**Содержание**

Введение

1.Определения и стандарты

2.Потребность в новых технологических стандартах

3.Основные составляющие

4.Базовые элементы электронной коммерции

5.Платежи в Интернете

5.1 Системы цифровых наличных

5.2 Технология «слепой подписи»

5.3 Платежные системы

5.4 Интернет-банкинг

6.Безопасность электронной коммерции

7.Что такое номер карты

8.Новая концепция электронной коммерции от Accenture

9.Отечественный В2В

Заключение

Список использованных электронных ресурсов

**Введение**

Тема контрольной работы «Интернет-коммерция».

Как известно, основными этапами любой коммерческой сделки являются:

- поиск информации;

- заключение контракта;

- поставка товара (услуги);

- платеж.

Эксперты ООН считают, что если любые два из этих четырех этапов выполняются в Интернете, то такая сделка считается электронной коммерцией. Электронная коммерция концентрируется на использовании коммуникационных технологий для того, чтобы сделать бизнес-транзакции более эффективными.

В литературе существует еще несколько определений термина «электронная коммерция»:

- любая форма бизнес-процесса, в котором взаимодействие между субъектами происходит электронным образом;

- любой процесс, который производится посредством сети, связанных между собой компьютеров. Здесь также необходимо выделить Интернет-коммерцию как часть коммерции электронной, ее особенность состоит в том, что все транзакции осуществляются посредством сети Интернет.

Электронные рынки Интернета предназначены для устранения имеющихся у большинства производителей проблем, позволяя поставщику востребованной на рынке продукции в автоматическом и полуавтоматическом режиме взаимодействовать со значительно большим числом продавцов и конечных потребителей, минимизируя время, затрачиваемое на регулярно повторяющиеся операции.

1. **Определения и стандарты**

«Электронная коммерция» как понятие во многом сформировалось после того, как появилась возможность осуществлять взаимодействие с клиентами или партнерами через Web-интерфейсы. Согласно документа «Европейская инициатива в области электронной коммерции», если для традиционной электронной коммерции сеть - это средство для передачи данных, то для электронной Интернет-коммерции, сеть - это рынок (см. табл. 1).

Таблица 1. Отличия традиционной и Интернет-коммерции

|  |  |
| --- | --- |
| Традиционная электронная коммерция | Электронная Интернет-коммерция |
| только «компания -компания» | компания - потребители (В2С)  компания - компания (В2В)  компания - государственные органы власти (B2G)  пользователь - пользователь (С2С) |
| закрытые «клубы», зачастую только для промышленности | открытое рыночное пространство, глобальный масштаб |
| ограниченное число корпоративных партнеров | неограниченное число партнеров |
| закрытые частные сети | открытые незащищенные сети |
| известные и пользующиеся доверием партнеры | известные и неизвестные партнеры |
| защита части сети | требуется защита и идентификация |
| РЫНОК - ЭТО КЛУБ | СЕТЬ - ЭТО РЫНОК |

Электронная коммерция всегда базируется на стандартах, представленных ниже в хронологической последовательности их появления:

- EDI (Electronic Data Interchange), другое название ANSI Х.12 (host-based);

- GTDI (General-purpose Trade Data Interchange standards);

- EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport), принятый ISO (ISO 9735) . В качестве транспортной среды EDIFACT выступает стандарт электронной почты Х.400 (подмножество Х.435);

- EDIINT (EDIFACT over Internet) на базе стандартов для электронной почты Интернет SMTP/S-MIME;

- OBI (Open Buying on the Internet), основанный на EDIINT.

1. **Потребность в новых технологических стандартах**

Простой поиск товаров или услуги в Интернете по их названию может выдать множество ссылок, не имеющих никакого отношения к желаемому результату. Компании Microsoft, Ariba, Hewlett-Packard, IBM и другие (всего более 100) создали консорциум по разработке основанного на XML стандарта Universal Dynamic Discovery and Integration (UDDI), так называемого стандарта электронных «желтых страниц», содержащих информацию о корпорациях всего мира и классифицирующих их. UDDI предлагает универсальный метод выяснения рода деятельности предприятия класса В2В, а также применяемых им протоколов связи и способов осуществления транзакций.

На «белых» страницах находятся названия предприятий, описание рода их деятельности и другая информация, включая используемые ими типы услуг и поддерживаемые технологии связи. «Зеленые» страницы информируют о типах документов, принимаемых компанией, точках входа для транзакций и технологиях, с помощью которых она может взаимодействовать с партнерами.

Компания Commerce One предлагает стандарт для обмена деловыми документами XML Common Business Library (xCBL) 3.0. Он разрабатывался с учетом специфики существовавших ранее стандартов (EDI и OBI) и разрешает использовать ряд стандартизированных форматов документов на основе XML.

Компании Vignette, Sun, Akamai, Macromedia, Rational Software и ряд других (всего 13) создали альянс extended Content Management (ХСМ) Alliance. Целью ХСМ Alliance является определение корпоративных стандартов к системам управления информацией, чтобы сделать совместимыми различные решения по управлению информацией.

Компания Cisco Systems сформировала альянс, целью которого является принятие новых стандартов доставки информации (что должно привести к ускорению развития рынка контент-провайдеров) и продвижение технологии Content Delivery Networks (CDN) сетей доставки информации. В рамках альянса будут разрабатываться открытые стандарты, протоколы и технологии для применения CDN в различных областях, а также будет разработана спецификация для авторизации информации, для совместного подключения и биллинга. Разнообразие охранных систем, используемых компаниями на своих Web-сайтах для персонификации и проверки пользователей и клиентов, препятствует возможности унифицированного обеспечения безопасности электронных транзакций. В связи с этим 45 известных компаний (Cap Gemini Ernst & Young, Citrix, Deloitte & Touche LLP, Epi-centric, Novell, Pricewater-houseCoopers, Royal Bank of Scotland и др.) сформировали рабочую группу AuthXML Working Group, которая будет разрабатывать единый стандарт, разрешающий пользователям Web-сайтов с разноплановой инфраструктурой и технологиями проводить онлайновые транзакции, не беспокоясь об их защищенности.

1. **Основные составляющие**

Как видно из определения, электронная коммерция, по сути, состоит из трех тесно связанных составляющих:

- бизнес-субъектов (участников);

- процессов;

- сетей (посредством которых связываются участники и обеспечиваются процессы).

Субъектами электронной коммерции являются:

*- Финансовые институты.*

Организации, оказывающие услуги, связанные с финансами, в первую очередь это банки, так как именно в них все остальные субъекты электронной коммерции имеют счета, по которым производится реальное движение средств;

*- Бизнес-организации.*

Любые организации, взаимодействующие через Интернет. В более узком смысле это организации, что-либо продающие или приобретающие через Интернет, т. е. осуществляющие торговые операции.

*- Клиенты.*

Это покупатели или потребители услуг.

В секторе *(business-to-business, В2В)* возможен очень широкий спектр взаимоотношений между организациями: производитель товара пытается его продать через своих поставщиков или через дистрибьюторов, которые в свою очередь работают через дилеров и реселлеров.

Когда конечный покупатель-клиент покупает что-либо для себя, то такой сектор рынка называется розничным сектором электронной коммерции, или business-to-consumer, В2С.

К системам В2С не относят:

*- Web-витрины.*

Размещенные в Интернете каталоги продукции или товаров, имеющие минимальные средства оформления заказа;

*- Интернет-магазины.*

Содержат, кроме витрины, всю необходимую бизнес-инфраструктуру для управления процессом электронной торговли через Интернет;

*- Торговые Интернет-системы.*

Интернет-магазины, полностью интегрирован с торговыми бизнес-процессами компаний.

1. **Базовые элементы электронной коммерции**

Одна из причин организации электронной коммерции через Интернет связана с относительно низкой стоимостью (расходы уменьшаются на 70-90 %) транзакций, осуществляемых при обслуживании клиентов и поставках товаров. Полнофункциональный сайт электронной коммерции представляет собой не просто средство отображения каталога товаров. Сайты электронной коммерции, основанные на Web-технологиях, реализуют простой в использовании процесс оформления заказов (через «корзину» или «тележку») с автоматическим подсчетом общей стоимости товаров, включая расходы на доставку товаров и налог с продаж.

В настоящее время сайты электронной коммерции доставляют клиенту информацию о продуктах и принимают заказы и платежи. Многие магазины электронной коммерции подтверждают получение заказов при помощи автоматизированной электронной почты и получают данные об авторизации кредитных карточек в реальном времени.

Краеугольным камнем электронной коммерции являются безопасные транзакции с кредитными карточками и операции по обработке платежей, что могут выполнять далеко не все сайты. Для приема заказов через Интернет с оплатой через кредитные карточки компания нуждается в защищенном сервере с ПО, способным установить защищенное соединение с Интернет-браузером покупателя (большинство покупателей настаивают на установлении защищенного соединения прежде, чем вводить информацию о кредитной карточке).

Компании нуждаются в отслеживании жизненного цикла транзакций. Для этого необходимо рассылать уведомления по электронной почте, принимать электронные сообщения, составлять онлайн-отчеты, отслеживать внутренние базы данных, производить онлайн-поиск по запросам, преобразовывать форматы сообщений и бланков и т. д. На интеграцию онлайн-заказов с имеющимися бизнес-функциями могут быть израсходованы существенные материально-технические и программные ресурсы.

ПО, представляющее собой электронные платежные ведомости, позволяет рассчитывать размеры выплат и налогов, распечатывать и доставлять чеки и формировать отчеты. Кроме того, в электронных платежных ведомостях возможны функции контроля списочного состава и автоматического заполнения налоговых деклараций. Такое ПО должно основываться на клиент-серверной технологии и быть сопряжено с другими внутренними электронными системами организации.

Интенсивность их потока на большинстве сайтов электронной коммерции такова, что типовой сервер баз данных должен обрабатывать до 50 ООО транзакций в минуту. Необходимо также обеспечить непрерывную техническую поддержку для быстрого разрешения возникающих проблем, чтобы не допускать продолжительных простоев.

Проблема обеспечения Web-безопасности является комплексной и включает гарантии безопасности компьютерных систем и сетей, аутентификации, аттестации сообщений, сохранения персональной тайны и криптографии. Поэтому все предприятия электронной коммерции заинтересованы в использовании программных систем обеспечения безопасности, которые предоставляли бы наивысший уровень безопасности и сохранения тайны. Фактическим стандартом безопасности для систем электронной коммерции стал протокол SSL 3.0, поскольку он обеспечивает аутентификацию, конфиденциальность и сохранение целостности сообщений.

Компании электронной коммерции принимают электронную почту, пересылают данные и загружают файлы, причем все эти операции сопряжены с риском вирусных атак. Антивирусная защита компании в таких условиях должна включать сканирование загружаемой информации, включая архивы и сообщения электронной почты, и сканирование и очистку от компьютерных вирусов всех устройств памяти.

При электронных сделках-продажах покупатели должны:

- сравнить уровень цен и разнообразие выбора товаров на различных площадках;

- выяснить предоставляемые площадками гарантии качества товаров и надежности продавцов;

- ознакомиться с предоставляемыми услугами по привлечению финансирования и организации логистики.

Для успешности электронной торговли через Интернет продавцы должны:

- сравнить размер комиссионных, взимаемых различными площадками, и комиссию традиционных дистрибьюторов;

- определить, обеспечивает ли выбранная площадка плотность покупательского потока, необходимую для того, чтобы окупить уплачиваемый комиссионный сбор;

- выяснить, как будет организована онлайновая презентация их торговой марки;

- подготовиться к возможности конфликта между новым и традиционным каналом сбыта таким образом, чтобы этот конфликт не помешал переводу части сбыта на электронный рынок, если этого желают определенные круги покупателей;

- учесть вероятность возникновения технологических проблем при интеграции серверных систем с торговыми площадками.

Покупатели и продавцы должны:

- определить, позволяет ли торговая площадка сохранить существующие межфирменные связи, например, сможет ли участник иметь дело с конкретным партнером, которого он предпочитает;

- узнать, насколько эффективна система идентификации недобросовестных участников.

1. **Платежи в Интернете**
   1. **Системы цифровых наличных**

Принцип работы

Первой системой цифровых наличных принято считать ecash (www.diqicash.com), созданную на основе «подписи вслепую», предложенной голландским криптографом Дэвидом Чомом. На российском и украинском рынках представлены две работающие системы цифровых наличных - WebMoney (www.webmoney.ru) и PayCash (www.paycash.ru).

В системе цифровых наличных обращаются цифровые сертификаты на предъявителя, т. е. финансовые обязательства эмитента (банка) по отношению к пользователю системы. Любой пользователь системы может как получать, так и передавать сертификаты другому пользователю, т. е. отсутствует деление пользователей на продавцов и покупателей. В такой системе имеет место математически доказанное отсутствие возможности в рамках системы установить соответствие между платежом и его источником. Эмитент не может отказаться от своих обязательств отдельному плательщику. После перевода средств в цифровую форму их невозможно изъять из обращения без знания секретных ключей пользователя.

Системы цифровых наличных разделяются на 2 класса:

*- Онлайновые.*

Магазин получает деньги после проверки банком, что цифровые сертификаты используются для платежа первый раз.

*- Оффлайновые.*

Магазин получает деньги сразу после получения сертификатов от покупателя и проверки подписи банка под ними. При этом цепочка платежей без предъявления сертификатов банку может быть достаточно длинной.

* 1. **Технология «слепой подписи»**

Для обеспечения анонимности участников сделки с цифровыми сертификатами используется «подпись вслепую» со следующим алгоритмом:

- Пользователь генерирует случайное число А и «ослепляет» его специальной криптографической функцией, параметр которой КФ известен только ему, и получает число А\*. Не зная КФ, невозможно получить А из А\* за приемлемое время;

- Пользователь подключается к банку, идентифицирует себя и передает банку число А\*. Банк подписывает ослепленное число А\* и передает пользователю подпись П\*. Одновременно с банковского счета пользователя списываются средства, равные номиналу монеты и комиссионных за банковскую операцию;

- Пользователь делает «зрячей» подпись П\* с помощью КФ и получает подпись П числа А. Пара (АП) становится цифровой монетой, а ее номинал определяется ключом, которым она было подписана.

* 1. **Платежные системы**

Пользователь может производить платежи и через своего доверенного субъекта - оператора платежной системы (рис. 1), например, надежный банк или положительно зарекомендовавшую себя Интернер-компанию. Чаще всего после формирования корзины заказов пользователя перенаправляют с Web-сайта магазина на Web-сайт платежной системы, где он может подтвердить или отвергнуть заказ. В некоторых системах пользователю предлагают подписать электронный документ, содержащий описание заказа, и передать его магазину; после этого магазин передает этот документ оператору платежной системы, который осуществляет платеж.

Существует 4 класса программного обеспечения, использующего протокол SET:

- цифровой кошелек;

- ПО Интернет-магазина;

- ПО сопряжения с сетями карточных операторов;

- ПО сертификации.

Все используемое ПО должно соответствовать спецификации SET (SET Specification) и пройти процедуру сертификации (www.setco.org). На этом сайте имеется список ПО, соответствующего спецификации SET, и матрица совместимости различных продуктов.



Рис. 1. Сайт платежной системы PayCash

Протокол SET (Secure Electronic Transaction) (www.visa.com/SET), обеспечивающий криптографическую защиту данных пластиковой карточки при платежах через Интернет, имеет следующие особенности:

- использует цифровые сертификаты для идентификации всех сторон сделки;

- не зависит от платежной сети;

- позволяет передавать данные для авторизации непосредственно банку-эмитенту карточки без разглашения финансовой информации;

- является полностью открытым.

Выполнение покупок и платежей по протоколу SET выполняется следующим образом. Покупатель открывает карточный счет в банке и устанавливает на своем компьютере ПО «цифровой кошелек». Кроме того, он получает цифровой сертификат у своего банка, у которого должен быть сертификат от оператора сети (например, VISA). При совершении покупки покупатель подключается к Web-сайту продавца и выбирает необходимый товар. После этого продавец передает «кошельку» покупателя счет, подписанный своим закрытым ключом вместе с цифровым сертификатом, соответствующим ключу. Покупатель проверяет подпись подсчетом, соглашается оплатить заказ и высылает цифровой чек продавцу. В цифровом чеке, кроме параметров заказа, передается информация о пластиковой карточке покупателя, зашифрованная на открытом ключе банка покупателя. Магазин передает чек своему банку, а тот в свою очередь передает чек банку покупателя. После этого банк покупателя авторизует платеж. Результат авторизации передается по цепочке обратно магазину, и он отпускает товар покупателю.

Ниже приведены Интернет-адреса некоторых платежных систем:

- CyberPlat (www.cyberplat.ru)

- E-cash (www.digicash.com)

- InterRussia (www.lnterRussia.com)

- Mondex (www, mondex. com)

- PayCash (www.paycash.ru)

- Russian Shopping Club (www.RussianShopping.com)

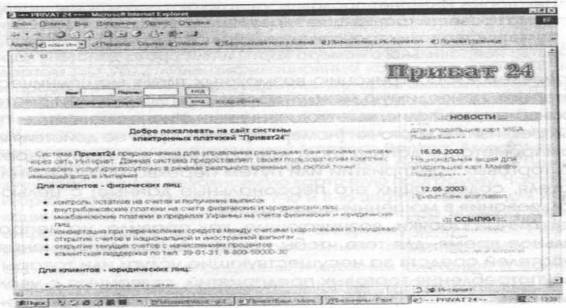
- АССИСТ (www.assist.ru)

- ЭлИТ (www.imbs.com/protokol.htm)

* 1. **Интернет-банкинг**

Основное назначение Интернет - банкинга заключается в управлении текущим счетом клиента через Интернет (рис. 2). С его помощью можно осуществлять покупки в Интернете. Для этого Интернет-магазин должен указать ссылку на сервер Интернет-банка, при переходе по которой клиентскому ПО Интернет-банка передаются реквизиты магазина и сумма платежа. Если клиент согласен с выставленным ему счетом, он производит платеж через Интернет-банк. Далее деньги переводятся на лицевой счет магазина по обычным банковским каналам.

Рис. 2. Реализация Интернет- банкинга на примере украинского банка



1. **Безопасность электронной коммерции**

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

Масштабы мошенничества

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

По данным консалтинговой компании Meridien Research, например, только в 2000 году сумма похищенных через Интернет средств достигла $1,6 млрд. Больше всего от электронных краж пострадали Соединенные Штаты. По прогнозам той же компании, если ситуация с безопасностью в электронной коммерции не поменяется кардинальным образом, в 2005 году объем потерь уже составлял 15,5 млрд. долларов.

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

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

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

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

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

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

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

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

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

Достаточно распространенным является способ, когда криминальные структуры организуют свои магазины и торговые агенты с главной целью получить в свое распоряжение значительные наборы реквизитов карт. Часто такие магазины представляют собой различного рода порносайты.

Второй тип мошенничества - компрометация персональных данных владельцев пластиковых карт - связан со взломом баз данных. Так только в последние несколько лет наиболее громкими «делами» стали кража в Уэльсе двумя подростками 26 ООО реквизитов карт из баз данных одного из электронных магазинов, российским хакером была вскрыта база даннх объемом 300 ООО записей, кража реквизитов 485 ООО карт, выставленных в сети National Aeronautic & Space Administration.

Поданным компании Meridien Research, уязвимость Интернет - магазинов усугубляется еще и тем, что лишь 30% онлайновых продавцов используют надежные системы защиты для борьбы с компьютерными мошенниками.

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

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

Когда же база данных о карточках незначительная, то транзакции выполняются на крупные суммы.

1. **Что такое номер карты**

Это число, состоящее из 16 десятичных цифр (в соответствии со стандартом ISO 7812 «Идентификационные карты - система нумерации и процедура регистрации идентификаторов эмитентов» номер карты может состоять из 19 цифр). 6 первых цифр представляют собой BIN (Bank Identification Number), предоставляемый банку либо международной платежной системой, участником которой он является, либо непосредственно организацией American Bankers' Association, уполномоченной ISO на выдачу идентификаторов банкам, если банк реализует собственную независимую карточную программу. Часто крупные и средние банки используют 7-ю и 8-ю цифры номера для идентификации своих филиалов и отделений. 9-я цифра номера карты - это цифра проверки на четность по алгоритму Luhn Check Parity, однозначно определяемая всеми остальными цифрами номера карты. Остальные цифры определены платежной системой и банком-эмитентом. Эти цифры не являются конфиденциальными, хотя бы потому, что содержатся в множестве различных таблиц, доступных широкому кругу специалистов.

Иногда, кроме номера карты и срока ее действия требуется дополнительно сообщить торговому предприятию специальный цифровой код, называемый в системе VISA CVV2, а в системах Europay/Master-Card - CVC2. Этот цифровой код состоит из трех десятичных цифр, которые печатаются методом индент-печати на оборотной стороне карты на панели подписи сразу вслед за номером карты, и получается с помощью специального открытого алгоритма, применяемого к таким параметрам карты, как номер карты и срок ее действия. Алгоритм базируется на применении алгоритма шифрования DES и использует пару секретных ключей, известных только эмитенту карты. Таким образом, зная номер карты и срок ее действия, вычислить цифровой код без знания секретных ключей невозможно. С 15 мая 2001 г. система VISA предлагает банкам на опционной основе внедрить специальные изменения в авторизационных запросах обслуживающего банка с целью поддержки метода AVS (VISA International Address Verification System).

1. **Новая концепция электронной коммерции от Accenture**

Специалисты лаборатории Accenture (Франция) «вживляют» в различные предметы датчики и радиопередатчики, обеспечивающие обмен информацией друг с другом (концепция торговли «object-to-object» (предмет - предмет)). Предполагается, что через несколько лет именно они будут совершать коммерческие транзакции, а не люди. Эта технология позволит перейти от продажи товаров к продаже услуг: будут платить не за саму вещь, а только за ее использование. Среди опытных образцов, - кукла Барби, которая может сама подбирать и покупать себе одежду в зависимости от программы предпочтений, заданной ей владельцем. На самом же деле, спектр возможностей этой технологии достаточно широк, начиная от заказа и покупки «умным» автомобилем своих запасных частей по мере их износа, и заканчивая «умными» складами, которые смогут заказывать товары по мере их распродажи, реагируя, таким образом, на колебания спроса.

Accenture уже использовала новую технологию для обьединения мобильного телефона и торгового автомата. Суть этого объединения заключается в том, что торговый автомат соединяется с телефоном и выдает список товаров, имеющихся в наличии. Покупатель выбирает товар, и автомат подключается к Интернету и через платежную систему осуществлял покупку.

1. **Отечественный В2В**

Сегодня наибольший рост показателей наблюдается в секторе «бизнес-бизнес» (В2В) и будет продолжаться в отраслях, ориентированных на экспорт. Это прежде всего такие сырьевые отрасли, как металлургия и химическая промышленность.

Для промышленных предприятий среднего масштаба, ориентированных прежде всего на внутренний рынок, развитие в области Интернет может осуществляться в трех основных направлениях:

- работа с клиентами;

- работа с поставщиками и партнерами;

- реализация маркетинговой стратегии, реклама, продвижение брэнда и т. д.

Последний пункт является информационным и не накладывает на предприятие каких-либо серьезных ограничений или требований к инфраструктуре, внутренним информационным системам и т. д. По большому счету все, зависит от фантазии руководства и бюджета на рекламу и маркетинг.

Развитие первых двух направлений в настоящее время весьма проблематично ввиду наличия ограничений: внутренних и внешних.

К внутренним ограничениям относится отсутствие на большинстве предприятий управленческих информационных систем. При этом речь идет не обязательно об интегрированных системах типа управления и планирования ресурсов (ERP- систем), но и об элементарных пакетных решениях для отдельных функций.

Так, например, предоставление клиенту информации о статусе его заказа в онлайном режиме является одной из основных услуг, предоставляемых через Интернет. Однако, если на предприятии отсутствует система отслеживания заказов, то есть информации о статусе заказа просто нет, ни о каком «онлайне» не может быть и речи.

Внутреннее ограничение заключается и в том, что многие бизнес процессы, которые применяются на Западе в Интернете и связаны с обслуживанием клиентов или с закупками, на украинских предприятиях не оптимизированы. Поэтому простая их реорганизация по сравнению с «интернетизацей» принесет много больше прибыли при меньших затратах. Кроме того, перенос процесса в Интернет часто подразумевает почти полную автоматизацию, что на наших предприятиях сделать сейчас почти невозможно.

К внешним ограничениям относится общая неразвитость рынка Интернет в Украине, особенно в регионах, отсутствие надежных платежных систем и распространение бартера.

Что же касается факторов, обеспечивающих эффективность Интернет-закупок, то это прежде всего возможность выбора наилучшего варианта поставок, часто путем организации тендера в Интернете. Но и здесь не все хорошо: в нашей стране такие факторы, как цена и срок поставки, не являются доминирующими, гораздо важнее личные связи и опыт работы с поставщиком.

**Заключение**

В процессе выполнения контрольной работы мы ознакомились с принципами, основными этапами и видами интернет - коммерции, осуществления электронных платежей и способами защиты электронной коммерции.

**Список использованных электронных ресурсов**

www.aup.ru

www.iis.ru

www.bizcom.ru

www.infocity.kiev.ua

www.bizon.ru

www.interface.ru

www.botik.ru

www.iteam.ru

www.ccc.ru

www. internetbook. ru

www.ci.ru

www.isuct.ru

www.citforum.ru

www.ixbt.com

www.comin.org.ua

www.management.com.ua

www.computer.library.ru

www.markbook.chat.ru

www.dis.ru

www.marketing-mix.ru

www.docflow.ru

www.marketing.spb.ru

www.erp.ru

www.mka.ru

www.eup.ru

www.oborot.ru

www.fiber-optica.ru

www.osp.ru

www.hpc.ru

www. plcsystems. kiev.ua

www.hrm.ru

www.projectmanagement.ru

www.hub.ru

www.promo.ru

www.i2r.ru

www.rusdoc.ru

www.ibo.ru

www.web-support.ru