизвестно. Присутствие такой неопределенности и ограниченность доступных ресурсов и средств не позволяют создать абсолютно безопасную систему. Поэтому при создании системы информационной безопасности электронной коммерции необходимо:

– минимизировать степень риска возникновения ущерба, исходя из особенностей угроз безопасности и конкретных условий предприятия, занимающегося электронной коммерцией;

– основываться на принципе достаточности, который заключается в том, что проводимые в интересах обеспечения информационной безопасности электронной коммерции мероприятия с учетом потенциальных угроз должны быть минимальны и достаточны.

Затраты на обеспечение информационной безопасности должны соответствовать существующим угрозам, иначе система безопасности будет экономически неэффективна. В соответствии с этим для обоснования эффективности мероприятий по обеспечению информационной безопасности электронной коммерции применяется ряд критериев, так или иначе основанных на сравнении убытков, возникающих при нарушении безопасности, и стоимости проведения мероприятий по обеспечению информационной безопасности электронной коммерции.

9.5.1. Классификация убытков

Убытки, которые могут возникать на предприятии, занимающемся электронной коммерцией, из-за нарушения информационной безопасности, можно разделить на прямые и косвенные.

Прямые убытки могут быть выражены:

– в стоимости восстановления поврежденной или физически утраченной информации в результате пожара, стихийного бедствия, кражи, ограбления, ошибки в эксплуатации, неосторожности обслуживающего персонала, взлома компьютерных систем и действий вирусов;

– в стоимости ничтожных (незаконных) операций с денежными средствами и ценными бумагами, проведенных в электронной форме путем несанкционированного проникновения в компьютерные системы и сети, а также злоумышленной модификации данных, преднамеренной порчи данных на электронных носителях при хранении, перевозке или перезаписи информации, передачи и получения сфальсифицированных поручений в сетях электронной передачи данных и др.;

– в стоимости возмещения причиненного физического и/или имущественного ущерба третьим лицам (субъектам электронной коммерции – клиентам, пользователям).

При пожарах, стихийных бедствиях и других событиях могут возникать убытки, напрямую не связанные с информационной безопасностью, например, убытки, определяемые стоимостью утраченного оборудования или расходами на восстановление поврежденного оборудования.

Косвенные убытки могут выражаться в текущих расходах на выплату заработной платы, процентов по кредитам, арендной платы, амортизации и потерянной прибыли, возникающих при вынужденной приостановке коммерческой деятельности предприятия из-за нарушения безопасности предприятия.

Убытки и связанные с их возникновением риски относятся к финансовым категориям, методики экономической оценки которых разработаны и известны. Поэтому мы не будем останавливаться на их подробном анализе.

9.5.2. Критерии эффективности систем защиты

Можно выделить два основных критерия, позволяющих оценить эффективность системы защиты:

– отношение стоимости системы защиты (включая текущие расходы на поддержание работоспособности этой системы) к убыткам, которые могут возникнуть при нарушении безопасности;

– отношение стоимости системы защиты к стоимости взлома этой системы с целью нарушения безопасности.

Смысл указанных критериев заключается в следующем: если стоимость системы защиты, обеспечивающей заданный уровень безопасности, оказывается меньше затрат по возмещению убытков, понесенных в результате нарушения безопасности, то мероприятия по обеспечению безопасности считаются эффективными.

Уровень безопасности при этом в силу объективной неопределенности факторов, влияющих на безопасность, оценивается, как правило, вероятностными показателями.

Таким образом, если, например, злоумышленник в процессе разработки мероприятий по нарушению безопасности обнаружит, что затраты, которые он понесет, будут сравнимы с убытками, которые он причинит фирме, то он, вероятно, откажется от своих планов. При этом он будет, конечно, продолжать искать брешь в системе безопасности, чтобы повысить эффективность своих действий.

9.6. Требования к электронным системам оплаты

Коммерциализация Интернета настоятельно требует наличия электронной системы оплаты.

Как и при традиционных методах оплаты, главная проблема электронных платежей состоит в том, что нельзя гарантировать стопроцентную защищенность от хищения информации кредитных карточек и электронных денег.

Для обеспечения успешного функционирования электронной системы оплаты необходимо, чтобы она отвечала следующим требованиям:

– *приемлемость* – система оплаты будет тем более успешной, чем шире круг покупателей и продавцов, которые согласны ею пользоваться;

– *анонимность* – по желанию клиентов необходимо обеспечить конфиденциальность информации личного характера;

– *конвертируемость* – участники финансовых операций должны иметь возможность свободно конвертировать электронные деньги в активы других типов;

– *эффективность* – стоимость транзакции должна приближаться к нулевой;

– *гибкость* – необходима поддержка нескольких способов оплаты;

– *интегрируемость* – чтобы обеспечить поддержку существующих в компании приложений, следует разработать интерфейсы для интеграции с приложением электронной оплаты;

– *надежность* – система оплаты должна быть широкодоступной и не содержать звеньев, которые могут допустить сбой в работе;

– *масштабируемость* – увеличение числа покупателей и торговцев, использующих систему оплаты, не должно приводить к разрушению инфраструктуры;

– *безопасность* – система должна допускать проведение финансовых транзакций через открытые сети, такие как Интернет;

– *удобство и простота* – процесс оплаты должен быть таким же простым, как и в реальном мире.

При использовании электронных систем оплаты на первый план выходит обеспечении информационной безопасности. Системы электронных платежей – самая соблазнительная добыча для мошенников всего мира. В случае покупки в магазине вы перелаете деньги продавцу, а при оплате через Интернет ваши деньги могут оказаться на совершенно посторонних банковских счетах, причем мошенничество удается обнаружить далеко не сразу. Таким образом, для обеспечения безопасности любой финансовой операции необходимо прибегать к защите с помощью цифровых подписей и технологий кодирования.

Если вы получаете электронные деньги, у вас всегда должна быть возможность перевести их в банк или партнеру для

безопасного хранения. Они должны приниматься так же, как кредитная карточка или наличные деньги, для чего требуется высокий уровень приемлемости используемой платежной системы.

Финансовые транзакции в Интернете требуют соблюдения конфиденциальности. Требование конфиденциальности может быть выдвинуто одной или всеми участвующими сторонами, поэтому необходимо добиться такого уровня защищенности, чтобы посторонние ни в коем случае не смогли перехватить транзакцию; а если им это удастся, транзакция не должна быть читаемой, другими словами, ее следует защитить с помощью кодирования. Личность покупателя, компания-продавец, а также содержание заказа должны быть известны только сторонам-участницам; более того, каждый из участников сделки должен знать только то, что ему положено знать.

Необходимо обеспечение целостности и аутентификации финансовых операций. Сообщение покупателя, отправляемое продавцу, должно быть снабжено подписью – это гарантия того, что никто из посторонних не сможет снять деньги со счета или кредитной карточки этого покупателя без его согласия. Каждое сообщение должно быть уникальным, чтобы финансовая операция могла выполняться только один раз, по завершении транзакции продавец посылает покупателю подтверждение.

Компания должна гарантировать доступность и надежность своей системы оплаты. Прерывание соединения при совершении оплаты однозначно приводит к потерям для всех участвующих сторон. Система должна обеспечить проведение финансовых операций всем сторонам и в любой момент. Надежность транзакции лучше всего обеспечивается ее простотой.

Транзакция никогда не должна оставаться незавершенной. Независимо от того, принимается платеж или отклоняется, никогда не должно возникать состояние неопределенности, которое может привести к потере денег в Интернете. Платежный протокол должен уметь обрабатывать отказы сети или включенных в нее компьютеров, в большинстве случаев вся транзакция аннулируется и ее приходится повторять, однако некоторые платежные системы после восстановления штатного режима

работы могут продолжать процесс с того момента, на котором он был прерван.

В системах оплаты, имитирующих оплату наличными, необходимо обеспечивать анонимность и невозможность отслеживания движения наличности. Это осуществимо только в случае, если в транзакции не участвует третья сторона. Анонимность позволяет скрыть личность покупателя, а невозможность отслеживания означает, что разные платежи, выполненные одним и тем же покупателем, нельзя связать между собой или установить по ним личность этого покупателя. В системе должна отсутствовать возможность выявления структуры потребления некоего лица или определения его источников дохода. С помощью кодирования всех сообщений, которыми обмениваются участники финансовой операции, можно сделать содержание транзакции недоступным для посторонних, и в большинстве случаев этого вполне достаточно. С другой стороны, такой подход обеспечивает также анонимность и невозможность отслеживания личности продавца. Если анонимность является ключевым требованием, расходы на отслеживание транзакции должны превышать ценность информации, которую можно получить в результате такого отслеживания.

С развитием Интернета требования, предъявляемые к электронным системам оплаты, будут также расти. Платежная система должна быть выстроена таким образом, чтобы увеличение числа покупателей и продавцов не привело к снижению эффективности. Для повышения устойчивости следует отдавать предпочтение распределенным системам, когда серверы, участвующие в процессе оплаты через Интернет, размещаются в разных точках Сети; так повышается уровень отказоустойчивости системы в случае прерывания одного из соединений или выхода из строя одного из серверов.

Инфраструктура системы оплаты должна поддерживать существующие интернет-приложения через программируемый интерфейс, чтобы не вносить изменения в приложения или, если без изменений все же не обойтись, ограничиться минимальными.

9.7. Классификация типов мошенничества в электронной коммерции

Международные платежные системы приводят следующую классификацию возможных типов мошенничества через Интернет:

– транзакции, выполненные мошенниками с использованием правильных реквизитов карточки (номер карточки, срок ее действия и т.п.);

– компрометация данных (получение данных о клиенте через взлом баз данных (БД) торговых предприятий или путем перехвата сообщений покупателя, содержащих его персональные данные) с целью их использования в мошеннических целях;

– магазины, возникающие, как правило, на непродолжительное время для того, чтобы исчезнуть после получения от покупателей средств за несуществующие услуги или товары;

– злоупотребления торговых предприятий, связанные с увеличением стоимости товара по отношению к предлагавшейся покупателю цене или повторными списаниями со счета клиента;

– магазины и торговые агенты (Acquiring Agent), предназначенные для сбора информации о реквизитах карт и других персональных данных покупателей.

Коротко остановимся на перечисленных типах мошенничества в отдельности. Как уже отмечалось, первый тип мошенничества является наиболее массовым. Для совершения транзакции мошеннику обычно достаточно знать только номер карты и срок ее действия. Такая информация попадает в руки мошенников различными путями. Наиболее распространенный способ получения мошенниками реквизитов карт – сговор с сотрудниками торговых предприятий (ТП), через которые проходят сотни и тысячи транзакций по пластиковым картам. Результатом сговора становится передача информации о реквизитах карт в руки криминальных структур.

Другой способ получения информации о реквизитах карт, ставший популярным в последнее время, это кража баз данных карточек в ТП. Еще одним способом генерации правильного номера карты являются специальные программы. Программа генерирует правильные номера карт, эмитированных некоторы-

ми банками, используя для генерации номеров тот же алгоритм, что и банк-эмитент.

Достаточно распространенным является способ, когда криминальные структуры организуют свои магазины, главной целью которых является получение в свое распоряжение значительных наборов реквизитов карт.

Другая функция подобных магазинов состоит в их использовании для «отмывания» полученных реквизитов карт. Через подобные сайты «прокачиваются» сотни тысяч и даже миллионы украденных реквизитов карт.

Наконец, существует и еще один способ узнать правильные реквизиты карт. Точнее не узнать, а эмпирически вычислить. Дело в том, что Интернет представляет собой прекрасный плацдарм для проведения различного рода «испытаний» с целью определения правильных реквизитов карт. Например, если мошеннику известен номер карты, но не известен срок ее действия, то определить этот параметр карты не составляет большого труда.

Действительно, пластиковая карта обычно выпускается сроком на два года. Параметр «срок действия карты» определяет месяц и последние две цифры года, когда действие карты заканчивается. Таким образом, мошеннику требуется перебрать всего лишь 24 возможных варианта этого параметра. В реальном мире сделать это не просто. В виртуальном мире решение подобной задачи не составляет труда. Мошеннику нужно отправить не более 24 авторизационных запросов для того, чтобы со 100 %-й вероятностью определить верный срок действия карты. После этого воспользоваться известными реквизитами карты можно различными способами. Проще всего совершить транзакцию. Более эффективный способ воспользоваться добытым знанием – изготовить поддельную карту с вычисленными реквизитами карты и использовать ее для оплаты покупок в реальных ТП. В этом случае такое мошенничество попадет в разряд «подделанная карта» (Counterfeit).

Остановимся на третьем типе мошенничества – магазинах-бабочках, открывающихся с целью «отмывания» украденных реквизитов карт. После того, как в руках криминальных структур появляются украденные реквизиты карт, возникает задача ими воспользоваться. Один из способов – организация

виртуального ТП, «торгующего» программным обеспечением или другими информационными ресурсами (программы телевизионных передач, подписка на новости и т.д.). В действительности такое ТП, как правило, имеет свой сайт, но ничем реально не торгует. При этом в обслуживающий банк регулярно направляются авторизационные запросы, использующие украденные номера карт. Следовательно, магазин регулярно получает от обслуживающего банка возмещения за совершенные в нем «покупки». Так продолжается до тех пор, пока уровень chargeback (отказов от платежей) от эмитентов украденных реквизитов карт не станет свидетельством того, что имеет место мошенничество. Обычно к этому моменту и сами магазины, понимая, что в скором времени к ним возникнут вопросы со стороны правоохранительных органов, исчезают и становятся предметом поиска для правоохранительных органов.

Магазины-бабочки обычно выбирают две крайние стратегии своей работы. Выбор стратегии определяется размером украденной БД карточек.

Если размер украденной БД достаточно большой (десятки тысяч карт), то выбирается стратегия, в соответствии с которой транзакции делаются на небольшие суммы (порядка $10 США). Основная идея такой стратегии заключается в том, что действительный владелец кар заметит небольшую потерю средств на своем счете далеко не сразу и в результате за имеющееся в распоряжении мошенников время (как правило, 1–3 месяца) можно на подобных небольших транзакциях украсть сотни тысяч долларов.

Наоборот, когда в распоряжении мошенников несколько десятков карт, выбирается стратегия выполнения транзакций на крупные суммы (несколько тысяч долларов). В этом случае активная жизнь магазина- бабочки составляет несколько недель, после чего магазин исчезает.

9.8. Способы решения проблемы безопасности в электронной коммерции

С самого начала внедрения электронной коммерции (ЭК) стало очевидно, что методы идентификации владельца карты, применяемые в обычных транзакциях, являются неудовлетворительными для транзакций ЭК.

Действительно, при совершении операции покупки в физическом магазине продавец имеет возможность рассмотреть предъявляемую для расчетов пластиковую карту на предмет ее соответствия требованиям платежным системам (в частности, проверить наличие голограммы, специальных секретных символов, сверить подпись на панели подписи и торговом чеке и т.п.). Кроме того, продавец может потребовать от покупателя документ, удостоверяющий его личность. Все это делает мошенничество по поддельной карте достаточно дорогим мероприятием.

В случае транзакции в ЭК все, что требуется от мошенника, это знание реквизитов карты. Затраты, связанные с изготовлением поддельной физической карты, в этом случае не требуются. Безусловно, это не может не привлечь внимание криминала к этому типу коммерции.

В мире пластиковых карт с магнитной полосой самым надежным способом защиты транзакции от мошенничества является использование PIN-кода для идентификации владельца карты его банком-эмитентом.

Секретной информацией, которой обладает владелец карты, является PIN-код. Он представляет собой последовательность, состоящую из 4–12 цифр, известную только владельцу карты и его банку-эмитенту. PIN-код применяется всегда при проведении транзакций повышенного риска, например при выдаче владельцу карты наличных в банкоматах. Выдача наличных в банкоматах происходит без присутствия представителя обслуживающего банка (ситуация похожа на транзакцию в ЭК). Поэтому обычных реквизитов карты для защиты операции «снятие наличных в банкомате» недостаточно и используется секретная дополнительная информация, т.е. PIN-код.

Более того, общая тенденция развития платежных систем – более активное использование PIN-кода для операций «покупка» по дебетовым картам. Казалось бы, использование подобно-

го идентификатора могло бы помочь решить проблему безопасности в ЭК, однако это не так. К сожалению, в приложении к ЭК этот метод в классическом виде неприменим.

Действительно, использование PIN-кода должно производиться таким образом, чтобы этот секретный параметр на всех этапах обработки транзакции оставался зашифрованным (PIN-код должен быть известен только владельцу карты и ее эмитенту). В реальном мире это требование реализуется за счет использования в устройствах ввода транзакции специальных физических устройств, называемых PIN – PAD и содержащих Hardware Security Module – аппаратно-программные устройства, позволяющие хранить и преобразовывать некоторую информацию весьма надежным способом. Эти устройства хранят специальным способом защищенный секретный коммуникационный ключ, сгенерированный обслуживающим банком данного ТП. Когда владелец карты вводит значение PIN-кода, оно немедленно закрывается (шифруется) коммуникационным ключом и отправляется внутри авторизационного запроса на хост обслуживающего банка. Точнее говоря, шифруется не сам PIN-код, а некоторый электронный «конверт», в который код помещается. На хосте обслуживающего банка зашифрованный идентификационный код перекодируется внутри Hardware Security Module хоста (хост обслуживающего банка также имеет свое устройство шифрования) в блок, зашифрованный на коммуникационном ключе платежной системы, и передается в сеть для дальнейшего предъявления эмитенту. По дороге к эмитенту PIN-код будет преобразовываться еще несколько раз, но для понимания процесса это неважно. Важно другое – для того, чтобы следовать классической схеме обработки PIN-кода, каждый владелец карты должен хранить криптограммы коммуникационных ключей всех обслуживающих банков, что на практике невозможно.

Классическую схему можно было бы реализовать с помощью применения асимметричных алгоритмов с шифрованием PIN-кода владельца карты открытым ключом ТП. Однако для представления PIN-кода в платежную сеть его необходимо зашифровать, как это принято во всех платежных системах, симметричным ключом. Однако в настоящее время неизвестно ни одного стандартного Hardware Security Module, способного выполнить трансляцию PIN-кода, зашифрованного с помощью

асимметричного крипто алгоритма, в PIN-код, зашифрованный на симметричном алгоритме шифрования.

Существует другое, неклассическое решение по использованию PIN – кода. Например, можно на компьютере владельца карты шифровать PIN-код плюс некоторые динамически меняющиеся от транзакции к транзакции данные на ключе, известном только эмитенту и владельцу карты. Такой подход потребует решения задачи распределения секретных ключей. Эта задача является весьма непростой (очевидно, что у каждого владельца карты должен быть свой индивидуальный ключ), и если уж она решается, то использовать ее решение имеет смысл для других, более эффективных по сравнению с проверкой PIN-кода методов аутентификации владельца карты.

В то же время идея проверки PIN-кода была реализована для повышения безопасности транзакций в ЭК по картам, БД которых хранится на хосте процессора STB CARD. В общих чертах STB CARD реализует следующую схему. Владельцы карт, эмитенты которых держат свою БД карточек на хосте STB CARD, могут получить дополнительный PIN-код, называемый PIN2. Этот код представляет собой последовательность из 16 шестнадцатеричных цифр, которая распечатывается в PIN-конверте, передаваемом владельцу карты (специальный бумажный конверт, используемый банком-эмитентом для хранения в нем секретной информации, относящейся к эмитированной карте), и вычисляется эмитентом с помощью симметричного алгоритма шифрования, примененного к номеру карты и использующего секретный ключ, известный только эмитенту карты.

Далее во время проведения транзакции в ЭК на одном из ТП, обслуживаемом банком STB CARD, у владельца карты в процессе получения данных о клиенте запрашивается информация по PIN2. Клиент вводит значение кода PIN2 в заполняемую форму и возвращает ее ТП.

Здесь нужно сделать важное замечание относительно сказанного ранее.

Владелец карты в действительности ведет диалог в защищенной SSL-сессии не с ТП, а с виртуальным POS-сервером, через который работает ТП (система STB CARD в настоящее время использует сервер Assist).

Защита от подставки (если форма, запрашивающая PIN2, предоставляется владельцу карты не ТП, а мошенником, желающим узнать значение PIN2) основана на надежности аутентификации клиентом сервера ТП, а также на подписании апплета секретным ключом сервера ТП. Поскольку нарушение обеих защит приводит только к появлению на экране монитора владельца карты соответствующего предупреждения, сопровождаемого вопросом – продолжить сессию или нет, то особенно доверять этим формам защиты не стоит. Обеспечить надежную защиту от подставки можно с помощью электронного бумажника клиента (специального программного обеспечения, которое клиент может «скачать» на свой компьютер с некоторого сайта), заменяющего по своей функциональности Java-апплет в форме ТП. Такой электронный бумажник может использовать сколь угодно мощные средства шифрования данных. Секретные ключи владельца карты могут держаться в порядке повышения надежности их хранения на диске компьютера, дискете или микропроцессорной карте. Доступ к электронному бумажнику должен производиться по паролю его владельца.

В результате проведенного анализа платежные системы сформировали основные требования к схемам проведения транзакции в ЭК, обеспечивающим необходимый уровень ее безопасности:

1. Аутентификация участников покупки (покупателя, торгового предприятия и его обслуживающего банка). Под аутентификацией покупателя (продавца) понимается процедура, доказывающая (на уровне надежности известных крипто алгоритмов) факт того, что данный владелец карты действительно является клиентом некоторого эмитента-участника (обслуживающего банка-участника) данной платежной системы.

Аутентификация обслуживающего банка доказывает факт того, что банк является участником данной платежной системы.

2. Реквизиты платежной карты (номер карты, срок ее действия и т.п.), используемой при проведении транзакции ЭК, должны быть конфиденциальными для ТП.

3. Невозможность отказа от транзакции для всех участников транзакции ЭК, то есть наличие у всех участников неоспоримого доказательства факта совершения покупки (заказа или оплаты).

9.9. Организация безопасной передачи данных

Использование SSL для передачи отчетности через Интернет

Хотя в России уже идет процесс по переводу организаций на сдачу отчетности в электронном виде, до совершенства еще далеко. В европейских странах также используются разнообразные варианты сдачи отчетности в государственные органы, однако четко прослеживается одна и та же закономерность: все государства стремятся сейчас получать большую часть документов от налогоплательщиков в электронном виде.

В Великобритании подаваемая бухгалтерская отчетность обычно защищается с использованием SSL, с аутентификацией клиента по паролю или по аутентификационному сертификату.

В Германии в отношении электронных счетов и прочих документов, относящихся к налогообложению, как правило, доступ предоставляется только налоговым органам; вид доступа определяется как «удаленный».

Данные должны сохраняться на носителе, не допускающем внесение изменений.

Во Франции компании обязаны электронным образом декларировать НДС. При подаче этой декларации через Интернет, она должна быть подписана цифровой подписью. Соединение осуществляется по защищенному каналу (по протоколу https), и используется аутентификация клиента (по сертификату).

В Италии компании должны ежегодно подавать финансовые отчеты в соответствующую торговую палату исключительно в электронном виде, подписывая их квалифицированной электронной подписью. Прочие документы, относящиеся к вопросам налогообложения, доверяются уполномоченному органу (налоговой службе). Таможенные декларации должны подписываться подписью, соответствующей п. 5(2) директивы 1999/93/EC.

В Испании компании могут электронным образом защищенно подавать свои бухгалтерские данные и ежегодные отчеты (балансы) в деловой регистр (BPR). Подача документов проводится ежегодно. При обмене данными используется защищенный канал (SSL). Электронные документы подписываются от-

правителем с целью защитить их целостность и идентифицировать личность отправителя, используя сертификат, выданный службой сертификации регистраторов SCR.

Государственные агентства подают (в защищенном режиме) подписанные отчеты о расходах и получают подписанные отчеты, авторизующие такие расходы или указывающие на потенциальные проблемы в поданных документах.

Использование HTTPS для интернет-магазинов

Протоколы HTTPS обязательно должны использовать сайты, на которых пользователи вводят свои платежные данные. Сервисы и интернет-магазины, которые не хотят терять покупателей и заботятся о своей репутации, делают это уже давно.

Но часто интернет-магазины используют технологию шифрования SSL только на странице регистрации или в корзине, где покупатель вводит персональную информацию. А на остальных страницах сайта используется старый, незащищенный протокол HTTP.

Теперь на HTTPS нужно переходить всем и использовать этот протокол для каждой страницы сайта по следующим причинам:

1. Новые версии популярных браузеров Google Chrome и Firefox начали помечать сайты, работающие без SSL-сертификата, как незащищённые.

В настоящее время серый значок незаметен, но в будущем браузеры планируют изменить индикатор безопасности на красный треугольник для страниц на HTTP. Покупать на таком сайте пользователи, скорее всего, побоятся.

2. Поисковая система Google теперь выше ранжирует сайты, работающие по HTTPS.

3. Крупные платежные сервисы (например, «Яндекс.Касса»), могут отказаться работать с сайтом без HTTPS. Другие (например, Apple Pay) уже работают только на HTTPS.

4. Люди больше доверяют магазину, когда видят, что их данные здесь под защитой.

10. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Лабораторная работа № 1

Поиск информации в World Wide Web

Цель работы: знакомство со службами Интернета и возможностями их применения в коммерции, приобретение навыков поиска информации в Интернете.

Интернет имеет три функции: *коммуникационную, информационную* и *управленческую*. Разные службы могут обеспечивать разные функции. Хотя в рамках службы World Wide Web есть сервисы, исполняющие коммуникационные и управленческие функции, основное назначение этой службы – информационное. Когда нам нужно разыскать какие-то сведения, мы обращаемся в первую очередь в информационное пространство Web. Это пространство отличается гигантскими размерами.

Поисковая система представляет собой специализированный web-узел. Пользователь сообщает поисковой системе данные о содержании искомой web-страницы, а система выдает ему список гиперссылок на страницы, соответствующие запросу. Существует несколько моделей, на которых основана работа поисковых систем, но исторически две модели приобрели наибольшую популярность – *поисковые каталоги* и *поисковые указатели*.

Поисковые каталоги

Поисковые каталоги устроены по тому же принципу, что и тематические каталоги крупных библиотек. Обратившись к поисковому каталогу, мы находим на его основной странице сокращенный список крупных тематических категорий.

Каждая запись в списке категорий – это гиперссылка. Щелчок на ней открывает следующую страницу поискового каталога, на котором данная тема представлена подробнее, например по предметам: «Предпринимательское право», «Защита прав потребителей», «Реклама и маркетинг», «Электронная коммерция» и др. Щелчок на названии темы (например, «Электронная коммерция») открывает страницу со списком разделов

(«Электронные платежные системы», «Интернет-магазины», «Налогообложение предприятий электронной коммерции» и т.д.). Продолжая погружение в тему, можно дойти до списка конкретных web-страниц и выбрать себе тот ресурс, который лучше подходит для решения задачи.

Работа с поисковыми каталогами интуитивно проста. В них поиск информации практически всегда завершается более или менее плодотворно. Однако за этой простотой скрывается высочайшая сложность создания и ведения каталога. Поисковые каталоги создаются вручную. Высококвалифицированные редакторы лично просматривают информационное пространство WWW, отбирают то, что, по их мнению, представляет общественный интерес, и заносят адреса в каталог. Основной проблемой поисковых каталогов является чрезвычайно низкий коэффициент охвата ресурсов WWW. И хотя для реферативного поиска это не выглядит критичным, все-таки существуют потребности в поиске актуальной, уникальной, специальной информации, которая не охвачена и не может быть охвачена поисковыми каталогами.

Поисковые указатели

Автоматическую каталогизацию web-ресурсов и удовлетворение запросов клиентов выполняют так называемые *поисковые указатели*.

Основной принцип работы поискового указателя заключается в поиске web-ресурсов по *ключевым словам*. Пользователь описывает искомый ресурс с помощью ключевых слов, после чего дает задание на поиск. Поисковая система анализирует данные, хранящиеся в своей базе, и выдает список web-страниц, соответствующих запросу. Вместе с гиперссылками выдаются краткие сведения о найденных ресурсах, на основании которых пользователь может выбрать нужные ему ресурсы.

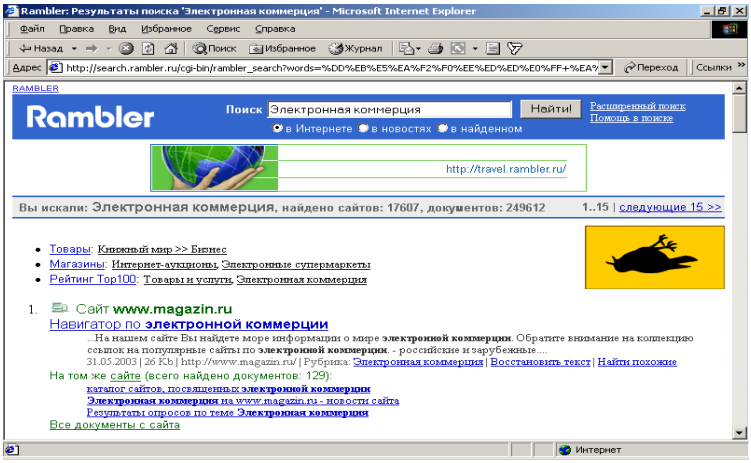

Рис. 8. Поисковая система «Рамблер»

Сегодня в мире существует множество поисковых указателей, их количество перевалило 10000. В России наиболее крупными и популярными являются следующие поисковые указатели: «Апорт 2000» (www.aport.ru), «Яндекс» (www.yandex.ru) и «Рамблер» (www.rambler.ru).

Разные поисковые указатели могут использовать разные информационные технологии для обработки запросов пользователей. Чтобы эффективно выполнять поиск информации в WWW, надо представлять достоинства и недостатки каждой из систем и хотя бы в общих чертах понимать принципы их работы.

Задание 1.

Поиск информации по ключевым словам

1. Запустите программу Internet Explorer
2. В поле адресной строки введите URL – адрес http://www.yandex.ru. Происходит загрузка титульной страницы поисковой системы.
3. Внимательно рассмотрите загруженную страницу, найдите поле для ввода ключевых слов и кнопку поиска. Будем искать web-страницы, посвященные электронной коммерции.
4. В поле для поиска введите слово «коммерция», осуществите поиск. Запишите, что вы увидели на экране.

5. Введите словосочетание «электронная коммерция», осуществите поиск. Запишите результаты поиска.

6. Введите словосочетание «e-commerce», осуществите поиск. Запишите результаты поиска. В чем отличия?

7. Уточните поиск: B2B и Статьи. Опишите результаты.

8. Выберите другой поисковый сервер. Повторите запросы, что получилось?

Задание 2.

Поиск информации с помощью каталогов ресурсов

Самостоятельно исследуйте каталоги ресурсов на наличие сведений об электронной коммерции.

Задание 3.

Используя средства поиска, самостоятельно найти информацию о федеральных и региональных программах, связанных с электронной коммерцией. Результаты работы представьте в виде таблицы:

Название	Адрес	Краткие характеристики

Задание 4.

Сравнение поисковых машин **«Яндекс»** и **Google**.

1. Для поисковых машин **«Яндекс»** и **Google** сформируйте и выполните следующие запросы:

1	На поиск всех страниц, содержащих ссылки на сайт Пермского филиала РГТЭУ
2	На поиск учебников по электронной коммерции в формате pdf
3	На поиск русскоязычных документов с фразой «электронная коммерция» в заголовках, измененных не позднее 3х месяцев назад

2. В каждом случае в таблицу **Excel** записывайте общее количество возвращенных результатов по запросу.

3. Постройте таблицу:

№ запроса	Число результатов в **«Яндекс»**	Число результатов в **Google**	Отклонение

4. Рассчитайте отклонение как (Число результатов в **«Яндекс»** – Число результатов в **Google**) / **МАКСИМУМ** (Число результатов в **«Яндекс»**; Число результатов в **Google**). Задайте процентный формат ячеек для столбца «Отклонение».

5. Рассчитайте суммарное отклонение.

6. Постройте диаграмму по рассчитанному столбцу отклонений. Назовите ее «Сравнение эффективности поиска».

7. Подведите итоги проделанной работы.

Лабораторная работа № 2
Классификаторы информации, стандарты, штриховое кодирование, радиочастотные системы

Цель работы: изучить основные возможности и назначение инструментария электронной коммерции.

Инструментарий ЭК – совокупность инструментов, с помощью которых осуществляется или может осуществиться выполнение технологических операций рассматриваемой коммерческой сделки.

Классификаторы информации

Классификаторы информации – полный перечень понятий из какой-либо предметной области, распределенных по принятому признаку классификации, и присвоенные им коды.

Рассмотрим один из классификаторов – **Страны мира** (международный классификатор с 1993 г.). В нем представлены все страны-члены ООН.

Структурно классификатор состоит из трех блоков:

- цифровой идентификации;
- наименований;

- буквенной идентификации.

Блок цифровой идентификации содержит трехзначный цифровой код страны мира, построенный с использованием порядкового метода кодирования. Блок наименований включает краткое наименование и полное официальное наименование страны мира. Отсутствие в позиции классификатора полного наименования страны мира означает его совпадение с кратким наименованием.

Блок буквенной идентификации стран мира содержит двухзначный (альфа-2) и трехзначный (альфа-3) буквенные коды, знаками которых являются буквы латинского алфавита. Основным принципом, который использовался при создании буквенных кодов, является принцип визуальной ассоциации кодов с наименованиями стран мира на английском, французском или других языках.

- Двузначные буквенные коды рекомендуются для международных обменов, они позволяют создавать визуальную ассоциацию с общепринятым наименованием страны мира без какой-либо ссылки на ее географическое положение или статус.
- Трехзначные буквенные коды применяются в особых случаях, определяемых компетентными организациями.

Цифровой код имеет преимущество перед буквенным кодом, заключающееся в том, что на него не влияют изменения в наименованиях стран мира, которые могут повлечь за собой изменения кодов альфа-2 и альфа-3. Формула структуры цифрового кода в ОКСМ: XXX. В классификаторе страны мира расположены в порядке возрастания их цифровых кодов.

Для удобства пользования классификатором в нем приведены **приложения А, Б и В**.

- **Приложение А** включает краткие и полные наименования стран мира, расположенные в алфавитном порядке кратких наименований, а также их буквенные и цифровые коды.
- **Приложение Б** содержит буквенные коды альфа-2, расположенные в порядке латинского алфавита, и соответствующие им краткие наименования стран мира.
- **Приложение В** содержит буквенные коды альфа-3, расположенные в порядке латинского алфавита, и соответствующие им краткие наименования стран мира.

- Для целей таможенной статистики в классификаторе приведено **приложение Г**, в котором содержатся территории, не включенные в ИСО 3166-97.

Наименование страны		Код		
краткое	полное	2-букв.	3-букв.	цифр.
АБХАЗИЯ	Республика Абхазия	AB	ABH	895
АВСТРАЛИЯ		AU	AUS	36
АВСТРИЯ	Австрийская Республика	AT	AUT	40
АЗЕРБАЙДЖАН	Республика Азербайджан	AZ	AZE	31
АЛБАНИЯ	Республика Албания	AL	ALB	8
АЛЖИР	Алжирская Народная Демократическая Республика	DZ	DZA	12
АМЕРИКАНСКОЕ САМОА		AS	ASM	16

Рис. 9. Классификатор «страны мира»

Задание 1.

Самостоятельно изучите и проанализируйте указанные ниже классификаторы. Сохраните основные сведения о них: назначение, информацию о структуре и др.

1. Классификатор сокращений для условий платежа «Пейтермс» (международный классификатор);
2. Товарная номенклатура внешнеэкономической деятельности СНГ (ТН ВЭД СНГ);
3. Таможенные режимы (Общероссийский классификатор) и др.
4. Формы расчетов (Общероссийский классификатор);
5. Виды транспорта (международный классификатор);
6. Классификатор «Алфавитный код для обозначения валют»;
7. Виды грузов, упаковки и упаковочных материалов (Общероссийский классификатор).

Стандарты, регламентирующие работу с данными, используемыми для формирования электронных сообщений

Наибольший вклад в разработку таких стандартов внесла Рабочая группа по упрощению процедур международной торговли, которая является вспомогательным органом Европейской экономической комиссии ООН.

Рабочая группа разработала несколько рекомендаций относительно ЭОД (электронного обмена данными):

- Представление в цифровой форме дат, времени и периодов;
- Упрощенную отгрузочную маркировку;
- Стандарты ЭДИФАКТ и др.

Представление в цифровой форме дат, времени и периодов (Женева, октябрь 1988 г.).

Информация о датах и периодах времени необходима в большинстве документов, используемых в международной торговле. Однако разнообразие методов представлений этих элементов данных приводило к путанице, а иногда и к судебным разбирательствам, особенно когда даты указываются в чисто цифровой форме (например, в Северной Америке 1.12.1988 означает 12 января 1988 года, в то время как в Европе те же цифры означают 1 декабря 1988 г.). Хотя некоторые из этих трудностей могут быть преодолены, если писать название месяца словом, чисто цифровая запись этих элементов данных могла бы значительно уменьшить трудности, возникающие в связи с различиями в языках и алфавитах, и облегчить сокращение и кодирование.

Настоящая Рекомендация устанавливает метод стандартизованного, точного, чисто цифрового обозначения дат, времени суток и периода. Она применяется во всех случаях, когда эти данные представляются как отдельные записи в цифровой форме, но исключая те случаи, когда они являются частью обычного текста.

Таблица 1

Представление в цифровой форме дат, времени, периодов

Представляемая информация	Возможные кодовые обозначения
Календарная дата Представление в цифровой форме года, месяца и дня в нисходящем порядке с разделением, когда это требуется, дефисом, с возможным опущением «столетия», когда это указание не является необходимым. Пример: 10 апреля 1988 г.	1988-04-10, 19880410, 88-04-10, 880410.
Порядковая дата Представление в цифровой форме года и даты, когда дата указывается порядковым числом, исчисляемым с 1 января (001) до 31 декабря (365 или 366). Пример: 10 апреля 1988 г.	1988102
Время суток Представление в цифровой форме часа и минут с постоянной длиной в четыре цифры. При указании одновременно с датой в качестве указателя начала представления времени необходимо указывать букву «Т». По взаимному согласию партнеров при обмене информацией буква «Т» может быть опущена в тех случаях, когда нет опасности путаницы одновременного представления даты и времени с другими представлениями в данной Рекомендации. Пример: десять часов 10 апреля 1988 г.	19880410T1000, 1988-04-10T1000, 198804101000
Скоординированное во всемирном масштабе время (СВВ) Для того чтобы выразить время суток в скоординированном во всемирном масштабе времени (ранее известном как среднее время по Гринвичу), необходимо использовать приведенные выше	

Продолжение табл. 1

Представляемая информация	Возможные кодовые обозначения
представления, после чего необходимо сразу же поставить указатель времени «Z». Разница между СВВ и местным временем показывается добавлением временной разницы, выраженной в часах и минутах, либо только в часах, с предшествующим знаком «+» или «-», в зависимости от случая. Пример: 23 часа 20 минут и 13 секунд. Пример: 15 часов 27 минут и 46 секунд по местному времени в Женеве и в Нью-Йорке, показанные в соответствии с СВВ.	 232013Z 152746+0100 (или + 01) 152746–0500 (или – 05)
Неделя Представления в цифровой форме периода из семи календарных дней, начиная с понедельника, и с нумерацией от 01 до 53, причем цифра 01 относится к первой неделе, содержащей по меньшей мере четыре дня нового года, и этой цифре предшествует, если это нужно, буква «W», чтобы избежать недоразумения. Пример: неделя 11–17 апреля 1988 г.	 1988 W 15, 198815
Другие периоды времени Представление в цифровой форме дат и времени с указанием соответственно начала и конца периода, разделенных двойным дефисом. (Вместо двойного дефиса в качестве разделительного знака можно использовать косую черту). Примеры: – Периоды, выраженные с точностью в годах: 1985 по 1987 г. – Периоды, выраженные с точностью в месяцах: Февраль-апрель 1988 г.	 1985--1987 1988-02--04 1988-02- -1988-03

Окончание табл. 1

Представляемая информация	Возможные кодовые обозначения
Февраль 1988 г. – апрель 1988 г. – Периоды, выраженные с точностью в неделях: 11 апреля – 23 мая 1988 г. 11 апреля 1988 г. – 23 мая 1988 г. – Периоды, выраженные с точностью в днях: 8 по 13 апреля 1988 г. 8 апреля по 10 мая 1988 г. 8 апреля 1988 г. – 10 мая 1988 г. – Периоды, выраженные с точностью в часах: 10–18 ч. 8 апреля 1988 г. 10 ч. 8 апреля – 18 ч. 10 апреля 1988 г. 10 ч. 8 апреля – 18 ч. 10 мая 1988 г. 10 ч. 8 апреля 1988 г – 18 ч. 10 мая 1988 г. (Во всех примерах дефисы и, при обоюдном согласии, обозначения в виде буквы «Т» могут быть опущены, как показано выше. Однако двойные дефисы должны всегда употребляться как указано.)	 1988 W 15- -21 1988 W 15- - 1988 W 21 1988-04-08- -13 1988-04-08- -05-10 1988-04-08- -1988-05-10 1988-04-08T1000- -1800 1988-04-08T1000- -10T1800 1988-04-08T1000- -05-10T1800 1988-04-08T1000--1988-05-0T1800

Представлению в цифровой форме определенного периода времени предшествует буква «Р», а после указателя количества лет, месяцев, недель, дней, часов и минут в данном представлении следуют соответственно буквы «Y», «M», «W», «D», «H» и «M». (Буква «Т» должна использоваться для обозначения раздела часов и минут в представлении.)

Примеры:

Период в два года, десять месяцев, 15 дней, 10 часов, 20 минут: P2Y10M15DT10H20M.

Период в один год, шесть месяцев, начиная с 8 апреля 1988 г.: 19880408- -P1Y6M.

Задание 2.

1. Рассмотрите стандарт «Упрощенная отгрузочная маркировка» (например на http://sklad-zakonov.narod.ru).

2. Изучите применение стандарта ЭДИФАКТ.

Штриховое кодирование

Штриховое кодирование – это категория для обозначения способа представления информации в графическом виде и предназначенная для считывания специальными оптико-электронными устройствами.

Рис. 10. Штрих-код

На сегодняшний день штриховое кодирование является одной из самых распространенных технологий автоматизированного сбора данных (автоматической идентификации – АИ). Автоматическая идентификация осуществляет автоматическое распознавание, расшифровку, обработку, передачу и запись информации, большей частью, с помощью нанесения и считывания информации, закодированной в ***штрих-коде***.

Штрих-коды позволяют быстро, просто и, самое главное, точно считывать и передавать информацию о тех предметах, которые нуждаются в прослеживании и контроле. В технологии **штрихового кодирования** можно выделить следующие основные этапы:

1. Создание штрихового кода при помощи специального программного обеспечения.

2. Маркировка товара штриховым кодом (многие товары уже имеют на своей упаковке штрих-код, распечатанный типографским способом).

3. Чтение штрихового кода (получение данных, закодированных в штриховом коде).

Задание 3.

Изучить технологию штрихового кодирования и ответить на вопросы:

1. Что такое штрих-код?
2. Где используются штрих-коды?
3. Из чего состоят системы сбора данных?
4. Как осуществляется печать штрих-кодов?
5. Как происходит считывание штрих-кодов?
6. Какие бывают типы штрих-кодов?
7. Перечислите преимущества использования штрихового кодирования.

(http://www.jasmi.ru/automation/automation.html)

Радиочастотные метки RFID

Радиочастотная идентификация (RFID) – технология бесконтактной идентификации объектов при помощи радиочастотного канала связи.

RFID в области автоматической идентификации сейчас рассматривается как уникальное средство управления данными, которое имеет ряд преимуществ по сравнению с технологией штрихового кодирования.

Система бесконтактной идентификации состоит из трех основных элементов:

- радиочастотной метки или транспондера;
- считывателя информации (ридера);
- компьютера для дальнейшей обработки информации.

Преимущества перед штрих-кодом:

- бесконтактное чтение и запись;
- работа вне прямой видимости;
- большая дальность считывания;
- перезапись данных;
- большой объем данных;
- одновременное считывание большого количества меток;
- долговечность метки.

Задание 4.

Самостоятельно изучите более подробную информацию о RFID (http://rfid-news.ru/02_tech_root.htm) и составьте отчет по следующим вопросам:

1. Классификация меток.
2. Виды считывателей.
3. Программное обеспечение RFID-системы.
4. Преимущества и недостатки радиочастотной идентификации.
5. Как используются радиочастотные системы в электронной коммерции?

Лабораторная работа № 3
Системы автоматизации управления ресурсами предприятия

Цель работы: изучить виды автоматизированных систем управления ресурсами предприятия, рассмотреть реальные примеры.

Бурный рост ЭК в последние годы определяется успешной реализацией электронных технологий в бизнесе. Системы управления ресурсами предприятия в интернет-экономике могут стать основой эффективных коммуникаций.

MRP (планирование материальных ресурсов)

MRP-система – интегрированная электронная информационная система управления, в которой для планирования потребности производства в материальных ресурсах используется информация о структуре и технологии производства конечного продукта, объемно-календарный план производства, данные складских запасов, заключенных договоров поставки материалов и комплектующих и т.п.

Основная цель MRP-систем состоит в том, что любая учетная единица материалов или комплектующих, необходимых

для производства изделия, должна быть в наличии в нужное время и в нужном количестве.

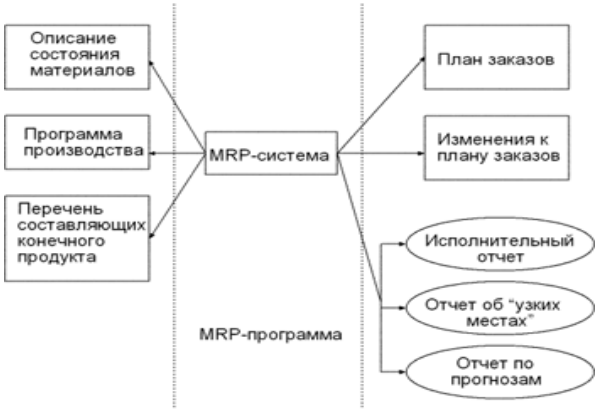

Рис. 11. Входящие и выходящие потоки информации в MRP-системах

Задание 1.

Изучите более подробно системы данного класса (http://www.kgau.ru/istiki/uip/ch07.html и другие информационные ресурсы) и ответьте на вопросы:

1. Опишите входные элементы MRP-систем.
2. Какие основные операции на основании входных данных выполняет MRP-система?
3. Опишите основные функции MRP-систем.
4. Назовите основной недостаток MRP-систем.

MRP II (планирование производственных ресурсов)

MRP II представляет собой методологию, направленную на более широкий охват ресурсов предприятия, нежели **MRP**. В отличие от MRP, в системе **MRP II** производится планирование не только в материальном, но и в денежном выражении и присутствует возможность прогнозирования и моделирования.

MRP II представляет собой интеграцию большого количества отдельных модулей, таких как планирование бизнес-

процессов, планирование потребностей в материалах, планирование производственных мощностей, планирование финансов, управление инвестициями и т.д. Результаты работы каждого модуля анализируются всей системой в целом, что, собственно, и обеспечивает её гибкость по отношению к внешним факторам.

MRP II, согласно стандартам, включает 16 функций:

1. Планирование продаж и операций (Sales & Operations Planning).
2. Управление спросом (Demand Management).
3. Главный календарный план производства (Master Production Schedule).
4. Планирование потребности в материалах (Material Requirements Planning).
5. Подсистема спецификаций (Bill of Material Subsystem).
6. Подсистема операций с запасами (Inventory Transaction Subsystem).
7. Подсистема запланированных поступлений по открытым заказам (Scheduled Receipts Subsystem).
8. Оперативное управление производством (Shop Floor Control or Production Activity Control).
9. Планирование потребности в мощностях (Capacity Requirements Planning).
10. Управление входным/выходным материальным потоком (Input/Output Control).
11. Управление снабжением (Purchasing).
12. Планирование ресурсов распределения (Distribution Resource Planning).
13. Инструментальное обеспечение (Tooling).
14. Интерфейс с финансовым планированием (Financial Planning Interfaces).
15. Моделирование (Simulation).
16. Оценка деятельности (Performance Measurement).

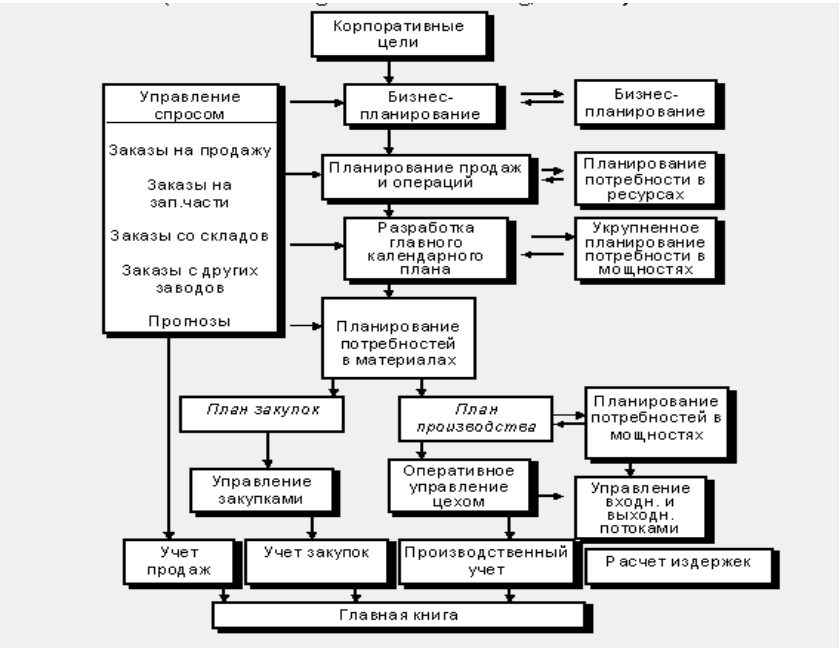

Рис. 12. Планирование ресурсов производства, MRP II

MRP II ориентируется на малые и средние производственные предприятия – предприятия «единичного позаказного» производства, «массового» производства или «серийного» производства сложной продукции.

Задание 2.

1. Дайте краткую характеристику каждому модулю системы MRP II.

2. Изучите принципы работы с программой MRP II (описание) на примере Мастер MRP II Excel (Компьютерная модель производственного планирования и учета для малых предприятий) на сайте http://www.vmgroup.ru/soft/mp_mrp.htm или на любом другом примере.

ERP (планирование ресурсов предприятия)

ERP-системы – это компьютерные системы, созданные для обработки деловых операций организации и для содействия комплексному и оперативному (в режиме реального времени) планированию, производству и обслуживанию клиентов. Как правило, ERP-системы строятся по модульному принципу и в той или иной степени охватывают все ключевые процессы деятельности.

В состав классической ERP-системы могут входить следующие подсистемы:

- производство;
- снабжение и сбыт;
- управление запасами;
- техобслуживание оборудования;
- послепродажное обслуживание произведенной продукции;
- кадры;
- научные разработки;
- финансы.

Различия между системами MRP II и ERP вытекают из функционального назначения. MRP-системы созданы для использования только на промышленных предприятиях, ERP-системы не ограничены сферой только промышленного производства, они могут использоваться в организациях сферы торговли и услуг, банках, страховых компаниях, образовательных учреждениях и т.д.

Интеграция систем ERP с системами интернет-коммерции секторов B2B и B2C – естественный и закономерный этап в развитии технологии управления ресурсами предприятия. Создание и эксплуатация систем интернет-коммерции, прежде всего систем сектора B2B, становится наиболее эффективной, если эти системы интегрированы в общекорпоративные бизнес-процессы и, соответственно, встроены в *ERP-систему*.

Межкорпоративная интеграция на уровне взаимосвязей между ERP-системами поставщиков и потребителей обеспечи-

вается через B2B-системы электронной коммерции – электронные системы сбыта *(e-distribution)*, снабжения *(e-procurement)* и торговые площадки *(e-marketplace)*. Поскольку электронная торговая площадка как система электронной коммерции B2B позволяет осуществить прямое взаимодействие между субъектами рынка – поставщиками и потребителями, то она может стать элементом интеграции между **ERP-системами** субъектов рынка. В этом случае отдельные корпоративные системы управления ресурсами становятся частью большого электронного рынка.

Задание 3.

1. С помощью средств поиска найти и составить отчет о достоинствах и недостатках ERP-систем.

2. Изучите составляющие и принципы работы ERP-систем «КОМПАС» (http://www.compas.ru/) и «ALFA» (http://www.alfasystem.ru/3).

Проведите их сравнительный анализ согласно таблице:

Показатели	«КОМПАС»	«ALFA»
Разработана компанией…		
Назначение		
Отрасли применения		
Пользователи системы		
Основные подсистемы (модули)		
Настройка системы (необходимость заказа программиста, наличие визуальной настройки)		
Преимущества системы		
Технологическая платформа, ее состав		

Рис. 13. Схема интеграции ERP-систем поставщиков и потребителей посредством B2B-систем электронной коммерции

CSRP (планирование ресурсов, синхронизированное с покупателем)

CSRP использует интегрированную функциональность ERP и перенаправляет производственное планирование от производства далее, к покупателю. CSRP предоставляет действенные методы и приложения для создания продуктов с повышенной ценностью для покупателя. Главная задача таких систем – синхронизировать покупателя с внутренним планированием и производством.

Рис. 14. Реализация ориентации на интересы покупателей в CSRP-системах

Непосредственная интеграция с информацией о конфигурации заказов позволяет производственным подразделениям увеличить целостность процесса планирования путем снижения количества повторной работы и снижения числа перерывов из-за наплыва заказов. Усовершенствование производственного планирования дает возможность обеспечить лучшую оценку сроков поставок и улучшить поставку вовремя. Производственное планирование теперь позволяет оптимизировать операции на основе действительных покупательских заказов, а не на прогнозах или оценках. С доступом в реальном времени к точной информации о заказах покупателей, подразделения планирования могут динамически изменять группирование работ, последовательность исполнения заказов покупателей, приобретения и

заключения субконтрактов с целью улучшения обслуживания покупателей и снижения стоимости. Требования покупателей к продукту могут передаваться непосредственно от покупателя к субконтрактору или поставщику, устраняя ошибки и задержки, которые встречаются при трансляции заказов покупателей в заказы на покупку. Изменения в заказе покупателя могут приводить к автоматическим изменениям в заказах поставщикам, уменьшая количество повторной работы и задержки. Качество продуктов и правильность заказа основных комплектующих могут быть значительно улучшены, а также уменьшены циклы их доставки.

Задание 3.

Средствами поиска найдите в Интернете описание системы данного класса и познакомьтесь с ней.

Лабораторная работа № 4
Системы B2C, C2C, B2B

Цель работы: изучить виды систем электронной коммерции, научиться определять принадлежность сайта к той или иной разновидности СЭК.

Система ЭК – комплекс наиболее существенных рыночных отношений и информационных потоков, которые связывают участников и клиентов ЭК с рынком.

Система B2C

Рассмотрим пример, интернет-магазин OZON.RU.

В адресной строке наберите www.ozon.ru. После перехода по указанному адресу отобразится начальная страница интернет-магазина «Озон». Слева отображен список категорий товаров и услуг. На горизонтальной панели отображаются интерфейсные элементы: моя корзина, мои заказы, помощь, поисковая строка и т.п.

При нажатии гиперссылки «нужна помощь?» открывается страница с описаниями основных принципов работы в интернет-магазине «Озон»:

Помощь

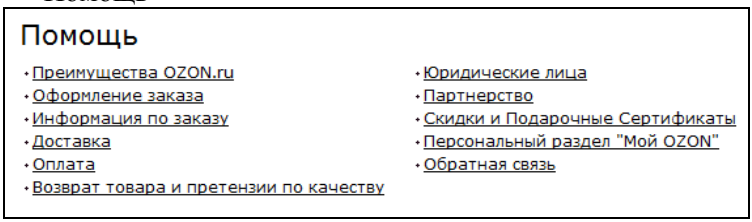

Рис. 15. Раздел «Помощь» в интернет-магазине «Озон»

Здесь можно найти ответы на вопросы, возникающие в ходе выбора товаров и услуг, способов оплаты и др.

При нажатии на логотип магазина осуществляется переход на главную страницу.

Рассмотрим, как совершаются покупки. Выберите категорию товаров, например «Детский мир», осуществите переход. Среди предложенных товаров выберите понравившийся и при помощи мыши нажмите на него. Откроется страница с подробным описанием товара, указанием цены, уточнением даты получения товара и т.п. (справа).

При нажатии кнопки «в корзину» происходит перемещение в нее товара. Аналогично можно выбрать различные товары из других категорий.

Для просмотра состояния корзины нажмите кнопку «перейти в корзину», информация отобразится следующим образом:

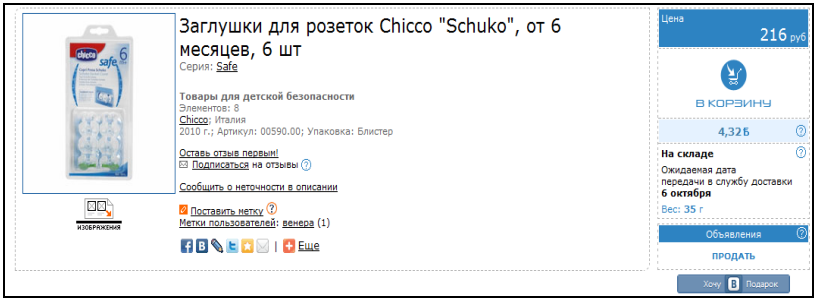

Рис. 16. Корзина покупателя в «Озоне»

Также данный интернет-магазин представляет дополнительные услуги: размещение объявлений, бронирование гостиниц и др.

Перед оформлением покупки обязательно познакомьтесь с условиями оплаты, доставки и т.п.

Система С2С

Интернет-аукцион «Молоток.Ру».

В адресной строке наберите www.molotok.ru.

После перехода по указанному адресу отобразится начальная страница интернет-аукциона. Рассмотрите существующие интерфейсные элементы: категории товаров, помощь, поиск, полезные ссылки, новости и др.

На «Молоток.Ру» тысячи пользователей продают новые и б\у товары. Ежедневно здесь можно найти большое количество самых разнообразных товаров, которые удовлетворят вкусы самого требовательного покупателя.

При нажатии на ссылку «Как пользоваться?» вы найдете помощник покупателя и продавца:

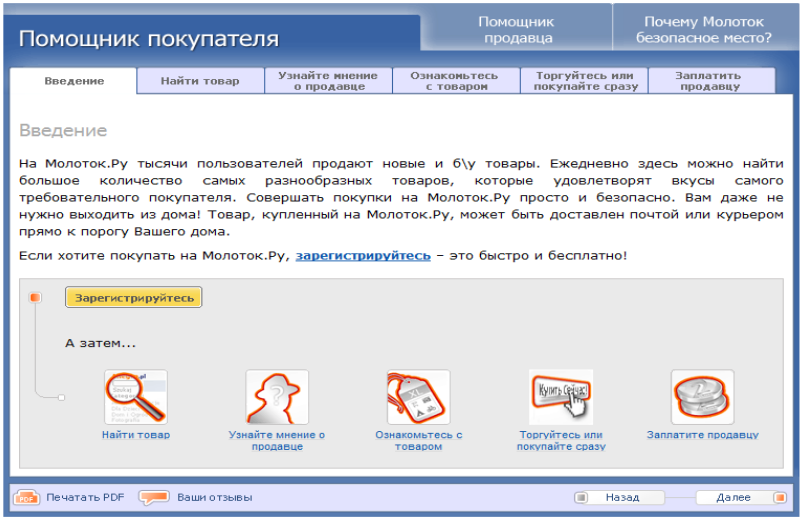

Рис. 17. Правила проведения операций на аукционе «Молоток»

Также на главной странице можно найти следующую информацию о компании, сервисе и инструментах аукциона (например, присутствует система поиска) и др.

Рассмотрим, как происходит процесс покупки товаров. Выберем категорию, например «Искусство, антиквариат». Уточним поиск, выбрав, например «Ювелирные изделия». Информация по выбранному критерию организована следующим образом:

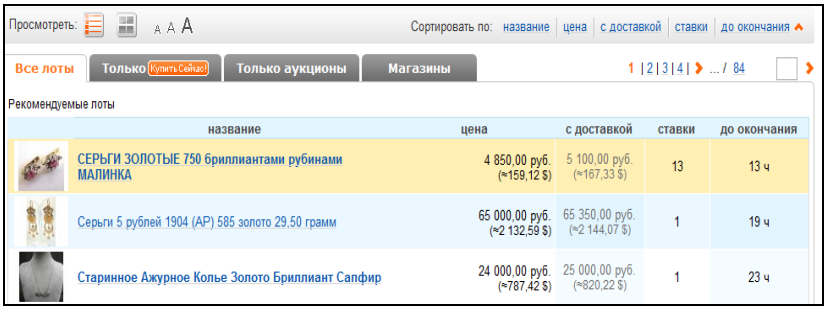

Рис. 18. Организация информации о товарах на «Молотке»

При нажатии на товар, получим информацию о состоянии торгов и описание этого лота:

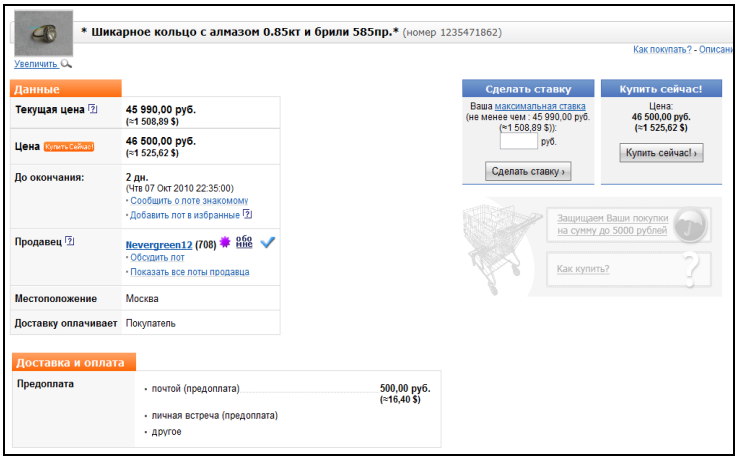

Рис. 19. Описание товара на «Молотке»

Изучите другие функциональные возможности продажи и покупки товара самостоятельно.

Система B2B

Торговая площадка .

В адресной строке наберите http://marketplace.rusbiz.ru/.

После перехода по указанному адресу отобразится начальная страница электронной торговой площадки. Рассмотрите существующие интерфейсные элементы.

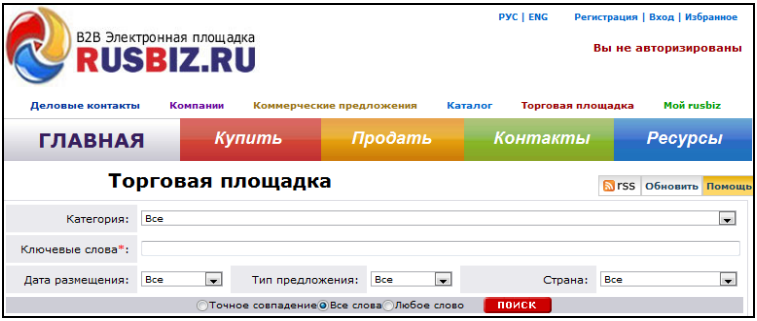

Рис. 20. Стартовая страница торговой площадки Rusbis

Для установления деловых контактов система предлагает пройти авторизацию:

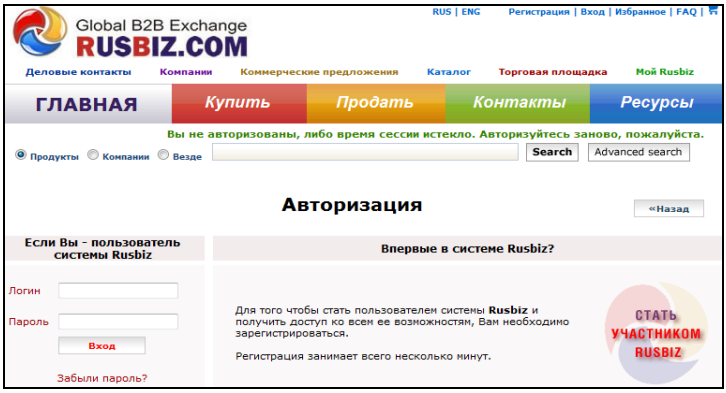

Рис. 21. Система авторизации на Rusbis

Здесь предусмотрен поиск деловых партнеров, товаров и услуг по каталогу (по коду ТН ВЭД), представлена информация об обучающих семинарах и курсах в области электронной коммерции и т.д.

Задание 1.

Самостоятельно изучите возможности приведенных ниже сайтов, укажите принадлежность каждого к той или иной разновидности классификации по типу взаимодействия субъектов ЭК путем размещения любого знака в соответствующей ячейке:

WWW – адрес	Классификация СЭК		
	B2B	B2C	C2C
www.medprom.ru			
www.ingos.ru			
www.zol.ru			
www.cenoved.ru			
www.rosno.ru			
www.iic.ru			
www.tradeline.ru			
www.faktura.ru			
www. formoza.ru			

Лабораторная работа № 5
Сравнение интернет-магазинов

Цель работы: изучение и сравнение функциональных возможностей интернет-магазинов.

Задание 1.

Провести сравнительный анализ Интернет-магазинов, согласно прилагаемой таблице для заданного товара.

Показатели	**Наименование магазина в Интернете, адрес**	**Наименование магазина в Интернете, адрес**
Скорость загрузки страницы		
Интерфейс		
Удобство и рациональность меню		

Организация пользовательской информации на странице		
Широта и полнота ассортимента товаров		
Ассортимент сопутствующих товаров		
Качество информации о товаре (наличие информации, ее информативность)		
Наличие и качество фото-, видеоинформации		
Уровень цен		
Наличие и гибкость системы скидок		
Удобство и простота процедуры оформления заказа		
Удобство и разнообразие форм оплаты		
Способы доставки товара		
Стоимость доставки		
Широта географии доставки		
Гарантии. Послепродажное обслуживание		

А. Книги.
Б. Автомобили.
В. Мебель.
Г. Аудио-, видеотехника.
Д. Холодильники.
Е. Одежда.
Ж. Обувь.
З. Компьютеры.
И. Аудио-, видеопродукция.
К. Цветы.
Л. Подарки.
М. Ювелирные изделия.
Н. Спортивные товары (кроме одежды и обуви).
О. Хозяйственные товары (кроме бытовой химии).
П. Бытовая химия.

Р. Кожевенные и галантерейные товары.
С. Меховые товары.

Задание 2.

Провести сравнительный анализ процесса совершения покупки в традиционном магазине и виртуальном Интернет-магазине.

Параметр сравнения	**Традиционный магазин**	**Интернет-магазин**
Место совершения покупки		
Способ перемещения покупателя по магазину		
Процесс выбора товара		
Получение консультации при выборе товара		
Заказ товара		
Процесс оплаты товара		
Доставка (получение товара)		

Лабораторная работа № 6
Сравнение интернет-аукционов

Цель работы: изучение и сравнение функциональных возможностей интернет-аукционов.

Задание 1.

Используя средства поиска информации в Интернете, найти аукцион, изучить его работу, составить отчет по следующим параметрам: товары, выставляемые на аукцион, способы доставки и оплаты, возможности поиска товара, процесс регистрации в качестве покупателя/продавца, особенности аукциона, гарантии безопасности и т.п.

Лабораторная работа № 7
Корпоративные web-сайты и информационные корпоративные порталы

Цель работы: изучение и сравнение функциональных возможностей интернет-сайтов компаний.

Задание 1.

1. Используя средства поиска информации в Интернете, найти корпоративный web-сайт и информационный корпоративный портал.

2. Провести их сравнительную характеристику, согласно таблице.

Характеристика сайта	**Имя сайта**	**Имя сайта**
Адрес сайта		
Скорость загрузки		
Способы организации 2-х сторонней связи с посетителями		
Информация о деятельности компании (область деятельности)		
1) Полнота и понятность		
2) Историческая справка о компании		
3) Адрес, телефоны		
4) Информация о покупаемой, продаваемой или производимой продукции		
Качество навигации по сайту		
Способы оплаты		
Условия доставки		
Пред- и после продажная поддержка		
Возможность стать участником (для информационно корпоративных порталов)		

Лабораторная работа № 8
Доставка товаров в СЭК

Цель работы: изучить способы доставки товаров и услуг в системах электронной коммерции.

Задание 1.

Используя средства поиска информации в Интернете, найти сайты курьерских служб и составить их сравнительную характеристику, согласно таблице:

Характеристики	Курьерская служба 1	Курьерская служба 2
Адрес в сети		
Краткая характеристика компании		
Услуги		
География		
Возможность отслеживания груза		
Виды грузов (возможные / запрещенные)		
Клиенты		
Способы доставки		
Удобство и разнообразие способов оплаты		
Особенности		

Лабораторная работа № 9
Кредитные платежные системы

Цель работы: изучить возможности кредитных платежных систем, принципы их функционирования, проанализировать их преимущества и недостатки.

Задание 1.

1. В сети Интернет войти на сайты кредитных платежных систем электронной коммерции, проанализировать их по следующим критериям и описать схему проведения платежа в этих системах:

Параметры кредитной системы	Кредитная система	Кредитная система
Название кредитной системы		
Где и кем (страна и фирма) разработана платежная система		
География действия платежной системы		
Использование системы в России		
Минимальная и максимальная сумма платежа		
Как стать участником платежной системы		
Комиссии за осуществление платежа и использование платежной системы		
Возможные участники платежной системы (банки, фирмы, предприятия, частные лица, государственные структуры и т.д.)		
Особенности платежной системы		
Сроки прохождения платежа		
Как «вводятся» в платежную систему реальные деньги		
Как выйти из платежной системы и вернуть реальные деньги		

Кредитные системы:

А. Cyber Cash.

Б. Open Market.

В. First Virtual.

Г. Assist.

Д. Cashew.

Е. Eaccess.

Ж. Cyber Plat.

З. Int.eCom.

И. Data Cash.

К. Check Free.

2. Провести их сравнительный анализ. Сделать вывод об их преимуществах и недостатках.

Лабораторная работа № 10
Дебетовые платежные системы

Цель работы: изучить возможности дебетовых платежных систем, принципы их функционирования, проанализировать их преимущества и недостатки.

Задание 1.

1. Изучить характеристики двух дебетовых платежных систем, указанных преподавателем, согласно приведенной таблице и описать схему проведения платежа в этих системах.

Параметры дебетовой системы	**Дебетовая система**	**Дебетовая система**
Название дебетовой системы		
Где и кем (страна и фирма) разработана платежная система		
География действия платежной системы		
Использование системы в России		
Минимальная и максимальная сумма платежа		
Как стать участником платежной системы		
Комиссии за осуществление платежа и использование платежной системы		
Возможные участники платежной системы (банки, фирмы, предприятия, частные лица, государственные структуры и т.д.)		
Особенности платежной системы		
Сроки прохождения платежа		
Как «вводятся» в платежную систему реальные деньги		
Как выйти из платежной системы и вернуть реальные деньги		

Дебетовые системы:

а) Web Money.
б) Pay Cash.
в) Instant!
г) Net Bill.
д) Net Cash.
е) Mondex.
ж) Net Chex.

з) E-Gold.

и) Net Cheque.

к) Pay Plat.

2. Провести их сравнительный анализ. Сделать вывод об их преимуществах и недостатках.

3. Сравнить кредитные и дебетовые платежные системы.

Лабораторная работа № 11
Российские платежные системы

Цель работы: изучить возможности платежных систем России, принципы их функционирования, сделать анализ их преимуществ и недостатков.

Задание 1.

1. Изучить характеристики двух российских платежных систем, указанных преподавателем, согласно приведенной таблице и описать схему проведения платежа в этих системах.

Параметры кредитной системы	**Платежная система**	**Платежная система**
Название платежной системы		
Где и кем (страна и фирма) разработана платежная система		
География действия платежной системы		
Использование системы вне России		
Минимальная и максимальная сумма платежа		
Как стать участником платежной системы		
Комиссии за осуществление платежа и использование платежной системы		
Возможные участники платежной системы (банки, фирмы, предприятия, частные лица, государственные структуры и т.д.)		
Особенности платежной системы		
Сроки прохождения платежа		
Как «вводятся» в платежную систему реальные деньги		
Как выйти из платежной системы и вернуть реальные деньги		

Российские платежные системы:
а) «Яндекс.Деньги».
б) RUpay.
в) RBS.
г) Telepat.
д) «Градо».
е) Eaccess.
ж) ЭлИТ.
з) AlfaPay.
и) «Телебанк».
к) SimMP.
л) PayPal.
м) AlfaPay.
н) SimMP.
о) Paymer.
п) «КредитПилот».

Лабораторная работа № 12
Туристский продукт и страхование

Цель работы: знакомство с услугами Интернета, привитие навыков пользования системами бронирования, заказа туров.

Торговля туристским продуктом

Туристский бизнес представляет собой предпринимательство в сфере туризма. Для рынка путешествий и перевозок объектом продажи являются не материальные продукты, а обязательства по выполнению услуг.

Туристский продукт включает в себя:

а) туры, объединенные их целесообразностью (познавательные, оздоровительные и т.п.);

б) туристско-экскурсионные услуги (размещение, питание, транспортные услуги и т.п.);

в) товары туристско-сувенирного назначения (карты, открытки, сувениры и т.д.).

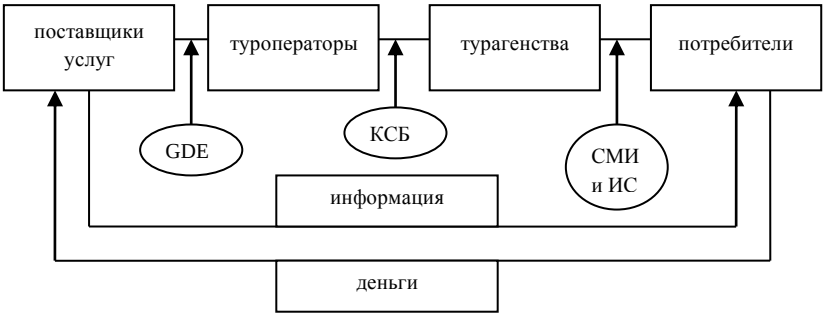

Рис. 22. Участники рынка туристических услуг

Поставщиками туристических услуг являются транспортные компании, объекты размещения и организаторы туристических мероприятий.

В обязанности **туроператоров** входит объединение услуг в пакеты и формирование турпродукта, который поступает в **турагентства** для их реализации конечным потребителям.

Связующее звено между поставщиками и туроператорами – глобальные системы резервирования (**GDS** – Global Distribution System). С их помощью удается объединить поставщиков услуг (авиакомпании, гостиницы). В России к этому классу относятся система бронирования самолетов «Сирена» (www.fly.ru) и система резервирования гостиниц (www.alean.ru).

КСБ – корпоративные системы бронирования – связывают между собой туроператоров и туристические агентства. Служат для открытия доступа к внутренней базе оператора на основе договора.

СМИ и ИС (интернет-сайт) нужны для передачи информации конечным потребителям и взаимодействия с ними в процессе оказания тур-услуг.

Задание 1.

Рассмотрите специальные туристические разделы поисковых систем. Составить сравнительный отчет о туристических разделах «Рамблера» и «Яндекса».

Задание 2.

Посетите в сети Интернет специализированные порталы и сайты:

www.tours.ru
www.mayakinfo.ru
www.votpusk.ru

Кратко опишите данные порталы, указав возможные сервисы. Сформулируйте преимущества для туризма, обусловленные Интернетом.

Задание 3.

При помощи поисковых систем Интернета зайти на сайты турфирм и сравнить их работу по следующим показателям:

Показатели	Турфирма 1	Турфирма 2
Название		
URL-адрес		
Направления отдыха		
Удобство интерфейса		
Подбор тура (присутствует, отсутствует)		
Информация о странах		
Советы, форумы, отзывы		
Ценовая политика		
Особенности		

Страхование в интернет

Со временем все большее число финансовых институтов используют возможности сети Интернет для предоставления своих услуг. Теперь к ним присоединились страховые компании. Страхование – это процесс установления и поддержания неких договорных отношений между Страхователем (покупателем страховых услуг) и Страховщиком (организацией, предоставляющей такие услуги). Страховщик разрабатывает и определяет программу страхования, предлагает ее клиенту, и в случае согласия последнего стороны заключают договор, в резуль-

тате которого клиент осуществляет единовременный или регулятивные платежи, а Страховщик обязуется при наступлении страхового случая выплатить Страхователю денежную компенсацию, определенную условиями данного договора. При совершении сделки формируется документ, называемый страховым полисом. Полис служит для Страхователя и для страховой компании юридическим документом, в котором оговариваются существенные моменты страхования: указывается объект страхования (имущество, человек, ответственность), страховой случай, от наступления которого заключается договор, начало и конец срока страхования, страховая сумма, страховая премия. Документ подписывается обеими сторонами[3] и в обязательном порядке должен храниться у Страхователя.

Таким образом, интернет-страхование (в полном смысле этого слова) – это все вышеперечисленные элементы взаимодействия между страховой компанией и клиентом, возникающие при продаже страхового продукта и его обслуживании, но производимые с помощью сети Интернет. Поэтому, чтобы интернет-представительство компании функционировало как виртуальный офис этой страховой компании, оно должно включать в себя следующие возможности:

- предоставление клиенту полной информации об общем и финансовом состоянии компании;
- предоставление клиенту информации об услугах компании и возможности детального ознакомления с ними;
- расчет величины страховой премии и определение условий ее выплаты для каждого вида страхования и в зависимости от конкретных параметров;
- заполнение формы заявления на страхование;
- заказ и оплата (в виде единовременной выплаты или периодических выплат) полиса страхования непосредственно через Интернет;
- передача полиса, заверенного электронно-цифровой подписью страховщика, клиенту непосредственно по сети Интернет;
- возможность информационного обмена между Страхователем и Страховщиком во время действия договора (для получения клиентом различных отчетов от страховой компании);

- информационный обмен между сторонами при наступлении страхового случая;
- оплата страховой премии Страхователю посредством сети Интернет при наступлении страхового случая;
- предоставление Страховщиком клиенту других услуг и информации: консалтинг, словарь страховых терминов и др.

Если всем этим требованиям отвечает интернет-представительство компании, то его можно назвать полноценным виртуальным офисом.

Задание 4.

В адресной строке **наберите** www.reso.ru. После перехода по указанному адресу отобразится начальная страница **ОАО «Ресо-Гарантия».**

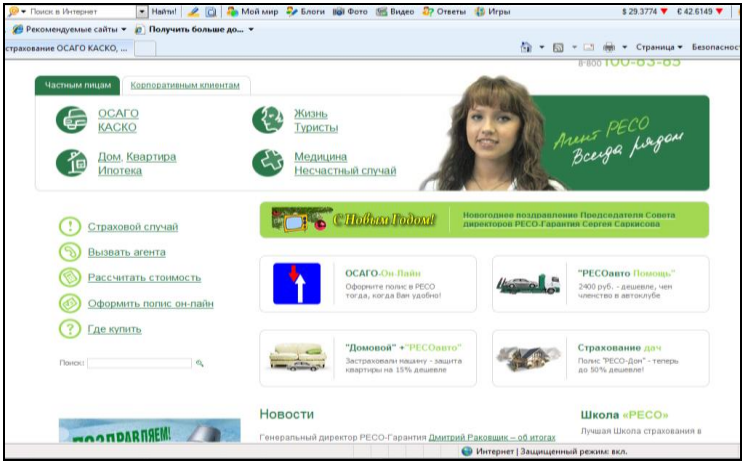

Рис. 23. Стартовая страница ОАО «Ресо-Гарантия»

В своем виртуальном офисе компания предлагает проводить несколько начальных этапов сделки. Заключительный этап, когда клиент получает полис, а вместе с полисом необходимые комментарии и более детальные объяснения правил страхования, проходит с помощью агентов. Таким образом, сначала клиент заходит на web-сайт компании, где размещены анкеты по всем видам страхования, заполнив которые, он может получить

предварительную котировку. Там же представлены правила страхования.

Web-сайт компании используется большей частью для консультации потенциальных клиентов из Москвы и регионов России. На сайте дается информация о котировках, правилах. Представлены общие сведения о компании, ее подразделениях, информация о руководстве и акционерах компании, краткая финансовая отчетность – страховые премии и выплаты за последние периоды, уставной капитал. На web-сайте посетитель может заполнить анкету для устройства на работу в Ресо-Гарантия.

Задание 5.

Войдите в каталог сайтов страховщиков по адресу: http://www.sdvb.ru, выберите две компании и составьте их сравнительную характеристику (название компаний, комплекс оказываемых интернет-услуг, статистика договоров, заключенных через Интернет, наличие дополнительных услуг и т.п.).

Лабораторная работа № 13
Влияние рекламы на объем продаж, однофакторная линейная модель

Цель работы: на основе статистических данных научиться оценивать параметры простейших моделей.

Анализ, прогнозирование и планирование объема продаж – важнейшие функции менеджера и маркетолога. В планах должны стоять конкретные цифры, которые получают с помощью определенных моделей. Например, зависимость объема продаж от затрат на рекламу можно выразить функцией:

$$Y=a_1*X+a_0,$$

где: Y – объем продаж, зависимая переменная (функция), X – затраты на рекламу, независимая переменная (фактор), a_1, a_0 – параметры модели.

Модель используется для прогнозирования объема продаж в зависимости от затрат на рекламу продукции. Параметры модели имеют конкретные числовые значения. Для выполне-

ния прогнозных и плановых расчетов необходимо знать эти значения.

Параметры однофакторной модели можно оценить методом наименьших квадратов с помощью Excel.

Задание 1.

С помощью систем поиска найдите статистические данные компаний о затратах на рекламу и объемах продаж (или воспользуйтесь данными, предоставленными преподавателем). На их основе постойте математическую модель зависимости объемов продаж от затрат на рекламу и численно оцените параметры модели.

Методика выполнения задания:

1. В **Excel** открыть рабочую книгу, заполнить столбцы данными.

2. Выделить колонки исходных данных, вызовите **Мастер диаграмм**, выбрать тип диаграмм – **Точечная**. Далее следовать подсказкам Мастера диаграмм и заполнить необходимые данные до появления кнопки **Готово**.

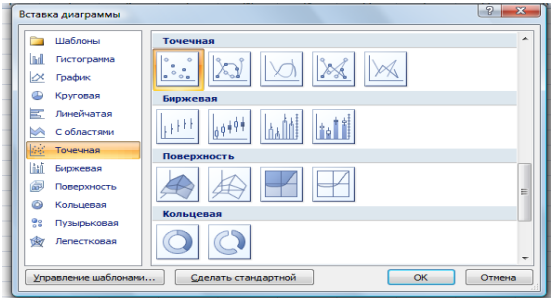

Рис. 24. Вставка диаграммы: выбор типа

3. Построить линию тренда и уравнение с оценкой параметров. Для этого выделить любую кнопку точечной диаграммы и вызвать контекстное меню. В нем выбрать команду **Добавить линию тренда**. В диалоговом окне тренда выбираем тип **Линейная**, показать уравнение на диаграмме, поместить на диаграмму величину достоверности аппроксимации (R^2).

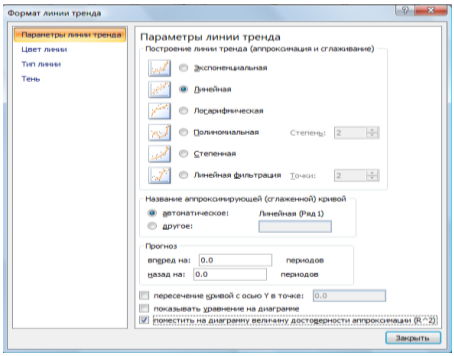

Рис. 25. Диалоговое окно линии тренда

На экране появится уравнение с числовыми параметрами и коэффициент достоверности оценки параметров.

4. Составьте прогноз на некоторый период.

Лабораторная работа № 14
Программно-аппаратные средства защиты от НСД

Цель работы: анализ возможностей программно-аппаратных средств защиты от несанкционированного доступа к информации.

Задание 1.

Проанализировать возможности и основные характеристики программно-аппаратных средств «СЗИ НСД Аккорд-АМДЗ» и «ПСКЗИ ШИПКА» на сайте http://www.accord.ru. Составить отчет, содержащий краткие сведения о данных продуктах.

Задание 2.

В сети Интернет с помощью средств поиска или по адресам, указанных преподавателем, найти и проанализировать информацию о программно-аппаратных средствах, обеспечивающих защиту от несанкционированного доступа к информации:

1. Программно-аппаратный комплекс «Аккорд».
2. Программно-аппаратная система защиты Secret-Net.
3. Программно-аппаратная система «Криптон-Вето».

Заполнить таблицу:

Характеристики системы	«Аккорд»	Secret-Net	«Крип-тон-Вето»
Поддерживаемые ОС			
Момент загрузки системы (н-р, перед ОС)			
Блокировка физических каналов			
Разграничение доступа к ресур-сам системы			
Идентификация/ аутентификация			
Ведение журнала событий			
Контроль целостности аппарат-ных и программных средств			
Подсистемы (компоненты)			
Особенности			

Лабораторная работа № 15
Межсетевые экраны

Цель работы: анализ возможностей межсетевых экранов.

Задание 1.

Используя поисковые системы, проанализировать инфор-мацию о межсетевых экранах, например, FireWall-1, Agnitum Outpost Firewall, ZoneAlarm Anti-Spyware, Comodo Firewall Pro.

Показатели	Брандмауэр 1	Брандмауэр 2
Название		
Производитель		
Назначение		
Поддерживаемые ОС		
Ключевые возможности		
Поддерживаемые протоколы		
Тип системы (программный, программно-аппаратный)		
Статистическая фильтрация		
Динамическая фильтрация		
Проксирование		

Лабораторная работа № 16
Средства антивирусной защиты информации

Цель работы: изучение возможностей средств антивирусной защиты информации, сравнение разных продуктов. Выявление преимуществ и недостатков.

Задание 1.

1. Найти в Интернете методы профилактики от заражения вирусами компьютера, признаки заражения и действия пользователя при наличии признаков заражения.

2. Зайти на сайт www.kaspersky.ru. Изучить понятия и терминологию, используемые в антивирусных программах.

Заполнить таблицу:

Лаборатория Касперского	
Клиенты	
Продукты	
Защита от следующих видов угроз:	
Защита типов устройств:	
Обслуживание (сервис)	
Kaspersky Internet Security 2010	
Поддерживаемые ОС	
Аппаратные требования	
Содержание данного продукта	
Новинки продукта	
Дополнительные возможности	

Задание 2.

Заполнить таблицу сведениями об антивирусных программах.

Технические характеристики программы	**AVP**	**Dr.Web**
Поддерживаемые ОС		
Монитор. Сканер		
Ревизор		
Эвристический анализатор		
Проверка архивов		
Проверка электронной почты		

Лабораторная работа № 17
Методы защиты информации. Шифр Цезаря.

Цель работы: освоить технологию шифрования и дешифрования информации в среде Excel с использованием шифра Цезаря.

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки). Свое название этот шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке.

При шифровании исходного текста каждая буква заменяется другой буквой того же алфавита по следующему правилу. Заменяющая буква определяется путем смещения по алфавиту к концу от исходной буквы на ***k*** букв. При достижении конца алфавита выполняется циклический переход к его началу.

Например: пусть **A** – используемый алфавит:

A={a1, a2,…,am,...,aN},

где: a1, a2,…,am,...,aN – символы алфавита; N – ширина алфавита.

Пусть k – число позиций сдвига символов алфавита при шифровании, 0<k<N. При шифровании каждый символ алфавита с номером m из кодируемого текста заменяется на символ этого же алфавита с номером m+k. Если m+k>N, номер символа в алфавите A определяется как m+k-N.

Для дешифрования текстовой информации номер позиции символа восстанавливаемого текста определяется как m-k. Если m-k<0, то вычисление этого номера производится как m-k+N.

Достоинством этой системы является простота шифрования и дешифрования. К недостаткам системы Цезаря следует отнести:

– подстановки, выполняемые в соответствии с системой Цезаря, не маскируют частот появления различных букв исходного и отрытого текста;

– сохраняется алфавитный порядок в последовательности заменяющих букв;

– при изменении значения k изменяются только начальные позиции такой последовательности;

– число возможных ключей k мало;

– шифр Цезаря легко вскрывается на основе анализа частот появления букв в шифре.

Задание 1.

Зашифровать текст с помощью шифра Цезаря.

Порядок выполнения задания

1. Войти в среду **Excel**. Создать новый документ, перейти на второй лист этого документа. Начиная с ячейки A1 до A40, набрать алфавит, как показано на рис. 26.

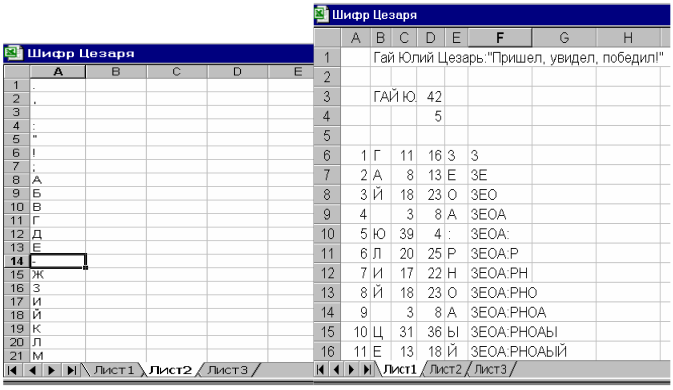

Рис. 26. Шифр Цезаря

Выделить весь диапазон алфавита и назначить ему имя «ABC» (через контекстное меню).

2. На первом листе документа в ячейке B1 набрать текст, который необходимо зашифровать. Например, Гай Юлий Цезарь: «Пришел, увидел, победил!» При наборе текста необходимо использовать только те символы, которые входят в алфавит.

3. В ячейке B3 записать формулу «=ПРОПИСН(B1)», функция ПРОПИСН переводит буквенные символы в строке в прописные буквы.

4. В ячейке D3 записать формулу «=ДЛСТР(B3)», функция ДЛСТР позволяет определить длину строки, что необходимо пользователю, для кодировки исходной строки.

5. В ячейку D4 записать значение k, например 5.

6. В столбце А, начиная с ячейки А6, пронумеровать ячейки числами последовательного ряда от 1 до N, где N – число символов в тексте, включая пробелы.

N рассчитано в ячейке D3.

7. В ячейку В6, записать формулу «=ПСТР(B$3;A6;1)», которая разделяет кодируемый текст на отдельные символы. Скопировать эту формулу в ячейки В7–В47.

8. В ячейку С6 записать формулу «=ПОИСКПОЗ(B6;ABC;0)». Функция ПОИСКПОЗ производит поиск индекса (номера позиции) символа в массиве ABC, который был определен на листе 2. Скопировать содержимое ячейки С6 в ячейки С7, С8….

9. Получив номер символа в алфавите ABC, произвести сдвиг нумерации алфавита для кодируемой последовательности символов. В ячейку D6 записать формулу: «=ЕСЛИ(ПОИСКПОЗ(B6;ABC;0)+$D$4>36;ПОИСКПОЗ(B6;ABC;0)+$D$4-36;ПОИСКПОЗ(B6;ABC;0)+$D$4)». **(1)**

Эта формула производит сдвиг номеров символов алфавита на величину k и определяет номер заменяющего символа из алфавита ABC. Содержимое D6 скопировать в область D7, D8….

10. Выбрать символы из алфавита ABC в соответствии с новыми номерами. В ячейку Е6 записать формулу «=ИНДЕКС(ABC;D6)». Скопировать содержимое ячейки Е6 в область Е7, Е8….

11. Для получения строки закодированного текста необходимо в ячейку F6 записать «=E6», в ячейку F7 соответственно – «=F6&E7». Далее скопировать содержимое ячейки F7, в область F8, F9…. В последней ячейке FN прочитать зашифрованный текст.

12. Для проверки шифрования произвести дешифрование полученного текста и сравнить его с исходным. На третьем листе выполнить дешифрование аналогично пунктам 2–11 задания. При этом необходимо учесть следующие особенности: в п. 2 набрать зашифрованный текст; в п. 9 в ячейку D6 записать формулу: =ЕСЛИ(ПОИСКПОЗ(B6;ABC;0)-$D$4<0;ПОИСКПОЗ(B6;ABC;0)-$D$4+40;ПОИСКПОЗ(B6;ABC;0)-$D$4). **(2)**

Получение исходного текста в итоговой ячейке F третьей страницы свидетельствует о корректном выполнении задания.

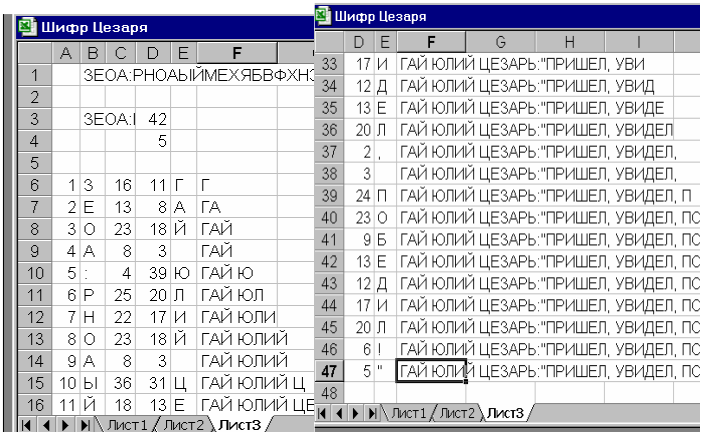

Рис. 27. Результат шифрования (шифр Цезаря)

Лабораторная работа № 18
Электронная цифровая подпись

Цель работы: изучить основы работы с программным средством ЭЦП на основе программы **Pretty Good Privacy** (PGP).

В России имеются нормативно-правовые акты, ограничивающие эксплуатацию нелицензированных программных средств, основанных на криптографии. В связи с этим правовой режим практической эксплуатации программы PGP на территории России в настоящее время не определен. В данном случае речь идет только об ее использовании в качестве наиболее доступной учебной модели.

Задание 1.

Создание ключей в системе PGP

Это и последующие упражнения предполагают, что на компьютере установлена программа PGP, автоматически стартующая при запуске операционной системы.

1. Щелкните на значке **PGPtray** на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт **PGPkeys.** Откроется окно служебного средства **PGPkeys.**

2. Щелкните на кнопке **Generate new keypair** (Сгенерировать новую пару ключей). Произойдет запуск **Мастера генерации ключей** (Key Generation Wizard). Щелкните на кнопке **Далее.**

3. Введите свое полное имя в поле **Full name** (Полное имя) и свой адрес электронной почты в поле **Email address** (Адрес электронной почты). Щелкните на кнопке **Далее.**

4. Установите переключатель **Diffie-Hellman/DSS**. Это более современный алгоритм генерации пары ключей. Щелкните на кнопке **Далее.**

5. Установите переключатель 2048 bits (2048 бит), определяющий длину ключа. Щелкните на кнопке **Далее**. (По надежности ключ такой длины соответствует примерно 128-битному ключу для симметричного шифрования.)

6. Для данного упражнения установите переключатель **Key pair never expires** (Пара ключей действует бессрочно). На практике рекомендуется задавать ограниченный срок действия ключей. Щелкните на кнопке **Далее.**

7. Дважды введите произвольную **парольную фразу** (Passphrase) в соответствующие поля. Так как в данном случае реальная секретность не существенна, можно **сбросить флажок Hide Typing** (Скрыть ввод), чтобы вводимый текст отображался на экране. Рекомендуется, чтобы парольная фраза легко запоминалась, но при этом содержала пробелы, буквы разного регистра, цифры, специальные символы. Качество (трудность подбора) ключевой фразы отображается с помощью индикатора **Passphrase Quality** (Качество ключевой фразы). Удобно использовать какую-нибудь известную цитату или пословицу на русском языке, но вводить ее в латинском регистре. После того как парольная фраза введена дважды, щелкните на кнопке **Далее.**

8. Просмотрите за процессом генерации пары ключей, что может занять до нескольких минут. После появления сообщения Complete **(Готово)** щелкните на кнопке **Далее**. Затем может потребоваться еще несколько щелчков на кнопках **Далее** и в конце – **Готово**, чтобы завершить создание ключей (публикацию ключа на сервере выполнять не следует).

9. Посмотрите, как отображается только что созданный ключ в списке **Keys** (Ключи). Убедитесь, что этот ключ автоматически подписывается его создателем, который, как предполагается, абсолютно доверяет самому себе.

10. Щелкните на ключе правой кнопкой мыши и выберите в контекстном меню пункт **Key Properties** (Свойства ключа). Убедитесь, что установлен флажок **Implicit Trust** (Полное доверие), указывающий, что вы доверяете владельцу данного ключа, то есть самому себе.

В этом упражнении мы научились создавать пару ключей, используемых для несимметричного шифрования в системе PGP. Мы также познакомились с механизмом доверия, используемым для подтверждения подлинности ключей.

Задание 2.

Передача открытого ключа PGP корреспондентам

1. Щелкните на значке **PGPtray** на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт **PGPkeys**. Откроется окно служебного средства **PGPkeys.**

2. Выберите в списке ключ, который планируется передать корреспонденту, и дайте команду **Edit ► Copy** (Правка ► Копировать).

3. Запустите используемую по умолчанию программу электронной почты. Далее мы будем предполагать, что это программа Outlook Express (Пуск ► Программы ► Outlook Express).

4. Щелкните на кнопке **Создать сообщение**. В окне создания нового сообщения введите условный адрес корреспондента, тему сообщения (например, «Мой открытый ключ») и произвольный текст сообщения, объясняющий его назначение.

5. Поместите курсор в конец сообщения и щелкните на кнопке **Вставить** на панели инструментов. Убедитесь, что в

текст сообщения был вставлен символьный блок, описывающий открытый ключ. Сохраните сообщение (отправлять его не обязательно).

6. Проверьте, можно ли перенести ключ в сообщение электронной почты методом перетаскивания.

7. Теперь предположим, что только что созданное сообщение на самом деле было получено по электронной почте. Порядок действий в этом случае очень похож на тот, который использовался для отправки ключа.

8. Выделите текст ключа, включая специальные строки, описывающие его начало и конец.

9. Скопируйте ключ в буфер обмена с помощью комбинации клавиш CTRL+C.

10. Переключитесь на программу PGPkeys.

11. Нажмите комбинацию клавиш CTRL+V. В открывшемся диалоговом окне щелкните на кнопке **Select All** (Выбрать все), а затем на кнопке **Import** (Импортировать).

12. В самом окне **PGPkeys** вы после этого никаких изменений не обнаружите, так как соответствующий ключ уже хранится на данном компьютере.

13. На самом деле пересылать ключи по электронной почте не вполне корректно, так как в таком случае корреспондент имеет естественное право на сомнение: действительно ли ключ поступил от вас. Ключ можно сохранить в файле и передать корреспонденту лично при встрече.

14. Чтобы экспортировать ключ в файл, выберите его и дайте команду **Keys ► Export** (Ключи ► Экспортировать).

15. Выберите каталог и укажите имя файла. Щелкните на кнопке **Сохранить**, чтобы записать ключ в текстовый файл.

В этом упражнении мы научились передавать открытые ключи системы PGP своим корреспондентам, а также получать ключи для расшифровки поступающих сообщений. Мы узнали, что ключ может передаваться по электронной почте или, что предпочтительнее, при личной встрече. Мы также выяснили, что ключ фактически представляет собой длинную последовательность алфавитно-цифровых символов.

Задание 3.

Передача защищенных и подписанных сообщений с помощью системы PGP

1. Запустите программу **Outlook Express** (Пуск ► Программы ► Outlook Express).

2. Щелкните на кнопке **Создать сообщение**. В окне создания нового сообщения введите адрес электронной почты, использованный при создании пары ключей, в качестве адреса отправителя, а также произвольные тему и текст сообщения.

3. Щелкните на значке **PGPtray** на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт **PGPkeys**. Откроется окно служебного средства **PGPkeys**. Выберите **Gurrent Windows**, далее **Sign** (Подписать). В открывшемся диалоговом окне введите парольную фразу, заданную при создании ключей, и щелкните на кнопке **ОК**. Обратите внимание на добавленные служебные строки и электронную подпись в виде последовательности символов, не имеющей видимой закономерности.

4. Выделите весь текст сообщения и нажмите комбинацию клавиш CTRL+C. Щелкните правой кнопкой мыши на значке **PGPtray** на панели индикации и выберите в контекстном меню команду **Clipboard ► Decrypt & Verify** (Буфер обмена ► Расшифровать и проверить). В открывшемся диалоговом окне обратите внимание на сообщение *** PGP Signature Status: good, указывающее на целостность сообщения.

5. Откройте это сообщение, внесите произвольные (большие или небольшие) изменения в текст сообщения или в саму подпись, после чего выполните повторную проверку, как описано в п. 6. Убедитесь, что программа PGP обнаружила нарушение целостности сообщения.

6. Создайте новое сообщение.

7. Щелкните на значке **PGPtray** на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт **PGPkeys**. Откроется окно служебного средства PGPkeys. Выберите **Gurrent Windows**, далее **Encrypt & Sign** (Зашифровать и подписать).

8. Скопируйте текст зашифрованного сообщения в буфер обмена и выполните его расшифровку. По запросу введите па-

рольную фразу. Убедитесь, что при этом как отображается текст исходного сообщения, так и выдается информация о его целостности.

9. Щелкните на кнопке **Copy to Clipboard** (Копировать в буфер обмена), чтобы поместить расшифрованный текст в буфер обмена.

10. Вставьте расшифрованный текст в любом текстовом редакторе и сохраните его как файл.

В этом упражнении мы научились создавать сообщения, снабженные электронной цифровой подписью, а также зашифрованные сообщения.

Задание 4.

Шифрование данных на жестком диске при помощи системы PGP

Система PGP может также использоваться для защищенного хранения файлов на жестком диске. Для шифрования и расшифровки файлов могут использоваться различные механизмы.

1. С помощью текстового процессора **WordPad** создайте произвольный документ и сохраните его под именем **pgp-test.doc**. Можно также скопировать под этим именем какой-либо из уже существующих файлов документов.

2. Откройте этот документ в программе **WordPad** и дайте команду **Правка ► Выделить все**. Нажмите комбинацию клавиш CTRL+C.

3. Щелкните правой кнопкой мыши на значке **PGPtray** на панели индикации и выберите в контекстном меню команду **Clipboard ► Encrypt & Sign** (Буфер обмена ► Зашифровать и подписать).

4. В открывшемся диалоговом окне перетащите созданный вами ключ в список **Recipients** (Получатели) и щелкните на кнопке **ОК**.

5. Введите парольную фразу, используемую для электронной подписи, и щелкните на кнопке **ОК**.

6. Вернитесь в программу WordPad, нажмите клавишу **DELETE** и далее комбинацию CTRL+V. Сохраните документ под именем **pgp-test-clp.doc**. Закройте программу WordPad.

7. Любым способом запустите программу Проводник и откройте папку, в которой лежит файл **pgp-test.doc**.

8. Щелкните правой кнопкой мыши на значке файла и выберите в контекстном меню команду **PGP ► Encrypt & Sign** (PGP ► Зашифровать и подписать). Далее действуйте в соответствии с пп. 4–5.

9. Убедитесь, что в папке появился **файл pgp-test.doc.pgp.**

10. Теперь расшифруем созданные файлы. Запустите программу WordPad и откройте файл **pgp-test-clp.doc**.

11. Щелкните правой кнопкой мыши на значке **PGPtray** на панели индикации и выберите в контекстном меню команду **Current Window ► Decrypt & Verify** (Текущее окно ► Расшифровать и проверить).

12. Введите парольную фразу и щелкните на кнопке ОК.

13. В открывшемся диалоговом окне **Text Viewer** (Просмотр текста) щелкните на кнопке **Copy to Clipboard** (Скопировать в буфер обмена).

14. Вставьте текст в окно программы WordPad и сохраните полученный файл.

15. Откройте программу Проводник и разыщите файл **pgp-test.doc.pgp**. Дважды щелкните на его значке.

16. Введите парольную фразу и щелкните на кнопке **ОК**.

17. Так как оригинал файла не был уничтожен, программа предложит указать, под каким именем следует сохранить файл. Введите это имя по своему усмотрению.

Мы научились отправлять файлы на защищенное хранение, шифруя их при помощи программы PGP. Мы выяснили, что для текстовых данных эту операцию можно применять непосредственно в текущем окне редактора или к данным, находящимся в буфере обмена. Для произвольных файлов выполнить шифрование можно через контекстное меню. Мы также узнали, как расшифровывать зашифрованные файлы, используя разные способы.

Лабораторная работа № 19
Анализ правовой базы ЭК

Цель работы: изучение законодательных актов и нормативных документов в области электронной коммерции.

Задание 1.

Проанализировать основные положения и структуру следующих законопроектов:

1. Федеральная целевая программа «Электронная Россия (2002–2010 гг.)» (кроме информационно-маркетинговых центров).
2. «Об электронной цифровой подписи».
3. «Об информации, информатизации и защите информации»
4. Типовой закон ЮНСИТРАЛ об электронной торговле (кроме электронной цифровой подписи).
5. «О государственном регулировании Внешнеторговой деятельности»
6. «Об электронной коммерции»
7. Рассмотреть влияние закона «Об электронном документе» на развитие электронной коммерции.
8. Какая роль отводится информационно-маркетинговым центрам в федеральной целевой программе «Электронная Россия (2002–2010 гг.)»?
9. «О сделках, совершаемых при помощи электронных средств (об электронных сделках)».
10. «Об участии в международном информационном обмене».
11. «Об электронной торговле».

Лабораторная работа № 20
Баннерная реклама, контекстная реклама, анкеты, системы статистики, online-панели

Цель работы: изучить виды рекламы в сети Интернет, направления и принципы маркетинговых исследований, познакомиться с различными сервисами и системами сбора статистики.

Задание 1.

1. С помощью средств поиска Интернет изучите работу одной из баннерных сетей, сохраните данные в отдельном файле (это могут быть: название сети, предложения, поддерживаемые форматы, статистика, клиенты, цены и т.д.).
2. С помощью средств поиска изучите предложения по организации контекстной рекламы в Интернете, сохраните данные в отдельном файле (это могут быть: название компании, предлагающей услуги, услуги, ценовая политика, клиенты и т.п.).
3. Что такое файлы cookie? Организация поддержки файлов браузером.

Задание 2.

1. В сети Интернет найдите сайты с анкетами, рассмотрите, какие типы вопросов задаются, на что направлено исследование и т.д.
2. Средствами поиска найдите книги отзывов в Интернете, укажите их основные составляющие (например, книга отзыва магазина, турфирмы и др.).

Задание 3.

1. Рассмотреть работу интернет-сервиса «Who is» для определения владельца прав на доменное имя. Есть ли коммерческая значимость определенных доменных имен?
2. Рассмотреть организацию «Желтых страниц в Интернете», определить основные показатели, указываемые в них.
3. Изучите принципы регистрации сайтов в поисковых каталогах и рейтингах.
4. Назовите способы защиты от спама.

5. Определите понятие вирусный маркетинг.
6. Полученную информацию сохраните в отдельном файле.

Задание 4.

Зайдите на сайт отдела интернет-исследований МАСМИ (Россия) – http://www.onlinemonitor.ru/, изучите принципы функционирования online-панели, принципы организации исследований, рассмотрите результаты мониторинга за 2008–2009 гг., условия участия в опросах.

Задание 5.

Изучите работу системы сбора и анализа статистики пользователей на примере систем SpyLog и HOTLog.

Лабораторная работа № 21
Рынок ЭК в Пермском крае

Цель работы*:* анализ развития электронной коммерции в Пермском крае.

Задание 1.

1. Найти в Интернете адреса пермских интернет-магазинов. Проанализировать товары, предлагаемые магазинами, способы оплаты и доставки товаров.
2. Найти информационные порталы Пермского края. Изучить информацию на порталах.
3. Зайти на сайт пермского интернет-аукциона www.1perm.ru. Изучить порядок проведения аукциона, методы поиска товаров, способы оплаты и доставки товара.
4. Провести сравнительный анализ пермских интернет-магазинов, информационных порталов и интернет-аукционов с аналогичными сайтами российских городов. Указать преимущества и недостатки пермских сайтов.
5. Провести анализ ассортимента предлагаемых товаров, уровня цен на товары, разнообразия способов оплаты и доставки товаров, предлагаемых услуг по пред- и послепродажному сервису пермских и российских виртуальных магазинов.

Лабораторная работа № 22
Создание электронной цифровой подписи. Основы шифрования.

Цель работы: изучение методов шифрования и создание ЭЦП.

Электронно-цифровая подпись (**ЭЦП**) используется физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью правомочного лица и скрепленного печатью.

Электронный документ – это любой документ, созданный и хранящийся на компьютере, будь то письмо, контракт или финансовый документ, схема, чертеж, рисунок или фотография.

ЭЦП – это программно-криптографическое средство, которое обеспечивает:

- проверку целостности документов;
- конфиденциальность документов;
- установление лица, отправившего документ.

В алгоритмах электронной подписи и асимметричного шифрования используются секретный и открытый ключи. Причем секретный должен браться абсолютно случайно, например с датчика случайных чисел, а открытый – вычисляться из секретного таким образом, чтобы получить второй из первого было невозможно.

Теоретически нужно проделать следующее.

1. Сначала создайте ключи электронной подписи. Как и в случае шифрования, они обычно хранятся в файлах, в частности на дискетах. Каждый из вас должен иметь свои секретный и открытый ключи.

2. Секретные ключи оставьте у себя, а открытыми обменяйтесь.

3. Секретным ключом подпишите письмо другу и отправьте свое послание вместе с подписью.

4. Получив письмо, снабженное электронной подписью, адресат с помощью вашего открытого ключа проверяет ее под-

линность. Результат проверки – один из ответов: «верна – неверна».

5. Электронная подпись подтверждает достоверность сообщения. Если в него в процессе пересылки были внесены какие-либо изменения, пусть даже совсем незначительные, то подмена обнаружится.

6. Секретный ключ вы должны тщательно хранить в тайне, ведь любой, кто узнает его, сумеет подделать вашу подпись. Если вы все же потеряете свой ключ, то обязательно предпримите определенные меры и, главное, сообщите всем своим потенциальным адресатам о том, что вашу подпись, которую они считали верной, отныне следует считать неверной. А до тех пор, пока вы этого не сделаете, считайте, будто только что подписали пачку пустых листов бумаги.

Сейчас существует множество алгоритмов ЭЦП, в том числе:

- отечественный стандарт электронной подписи ГОСТ Р34.10-94, который, как и стандарт симметричного шифрования ГОСТ 28147-89, обязателен для применения в государственных организациях России и обменивающихся с ними конфиденциальной информацией коммерческих организациях;
- новый отечественный стандарт ГОСТ Р34.10-2001, который должен заменить предыдущий с 1 июля 2002 г.
- различные общеизвестные алгоритмы ЭЦП, например RSA (Rivest – Shamir – Adleman), Эль-Гамаля, DSA (Digital Signature Algorithm).

Использование **ЭЦП** позволит:

- значительно сократить время, затрачиваемое на оформление сделки и обмен документацией;
- усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов;
- гарантировать достоверность документации;
- минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена;
- построить корпоративную систему обмена документами.

Подделать **ЭЦП** невозможно, так как это требует огромного количества вычислений, которые не могут быть реализова-

ны при современном уровне математики и вычислительной техники за приемлемое время, то есть пока информация, содержащаяся в подписанном документе, сохраняет актуальность. Дополнительная защита от подделки обеспечивается сертификацией Удостоверяющим центром открытого ключа подписи.

С использованием **ЭЦП** работа по схеме «разработка проекта в электронном виде – создание бумажной копии для подписи – пересылка бумажной копии с подписью – рассмотрение бумажной копии – перенос ее в электронном виде на компьютер» уходит в прошлое.

Задание 1.

Создание ключей в системе PGP

Это и последующие упражнения предполагают, что на компьютере установлена программа PGP, автоматически стартующая при запуске операционной системы.

1. Щелкните на значке **PGPtray** на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт **PGPkeys**. Откроется окно служебного средства **PGPkeys.**

2. Щелкните на кнопке **Generate new keypair** (Сгенерировать новую пару ключей). Произойдет запуск **Мастера генерации ключей** (Key Generation Wizard). Щелкните на кнопке **Далее.**

3. Введите свое полное имя в поле **Full name** (Полное имя) и свой адрес электронной почты в поле **Email address** (Адрес электронной почты). Щелкните на кнопке **Далее.**

4. Установите переключатель Diffie-Hellman/DSS. Это более современный алгоритм генерации пары ключей. Щелкните на кнопке **Далее.**

5. Установите переключатель 2048 bits (2048 бит), определяющий длину ключа. Щелкните на кнопке **Далее**. (По надежности ключ такой длины соответствует примерно 128-битному ключу для симметричного шифрования.)

6. Для данного упражнения установите переключатель Key pair never expires (Пара ключей действует бессрочно). На практике рекомендуется задавать ограниченный срок действия ключей. Щелкните на кнопке **Далее.**

7. Дважды введите произвольную парольную фразу (Passphrase) в соответствующие поля. Так как в данном случае реальная секретность не существенна, можно сбросить флажок **Hide Typing** (Скрыть ввод), чтобы вводимый текст отображался на экране. Рекомендуется, чтобы парольная фраза легко запоминалась, но при этом содержала пробелы, буквы разного регистра, цифры, специальные символы. Качество (трудность подбора) ключевой фразы отображается с помощью индикатора Passphrase Quality (Качество ключевой фразы). Удобно использовать какую-нибудь известную цитату или пословицу на русском языке, но вводить ее в латинском регистре. После того как парольная фраза введена дважды, щелкните на кнопке **Далее.**

8. Просмотрите за процессом генерации пары ключей, что может занять до нескольких минут. После появления сообщения **Complete** (Готово) щелкните на кнопке **Далее**. Затем может потребоваться еще несколько щелчков на кнопках **Далее** и в конце – **Готово**, чтобы завершить создание ключей (публикацию ключа на сервере выполнять не следует).

9. Посмотрите, как отображается только что созданный ключ в списке **Keys** (Ключи). Убедитесь, что этот ключ автоматически подписывается его создателем, который, как предполагается, абсолютно доверяет самому себе.

10.Щелкните на ключе правой кнопкой мыши и выберите в контекстном меню пункт **Key Properties** (Свойства ключа). Убедитесь, что установлен флажок **Implicit Trust** (Полное доверие), указывающий, что вы доверяете владельцу данного ключа, то есть самому себе.

В этом упражнении мы научились создавать пару ключей, используемых для несимметричного шифрования в системе PGP. Мы также познакомились с механизмом доверия, используемым для подтверждения подлинности ключей.

Задание 2.

Передача открытого ключа PGP корреспондентам

1. Щелкните на значке **PGPtray** на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт **PGPkeys**. Откроется окно служебного средства **PGPkeys.**

2. Выберите в списке ключ, который планируется передать корреспонденту, и дайте команду **Edit ► Copy** (Правка ► Копировать).

3. Запустите используемую по умолчанию программу электронной почты. Далее мы будем предполагать, что это программа **Outlook Express** (Пуск ► Программы ► Outlook Express).

4. Щелкните на кнопке **Создать сообщение**. В окне создания нового сообщения введите условный адрес корреспондента, тему сообщения (например, «Мой открытый ключ») и произвольный текст сообщения, объясняющий его назначение.

5. Поместите курсор в конец сообщения и щелкните на кнопке **Вставить** на панели инструментов. Убедитесь, что в текст сообщения был вставлен символьный блок, описывающий открытый ключ. Сохраните сообщение (отправлять его не обязательно).

6. Проверьте, можно ли перенести ключ в сообщение электронной почты методом перетаскивания.

7. Теперь предположим, что только что созданное сообщение на самом деле было получено по электронной почте. Порядок действий в этом случае очень похож на тот, который использовался для отправки ключа.

8. Выделите текст ключа, включая специальные строки, описывающие его начало и конец.

9. Скопируйте ключ в буфер обмена с помощью комбинации клавиш CTRL+C.

10. Переключитесь на программу PGPkeys.

11. Нажмите комбинацию клавиш CTRL+V. В открывшемся диалоговом окне щелкните на кнопке **Select All** (Выбрать все), а затем на кнопке **Import** (Импортировать).

12. В самом окне PGPkeys вы после этого никаких изменений не обнаружите, так как соответствующий ключ уже хранится на данном компьютере.

13. На самом деле, пересылать ключи по электронной почте не вполне корректно, так как в таком случае корреспондент имеет естественное право на сомнение: действительно ли ключ поступил от вас. Ключ можно сохранить в файле и передать корреспонденту лично, при встрече.

14. Чтобы экспортировать ключ в файл, выберите его и дайте команду **Keys ► Export** (Ключи ► Экспортировать).

15. Выберите каталог и укажите имя файла. Щелкните на кнопке **Сохранить**, чтобы записать ключ в текстовый файл.

Задание 3.

Передача защищенных и подписанных сообщений с помощью системы PGP

1. Запустите программу **Outlook Express** (Пуск ► Программы ► Outlook Express).

2. Щелкните на кнопке **Создать сообщение**. В окне создания нового сообщения введите адрес электронной почты, использованный при создании пары ключей, в качестве адреса отправителя, а также произвольные тему и текст сообщения.

3. Щелкните на значке **PGPtray** на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт **PGPkeys**. Откроется окно служебного средства **PGPkeys**. Выберите **Gurrent Windows**, далее **Sign** (Подписать). В открывшемся диалоговом окне введите парольную фразу, заданную при создании ключей, и щелкните на кнопке **ОК**. Обратите внимание на добавленные служебные строки и электронную подпись в виде последовательности символов, не имеющей видимой закономерности.

4. Выделите весь текст сообщения и нажмите комбинацию клавиш CTRL+C. Щелкните правой кнопкой мыши на значке **PGPtray** на панели индикации и выберите в контекстном меню команду **Clipboard ► Decrypt** & **Verify** (Буфер обмена ► Расшифровать и проверить). В открывшемся диалоговом окне обратите внимание на сообщение *** PGP Signature Status: good, указывающее на целостность сообщения.

5. Откройте это сообщение, внесите произвольные (большие или небольшие) изменения в текст сообщения или в саму подпись, после чего выполните повторную проверку, как описано в п. 6. Убедитесь, что программа PGP обнаружила нарушение целостности сообщения.

6. Создайте новое сообщение.

7. Щелкните на значке **PGPtray** на панели индикации правой кнопкой мыши и выберите в контекстном меню пункт

PGPkeys. Откроется окно служебного средства **PGPkeys**. Выберите **Gurrent Windows**, далее **Encrypt** & **Sign** (Зашифровать и подписать).

8. Скопируйте текст зашифрованного сообщения в буфер обмена и выполните его расшифровку. По запросу введите парольную фразу. Убедитесь, что при этом как отображается текст исходного сообщения, так и выдается информация о его целостности.

9. Щелкните на кнопке **Copy to Clipboard** (Копировать в буфер обмена), чтобы поместить расшифрованный текст в буфер обмена.

10. Вставьте расшифрованный текст в любом текстовом редакторе и сохраните его как файл.

Задание 4.

Шифрование данных на жестком диске при помощи системы PGP

Система PGP может также использоваться для защищенного хранения файлов на жестком диске. Для шифрования и расшифровки файлов могут использоваться различные механизмы.

1. С помощью текстового процессора WordPad создайте произвольный документ и сохраните его под именем pgp-test.doc. Можно также скопировать под этим именем какой-либо из уже существующих файлов документов.

2. Откройте этот документ в программе WordPad и дайте команду **Правка ► Выделить все**. Нажмите комбинацию клавиш CTRL+C.

3. Щелкните правой кнопкой мыши на значке **PGPtray** на панели индикации и выберите в контекстном меню команду **Clipboard ► Encrypt & Sign** (Буфер обмена ► Зашифровать и подписать).

4. В открывшемся диалоговом окне перетащите созданный вами ключ в список **Recipients** (Получатели) и щелкните на кнопке **ОК**.

5. Введите парольную фразу, используемую для электронной подписи, и щелкните на кнопке **ОК**.

6. Вернитесь в программу WordPad, нажмите клавишу **DELETE** и далее комбинацию CTRL+V. Сохраните документ под именем pgp-test-clp.doc. Закройте программу WordPad.

7. Любым способом запустите программу «Проводник» и откройте папку, в которой лежит файл pgp-test.doc.

8. Щелкните правой кнопкой мыши на значке файла и выберите в контекстном меню команду **PGP ► Encrypt & Sign** (PGP ► Зашифровать и подписать). Далее действуйте в соответствии с пп. 4–5.

9. Убедитесь, что в папке появился файл pgp-test.doc.pgp.

10. Теперь расшифруем созданные файлы. Запустите программу WordPad и откройте файл pgp-test-clp.doc.

11. Щелкните правой кнопкой мыши на значке **PGPtray** на панели индикации и выберите в контекстном меню команду **Current Window ► Decrypt & Verify** (Текущее окно ► Расшифровать и проверить).

12. Введите парольную фразу и щелкните на кнопке **ОК**.

13. В открывшемся диалоговом окне **Text Viewer** (Просмотр текста) щелкните на кнопке **Copy to Clipboard** (Скопировать в буфер обмена).

14. Вставьте текст в окно программы WordPad и сохраните полученный файл.

15. Откройте программу «Проводник» и разыщите файл pgp-test.doc.pgp. Дважды щелкните на его значке.

16. Введите парольную фразу и щелкните на кнопке **ОК**.

17. Так как оригинал файла не был уничтожен, программа предложит указать, под каким именем следует сохранить файл. Введите это имя по своему усмотрению.

СПИСОК ЛИТЕРАТУРЫ

1. Брагин Л. А. Экономика торгового предприятия. Торговое дело: учеб. для студентов вузов / Л. А. Брагин, Г. Г. Павлов, Б. Л. Межиров и др.; под ред. Л. А. Брагина; Рос. экон. акад. им. Г. В. Плеханова. Москва: Инфра-М, 2010. 314 с.

2. Бунеева Р. И. Коммерческая деятельность: организация и управление: учебник / Р. И. Бунеева. Ростов-на-Дону: Феникс, 2009. 365 с.

3. Гаврилов Л. П. Информационные технологии в коммерции и бизнесе / Л. П. Гаврилов. Москва: Юрайт, 2013.

4. Гаврилов Л. П. Электронная коммерция. Учебное пособие по выполнению практических работ. М.: СОЛОН – Пресс, 2019.

5. Гореткина Е. ИТ в ритейле: взвешенный подход (обзор) / Е. Гореткина // PC Week. 2014. № 10.

6. Дашков Л. П. Организация и управление коммерческой деятельностью: учеб. для студ. вузов / Л. П. Дашков, О. В. Памбухчиянц. Москва: Дашков и К°, 2012. 688 с.

7. Калужский М. Л. Электронная коммерция: маркетинговые сети и инфраструктура рынка / М. Л. Калужский; ОмГТУ. Москва: Экономика, 2014. 328 с.

8. Киселева Е. Н. Организация коммерческой деятельности по отраслям и сферам применения: учеб. пособие для студ. вузов / Е. Н. Киселева, О. Г. Буданова. Москва: Вузовский учебник, 2011. 192 с.

9. Кобелев О. А. Электронная коммерция: Учебное пособие / Под ред. проф. С. В. Пирогова. 3-е изд., перераб. и доп. М.: Издательско-торговая корпорация «Дашков и К^0», 2018. 684 с.

10. Мобильные коммуникации в электронной коммерции и бизнесе: Учебное пособие / Л. П. Гаврилов. М: Финансы и статистика, 2016. 336 с.

11. Пантелеева Е. К. Потребительский опыт в e-commerce: анализ рациональных и эмоциональных потребительских инсайтов / Е. К. Пантелеева, Н. И. Михайлова // Маркетинг и маркетинговые исследования. 2016. № 6. С. 458–469.

12. Сибирская Е. В., Старцева О. А. Электронная коммерция: учебное пособие / Е. В. Сибирская, О. А. Старцева. М.: ФОРУМ, 2018. 288 с.: ил. (Высшее образование).

13. Системы электронной коммерции (практическое руководство): Учебное пособие / Я. В. Ахромов. М: Издательство Оникс, 2017. 416 с.

14. Электронный бизнес и коммерция: ответы на экзаменационные вопросы / Т. Ф. Старовойтова. Минск: ТетраСистемс, 2009. 144 с.

15. Глотов В. С., Шалатов Д. В. Интернет-технологии и электронная торговля: экономика, право, программное обеспечение. Изд. 2-е, перераб. и доп. В 2-х ч. / Под. ред. С. А. Глотова / Центр прав человека и защиты прав потребителей РГТЭУ, Кубанский научный Центр социальных исследований «Законодательная инициатива», Краснодарский ин-т (филиал) РГТЭУ. М.: НИЦ «Инженер», 2007. 452 с.

16. Информационные технологии управления: Учеб. пособие для вузов / Под ред. проф. Г. А. Титоренко. 2-е изд., доп. М.: ЮНИТИ-ДАНА, 2007. 439 с.

17. Калинина А. Э. Интернет-бизнес и электронная коммерция: Учебное пособие. Волгоград: Изд-во ВолГУ, 2004. 148 с.

Интернет-источники

1. Система электронных платежей ASSIST. Режим доступа: www.assist.ru

2. Платежная система «КиберПлат». Режим доступа: www.cyberplat.ru

3. Информационно-консалтинговый центр по электронному бизнесу. Режим доступа: www.e-commerce.ru

4. « Молоток.Ру» – крупнейшая торговая площадка, интернет-аукцион. Режим доступа: www.molotok.ru

5. Подборка законов и др. законных, подзаконных и незаконных актов по логистике. Режим доступа: www.sklad-zakonov.narod.ru

6. Платежная система WebMoney. Режим доступа: www.webmoney.ru

7. Шалева О. И. Электронная коммерция / О. И. Шалева. URL: http://uchebnikionline.com/informatika/elektronnakomertsiya

shaleva_oi/organizatsiya_tehnologiya_roboti_internet-magazinu.htm (дата обращения 11.01.20).

8. Федеральный закон от 27 июня 2011 г. № ФЗ-161 «О национальной платежной системе» [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/consdoc LAW115625/

Учебное издание

Вологжанин Олег Юрьевич
канд. техн. наук, доцент Пермского государственного
национального исследовательского университета

Ильин Вадим Владимирович
д-р техн. наук, профессор Пермского государственного
национального исследовательского университета

Галкина Людмила Сергеевна
канд. пед. наук, доцент Пермского института (филиала)
РЭУ имени Г. В. Плеханова

Электронная коммерция

Учебное пособие

Редактор *А. С. Серебреников*
Корректор *С. А. Вороненко*
Компьютерная верстка: *Е. А. Шкураток*

Объем данных 2,40 Мб
Подписано к использованию 21.02.2024

Размещено в открытом доступе
на сайте www.psu.ru
в разделе НАУКА / Электронные публикации
и в электронной мультимедийной библиотеке ELiS

Управление издательской деятельности
Пермского государственного
национального исследовательского университета
614068, г. Пермь, ул. Букирева, 15