Ю.В. КРУТИН

ЭЛЕКТРОННАЯ КОММЕРЦИЯ

ЕКАТЕРИНБУРГ

2018

АННОТАЦИЯ

Данное электронное пособие предназначено для студентов всех форм обучения направления подготовки 09.03.03 Прикладная информатика профиля «Прикладная информатика в экономике», изучающих дисциплину «Электронная коммерция».

Целью изучения курса «Электронная коммерция» является формирование у студентов профессиональных компетенций в области электронной коммерции, развитие элементарных практических умений в области оценки, эксплуатации, адаптации и сопровождения информационных систем и сервисов электронной коммерции.

Задачи изучения дисциплины:

- освоение теоретических основ организации и функционирования предприятий электронной коммерции;
- изучение вопросов, связанных с обеспечением безопасной и эффективной деятельности предприятий электронной коммерции;
- изучение вопросов, связанных с построением безопасной и эффективной инфраструктуры предприятий электронной коммерции;
- освоение технологии использования и поддержки основных сервисов электронной коммерции;
- освоение технологии настройки, эксплуатации и сопровождения информационных систем электронной коммерции;
- изучение принципов и методов анализа рынка программно-технических средств, информационных продуктов и услуг для создания и модификации информационных систем электронной коммерции.

В результате изучения курса студенты должны:

знать:

- сущность и основные бизнес-модели электронной коммерции;

- технологию настройки, эксплуатации и сопровождения информационных систем и сервисов электронной коммерции;
- принципы и методы анализа рынка программно-технических средств, информационных продуктов и услуг для создания и модификации информационных систем электронной коммерции.

уметь:

- анализировать печатные и интернет-источники для поиска новых возможностей развития предприятий электронной коммерции;
- использовать финансовую отчетность для определения эффективности деятельности предприятий электронной коммерции;
- адаптировать, эксплуатировать и сопровождать информационные системы и сервисы электронной коммерции.

владеть:

- навыками установки, адаптации, настройки и сопровождения информационных систем и сервисов электронной коммерции;
- методами анализа рынка информационных систем и сервисов электронной коммерции.

В электронном учебном пособии представлены следующие темы:

Тема 1. «Электронный бизнес и электронная коммерция: основные понятия».

Тема 2. «Платежные системы Интернет».

Тема 3. «Роль поисковых систем в электронной коммерции и продвижении сайтов».

Тема 4. «Интернет-маркетинг и веб-аналитика».

Тема 5. «Информационная безопасность в сфере электронной коммерции»

СОДЕРЖАНИЕ

ТЕМА 1. ЭЛЕКТРОННЫЙ БИЗНЕС И ЭЛЕКТРОННАЯ КОММЕРЦИЯ: ОСНОВНЫЕ ПОНЯТИЯ

Электронный бизнес

Развитие телекоммуникаций привело к тому, что в настоящее время частные лица и компании во всем мире связаны друг 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 — 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 годов XX века. 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:

Рисунок 1 - Торговая марка "Электронный бизнес"

«***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, онлайн-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.

Электронная коммерция

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» - узкое и широкое.

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.

Электронная 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.

Предпосылки возникновения электронной коммерции

Существуют экономические и технические предпосылки возникновения электронной коммерции.

Экономические предпосылки

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

- в I-й четверти XX века - внедрения принципов массового производства;
- во II-й четверти XX века – расширенной механизации производства;
- в III-й четверти XX века - автоматизации производства;
- в IV-й четверти XX века – 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 продвижения товаров от производителя к потребителю. ***Поэтому, 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 века 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 Интернет, так как благодаря этому, а также развитию сетей телекоммуникаций открылась возможность комплексной автоматизации коммерческой деятельности.

Часто при анализе взаимосвязи ЭК и Интернет, 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.

ТЕМА 2. ПЛАТЕЖНЫЕ СИСТЕМЫ ИНТЕРНЕТ

Основные понятия и классификация платёжных систем

Платежная система Интернет - 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 Интернет, 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 оффлайновым 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 Интернет, 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 онлайновом 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.

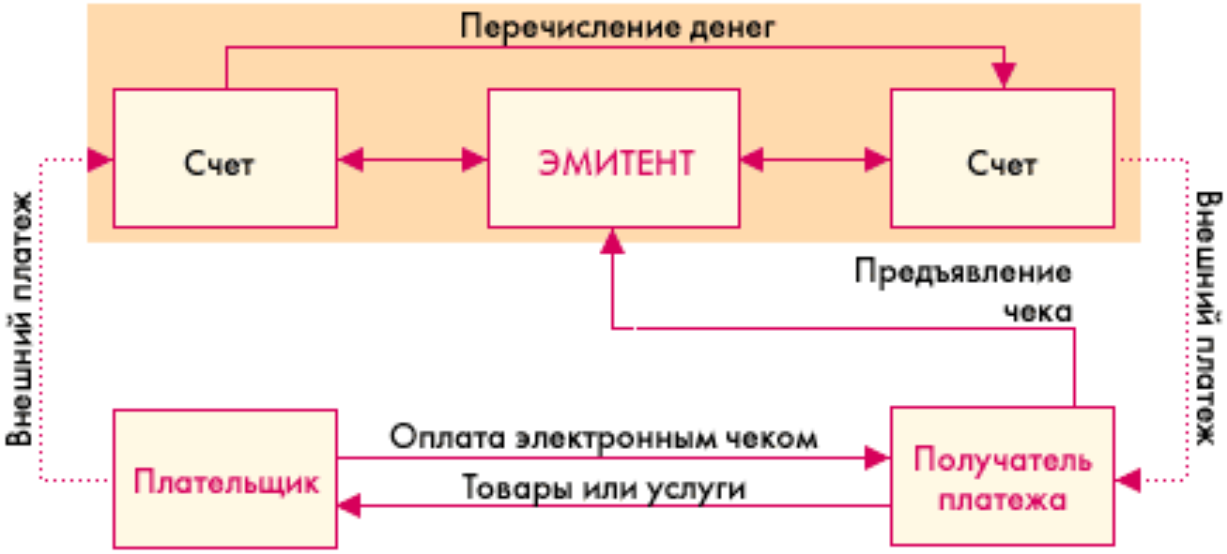

Рисунок 2 - Схема платежа с исползованием электронных чеков

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 оффлайновых 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 институтами, 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, например, «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. Так, 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 предавторизованных 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.

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.

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.

Ниже 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 реальных денег на счет они заверяются печатью и отправляются обратно клиенту.

Наряду с удобствами такого хранения, у него имеются и недостатки. Порча диска или смарт-карты 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.

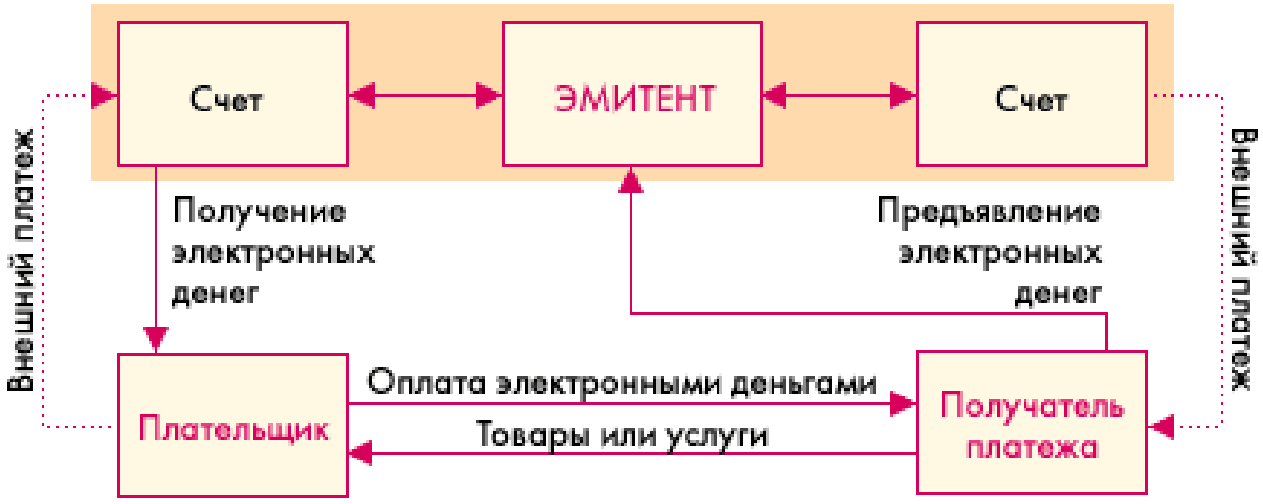

Рисунок 3 - Схема платежей с использованием электронных денег

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 Интернет.

Наиболее известными платежными системами в России являются Webmoney, Yandex.Деньги, CyberPlat, Mondex и другие.

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 в Интернет.
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 Интернет. Электронные компоненты, являющиеся посредниками между остальными участниками.

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

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.

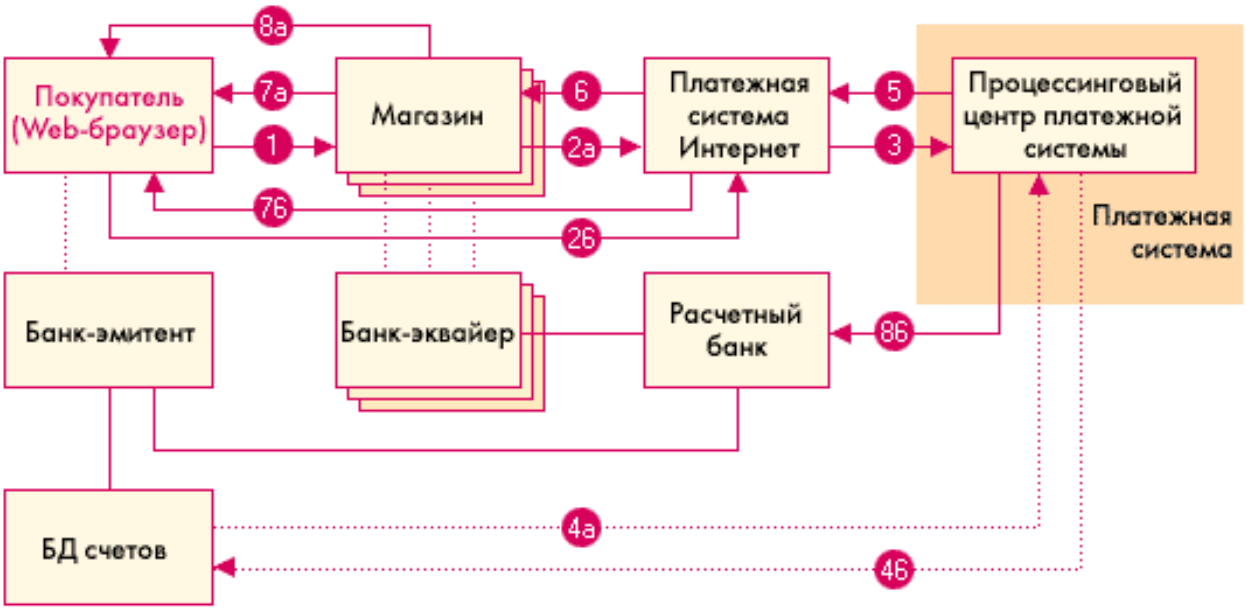

Рисунок 4 - Схема платежей в кредитной системе

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 Интернет передает запрос на авторизацию традиционной платежной системе.

2. Последующий шаг зависит от того, ведет ли банк-эмитент онлайновую 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 запросы 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.

Примеры платежных систем

WebMoney Transfer

WebMoney Transfer представляет собой систему мгновенных расчетов электрон¬ными 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.

Территория WebMoney сегодня - 1970 населенных пунктов в 42 странах мира.

Программное обеспечение

Общение пользователей системы (как владельцев магазинов, так и покупателей) друг с другом производится с помощью WebMoney Keeper. WebMoney Keeper - программа, предназначенная для широкого примене-ния пользователями системы WebMoney Transfer и позволяющая хранить, накапливать, принимать и переводить электронные деньги. Такие программы

обычно называют «электронными кошельками» (но в данном случае это выражение 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 неудовлетворен 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

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

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

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

• Пользователь может перевести любую валюту в электронные деньги.

• 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 (пользователь 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

Как и обычный кошелек, «кошелек электронный» нуждается в регулярном пополнении. Эту задачу можно выполнить несколькими путями:

- 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.
- Перевести российские рубли через любое отделение СБЕР-БАНКА 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.
- 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.

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

- Система поддерживает одновременное использование до 255 валют.
- Сумма платежа может быть выражена практически любым числом с точностью до 0,001 копейки.
- 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.

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

CyberPlat

Система CyberPlat была создана в 1997 году, 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 Интернет, 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 электрон-ной цифровой подписью с длиной ключа 512 бит. Благодаря перечисленным свойствам, подсистема используется в схемах класса business-to-business.

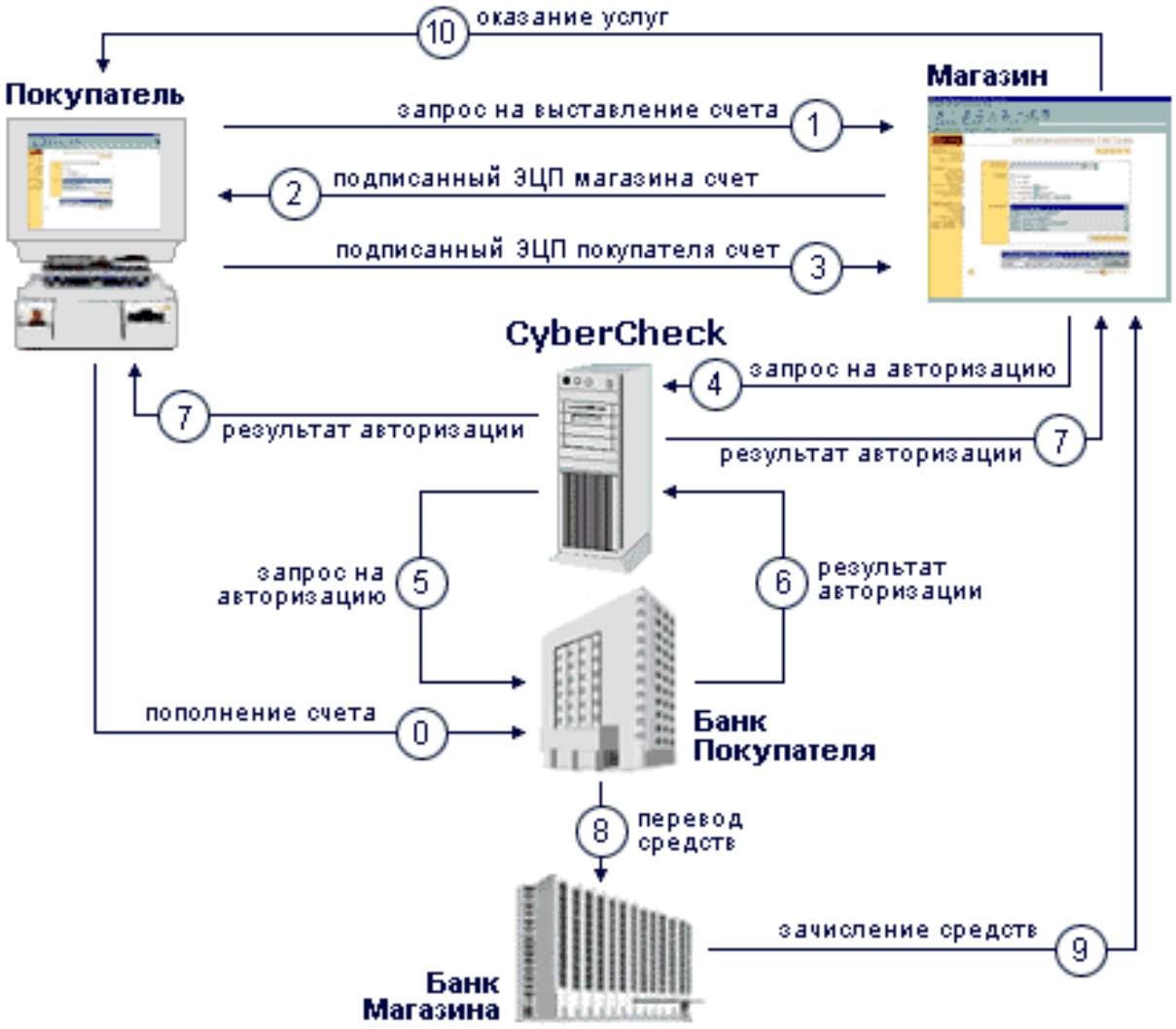

Рисунок 5 - Online покупка и проведение платежа

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 реги-страции 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 предоставляются 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 документов, которые заверяются электронными цифровыми подписями (ЭЦП) сторон, имеют юридическую силу (ст. 160, п.2 Гражданского Кодекса РФ) и пригодны для разбирательства в обычном

арбитражном 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

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 зарегистрироваться 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.

Денежная составляющая платежной системы: правовой подход

Правовая природа электронных денег: обязательно-правовая модель

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 статье 27 Федерального закона «О Центральном банке Российской Федерации (Банке России)», которая прямо запрещает введение на территории Российской Федерации других денежных суррогатов. В соответствии со статьёй 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 нари-цательной 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 дан-ном 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, право-отношения, 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.

Эмиссия электронных денег

Условиями эмиссии электронных денег являются:

- Заключение договора между эмитентом и будущим держателем электронных денег – клиентом эмитента. Заключаемы 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.

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

Обращение электронных денег

Юридически обращение электронных денег происходит путем уступки требования к эмитенту в соответствии со статьей 382 (1) ГК РФ. В данном случае уступка требования рассматривается в качестве основной фор-мы обращения электронных денег, хотя для его юридического обоснования может использоваться также институт исполнения обязательств третьим лицом (статья 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 статьей 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 статьей 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 статье 407 (1) ГК РФ, предусматривающей. 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».

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.

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. Статья 160 ГК допускает при заключении сделок использование не собственноручной подписи, а ее аналога. В соответствии со статьей 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 г.). 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.

Дальше все просто - 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 виртуальные 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 тому подобное. 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 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 онлайновой 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.

Дабы 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 - 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 была 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 платежной 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 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 (будущим плательщиком). Размер обеспечения составляет 100%, то

есть банк выпускает электронных денег ровно столько, насколько ему поступает денег обычных.

Итак, благодаря «слепой подписи», «Яндекс.Деньги» обеспечивают высокую степень анонимности платежей. Благодаря использованию механизма платежных книжек и виртуальных счетов обеспечивается юридическая сторона платежной системы. Благодаря привязке 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.

В заключение хотелось бы добавить, что без адекватного правового регулирования на государственном уровне нельзя говорить о едином электронном бизнес-пространстве, которое в настоящее время становится реальностью во многих странах.

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.

ТЕМА 3. РОЛЬ ПОИСКОВЫХ СИСТЕМ В ЭЛЕКТРОННОЙ КОММЕРЦИИ И ПРОДВИЖЕНИИ САЙТОВ

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».

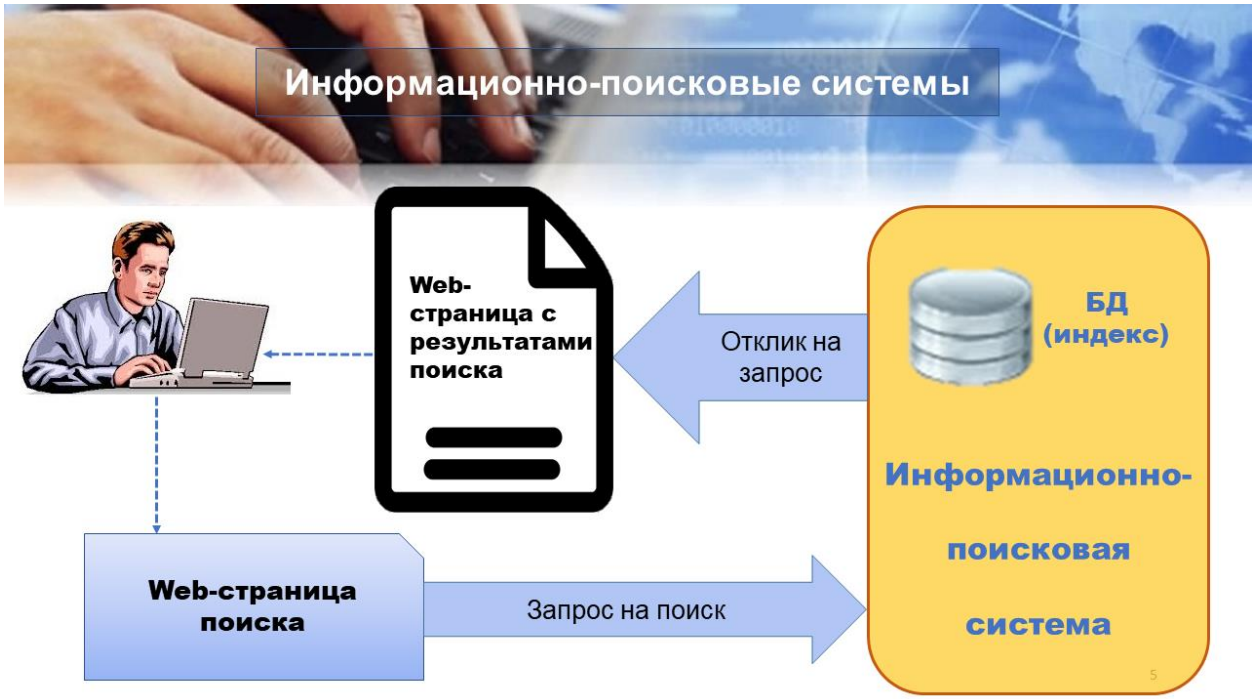

Рисунок 6 - Как ИПС отвечает на запросы пользователей

Поисковая машина – это комплекс программ, предназначенный для поиска информации. Поисковая машина являются ключевым инструментом поиска информации для пользователя, поскольку содержат 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;
- Рэмблер – 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 просматривают 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 достаточно 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.

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.

Возможны проблемы с работой сервера.

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

ТЕМА 4. ИНТЕРНЕТ-МАРКЕТИНГ И WEB-АНАЛИТИКА

Понятие Интернет-маркетинга

По определению Американской маркетинговой ассоциации (AMA) 2004 года «***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, привело к тому, что маркетинг в последние десятилетия все больше рассматривается как направляющая сила деятельности всего предприятия в целом [**1, 4**].

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:

- 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 ж 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.

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 соц. сетях, 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 ими 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. Необходимо 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.

Показатели эффективности для интернет-магазина

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.

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.

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.

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.

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

Отслеживайте не просто источники привлечения посетителей, а их отдачу. Если один из каналов показывает хорошую вовлеченность посетителей на сайте и рост продаж – увеличивайте бюджет на этот канал. А если канал не эффективен, подумайте 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.

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.

Начинайте с оптимизации наиболее важных страниц сайта:

- товарная карточка;
- регистрация;
- корзина;
- оформление заказа.

Тестируйте кнопки “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).

Отслеживайте не просто источники привлечения посетителей, а их отдачу. Если один из каналов показывает хорошую вовлеченность посетителей на сайте и рост продаж – увеличивайте бюджет на этот канал. А если канал не эффективен, подумайте 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.

9. 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.

Постоянно проверяйте работу корзины товаров в вашем интернет-магазине. Тестируйте новые идеи по оптимизации процесса оформления заказа.

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. Для работы с брошенными корзинами можно использовать ***Convead***, он позволяет настраивать воронку продаж, создавать сегмент пользователей, которые не завершили оформление заказа и отправлять им “дожимающие” письма.

ТЕМА 5. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ

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.

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, необходимо провести ее анализ на приоритетность и критичность 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 систем, 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 планирую выход на международную арену.

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.

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.

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.

Проблемы и основные требования безопасности в электронной коммерции

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 Интернет 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 Интернет. 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 Интернет 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.

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, — кража баз данных карточек в ТП. Еще одним способом генерации правильного номера карты являются специальные программы. Программа генерирует правильные номера карт, эмитированных некоторыми 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, почувствовав запах жаренного, 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 ты 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.

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 — 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 PINкода 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 подобного 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 криптоалгоритма, в PIN-код, зашифрованный на симметричном алгоритме шифрования.

Существует другое, неклассическое решение по использованию PINкода. 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 пред приятия и его обслуживающего банка). Под аутентификацией покупателя (продавца) понимается процедура, доказывающая (на уровне надежности известных криптоалгоритмов) факт того, что данный владелец карты действительно является клиентом некоторого эмитента-участника (обслуживающего банка-участника) дан ной 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).

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 [5]. 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 допускающее 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, защищено 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 отправителем 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

Протокол 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.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Капон Н., Колчанов В., Макхалберт Дж. Управление маркетингом. [Электронный ресурс]. — Режим доступа: https://getabook.pp.ua/books/upravlenie-marketingom

2. Котлер Ф., Армстронг Г., Вонг В., Сондерс Дж. Основы маркетинга. [Электронный ресурс]. — Режим доступа: http://artlib.osu.ru/web/books/content_all/1917.pdf

3. Котлер Ф., Келлер К.Л. Маркетинг менеджмент. Экспресс-курс. — [Электронный ресурс]. — Режим доступа: https://nataliaakulova.ru/wp-content/uploads/2015/02/01/Filipp_Kotler_Kevin_Keller_Marketing_menedzhmen.pdf

4. Катаев А.В. Маркетинг: сущность, определения и виды. [Электронный ресурс]. — Режим доступа: http://kataev.ru/28/

5. Горелик С.Л. «Информационная безопасность в системах электронных услуг» [Электронный ресурс]. — Режим доступа: https://elibrary.ru/item.asp?id=22285544

6. Дшхунян В.Л. Электронная идентификация. [Текст] / В.Л Дшхунян; В.Ф. Шальгин. — Москва: АСТ, 2013. — 376 с.

7. Обзор рисков в области электронной коммерции [Электронный ресурс]. — Режим доступа: http://nbj.ru/publs/ot-redaktsii/2014/08/13/obzorriskov-v-oblasti-elektronnoi-kommertsii/index.html

8. Семёнов Ю.А. Протоколы Internet для электронной торговли [Электронный ресурс]. — Режим доступа: http://padabum.com/d.php?id=36936

9. Федеральный закон от 27 июня 2011 г. № ФЗ-161 «О национальной платежной системе» [Электронный ресурс]. — Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_115625/