

Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ
Кафедра Защиты информации

Храйба Мохаммед, Азиз

**МОДЕЛЬ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ
ПРЕДПРИЯТИЙ ТОРГОВЛИ**

АВТОРЕФЕРАТА

на соискание степени магистра технических наук
по специальности Методы и системы защиты
информации, информационная безопасность

Научный руководитель

Вишняков В. А. – д-р. техн. наук, профессор

Минск 2015

Общая характеристика работы

Актуальность темы исследования. Информационная безопасность приобрела большое значение, особенно в системах электронной коммерции, поэтому тема исследований является актуальной.

Связь работы с крупными научными программами и темами. Диссертационное исследование выполнялось в рамках НИР «Модели и средства информационного управления и электронного маркетинга предприятия» № ГР 20115472 от 22.12.2011.

Цели и задачи исследования. Цель магистерской работы – исследовать методы и средства информационной безопасности в системах электронной коммерции (ЭК).

Для достижения поставленной цели необходимо решить следующие взаимосвязанные задачи:

- провести анализ информационных средств реализации объектов электронной коммерции;
- представить анализ моделей и средств защиты в системах ЭК;
- представить программную реализацию защиты в электронном магазине.

Объект и предмет исследования. Объектом исследования является методы и средства защиты информации в системах ЭК.

Предметом исследования выступает защита информации в системах ЭК.

Основные положения исследования, выносимые на защиту:

1. Анализ методов и средств защиты информации в системах ЭК.
2. Представлен анализ моделей и средств защиты информации в системах электронной коммерции
3. Представлена программная реализация защиты информации в электронном магазине.

Апробация результатов исследования. Основные положения данной работы представлялись на XII и XIII Белорусско-российских НТК «Технические средства защиты информации» в 2014 и 2015 гг.

Опубликованность результатов. По результатам выполненных исследований опубликовано 2 научные работы (тезисы докладов). В том числе 2 – в материалах научных конференций.

Структура и объем диссертации. Структурными частями диссертации являются: введение, общая характеристика работы, три главы, заключение, библиографический список, состоящий из 15 наименований, приложения. Работа изложена на 69 страницах и включает в себя 15 рисунков, 5 таблиц.

Введение

В магистерской диссертации освещены вопросы, связанные с электронным бизнесом, электронной коммерцией (ЭК), интернет-магазинами, технологией электронной торговли и организации защиты информации в системах ЭК.

Электронная коммерция занимает долю ВВП, объем которого в мировой экономике быстро растет. Например, фирмы IBM, Cisco имеют месячный оборот более 1,3 млрд долларов от использования электронных продаж. Объем мирового рынка электронной коммерции по итогам 2014 года впервые превысил порог в 1,1 трлн. долларов, [сообщает](#) eMarketer. А уже в 2015 году этот показатель увеличится до 1,3 трлн., прогнозируют аналитики [11].

В Республике Беларусь электронная коммерция также быстро развивается. В планах по развитию информационных технологий (ИТ) на 2011–2015 гг. предусмотрено увеличение средств электронной коммерции на 30 % [11].

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В первом главе:

электронной коммерции

Электронная коммерция -это система продажи товаров в интернете . можно сказать, что он начал с продажи продукции бросать электронной почты в 1971 году. Позволяет обмениваться информацией между продавцом и клиентом ,следующим важным шагом было сделать ТСП/IP-протокол и доменное грива , которая упростила работу между офисом и складом в электронной коммерции мира, и дать клиенту возможность выбрать продукцию непосредственно с сайта

сетевой экономики

Понятие сетевой экономики возникло в условиях использования различных информационных сетей. Можно, классифицировать информационные сети по уровню интеграции следующим образом:

- корпоративные сети (интранет).
- сети делового партнерства (экстранет).
- глобальные сети (например, интернет).

сетевой экономики определена следующим образом:

Сетевая экономика = Традиционная экономика + Информационные ресурсы и технологии

Продукция сетевой эконмики

В общем случае под продуктом понимается объект, имеющий вещественную форму и способный удовлетворять те или иные потребности. Продукт получается из исходного сырья или материалов путем применения тех или иных технологий. При этом свойства исходного материала исчезают, а продукт приобретает самостоятельную потребительскую ценность. Классификация продукции в сетевой экономике в целом и ее состав в укрупненном виде представлены на рисунке.

электронны бизнеса

Электронные аукционы: Интернет сделал аукцион более демократичным, позволив каждому, у кого есть доступ в глобальную сеть, торговаться за любые выставляемые на торги предметы.

Электронные банки банковское дело в интернете — одно из самых процветающих электронных начинаний. Электронный банк позволяет клиентам получать доступ к их счетам и осуществлять различные финансовые операции с помощью простого в использовании веб-сайта.

Электронная коммерция: Магазин в интернете не ограничен в пространстве и времени. Ассортимент товаров, которые предлагает магазин, также неограничен. Например, Amazon.com предлагает свыше 4,7 миллионов книг

Электронные магазины

Виды интернет-магазинов в зависимости от видов продаж:

1. 1. Продажи на потребительском рынке (B2C): продажи на потребительском рынке. Клиенты компании по данному направлению продаж - физические лица со всеми процедурами, принятыми гражданским кодексом для осуществления продаж физическим лицам.
2. 2. Продажи на корпоративном рынке (B2B): продажи на корпоративном рынке. Вы работаете в секторе B2B, если ваши клиенты — юридические лица со всеми процедурами, принятыми Гражданским кодексом для взаимодействия между юридическими лицами. К этому сектору также относятся компании, которые работают с потребителями через посредников – дилеров.

Виды интернет-магазинов в зависимости от представляемых товаров в каталоге

3. Интернет-витрина: он представляет собой логическое расширение обычного web-сайта, когда на него просто выкладывается вся необходимая информация о товарах, которая по мере надобности обновляется.
4. Торговый автомат: в отличие от интернет-витрины, осуществляет реальную торговлю. Система ведения торговых операций некоторым образом интегрирована с бизнес-процессами организации.
5. . Автоматический магазин: в общем случае позволяет в автоматическом режиме принимать заказ, выписывать счет, принимать платеж, а также формировать заявку на доставку товара покупателю.

Недостатки интернет-магазинов

- Нет возможности рассмотреть выбранный товар
- Нет возможности получить консультацию продавца
- Недостаточная отлаженная процедура доставки товара
- Нет возможности получить выбранный товар немедленно

Преимущества интернет-магазинов

- Широкий ассортимент,
- Низкие цены.
- Совершение покупок в удобное время
- Информация о надежности продавца.

Во второй главе

Классификация угроз безопасности информации

Известно большое количество разноплановых угроз безопасности информации различного происхождения. В качестве критериев деления множества угроз на классы могут использоваться виды порождаемых опасностей, степень злого умысла, источники проявления угроз и т.д. Все многообразие существующих классификаций может быть сведено к некоторой системной классификации: методы обеспечения безопасности

Шифрование

В основе шифрования — два понятия: алгоритм и ключ. Криптографический алгоритм — математическая функция, которая комбинирует открытый текст или другую понятную информацию с цепочкой чисел, называемых ключом, для того чтобы в результате получился бессвязный зашифрованный текст. Алгоритм и ключ — основа процесса шифрования.

основные криптографические алгоритмы

- симметричного алгоритма
- асимметричные алгоритма

Аппаратные и программные брандмауэры

Брандмауэр – это система, которая предотвращает несанкционированный доступ к сети и из сети. На персональных компьютерах брандмауэр чаще всего является программой, которая работает в фоновом режиме и тщательно проверяет все входящие и исходящие данные. В больших сетях, таких как локальные домашние сети или корпоративные сети, могут использоваться аппаратные брандмауэры.

Функции брандмауэра заключаются в сканировании всей информации, проходящей через него, и применение к ней набора установленных правил. Эти правила в простейшем виде могут быть представлены белым и черным списком.

В третьей главе

при разработке онлайн магазина мы использовали следующие методы для защиты нашей сайте

Методы Шифрование

Использован алгоритм MD5 и кэш для хранения паролей, MD5 – это алгоритм, который, использует в качестве входных данных сообщение произвольной длины и выдает на выходе 128-битовое значение. Вводимые данные последовательно разбиваются на блоки по 512 бит.

```
public function hash($data) {
```

```
return md5($data);
```

```
}
```

Брандмауэр

создает дополнительный слой безопасности по всему Интернет-магазину. С помощью правила брандмауэра, он будет блокировать нападавших или вносить их

в черные списки и запрещать им доступ к сайту. Он имеет сканер для предоставления рекомендации о установке в нашем магазине.

Защищенный протокол

Secure Sockets Layer (SSL) используя протокол защищенных Сокетов (SSL) с ключом шифрования длиной 128-бит (самый высокий уровень, имеющихся в продаже).

Онлайн-транзакции

Онлайн-транзакции состоит из двух частей: продукты и платежи. Подсистема zorbashop.com, вместе с системой PayPal, делает то же самое для электронных платежей. PayPal помогает увеличить продажи, снизить риски и обеспечить лучшее обслуживание клиентов. Интеграции являются простыми, безопасными и легко подключиться к хранилищу данных.

Заключение

1. Электронный бизнес – преобразование бизнес процессов на основе Интернет-технологий, включающий основные составляющие: e-commerce, m-commerce, e-work, e-banking, e-trading, e-education, e-marketing, e-management, e-gavement и т. д. Электронная коммерция — любая сделка, совершенная посредством сетей, по завершении которой происходит передача права собственности или права пользования вещественными товарами или услугами. Выделяют 9 направлений ЭК во взаимоотношениях бизнеса – В, потребителя – С и администрации – А.; основные из них В2В, В2С, В2А, С2С.

2. К достоинствам электронной коммерции относятся круглосуточный режим работы, расширение рынков сбыта, меньшие затраты на рекламу и создание инфраструктуры, доступность из любой точки мира, меньшая себестоимость, большие маркетинговые возможности и т. д. К недостаткам электронной коммерции относятся: долгий процесс поиска самой дешевой модели; не всегда Интернет-магазины предоставляют самый удобный вариант оплаты; при неправильной организации навигации пользователь может запутаться в информации по сайту магазина.

3. Средства защиты в СЭК. Шифрование данных, препятствующее их прочтению или искажению; проверка подлинности отправителя и получателя осуществляется технологией цифровой подписи, фильтрация трафика, поступающего в сеть или на сервер защищается брэндмауэрами. Криптографические технологии обеспечивают три основных типа услуг для электронной коммерции: аутентификацию (которая включает идентификацию), невозможность отказа от совершенного и сохранение тайны.

4. Модели защиты – 2 вида шифрования. Симметричное шифрование, или шифрование с секретным ключом. При шифровании по такой схеме отправитель и получатель владеют одним и тем же секретным ключом, с помощью которого и тот, и другой могут зашифровывать и расшифровывать информацию. Асимметричное шифрование. Одна часть ключевой пары – личный ключ, известна только ее владельцу. Другая половина – открытый ключ, распространяется среди всех его корреспондентов, но связана только с этим владельцем. зашифрованные любым из ключей пары, могут быть расшифрованы только другим ключом из этой пары

5. Технология ЦП. При помощи хеш-функции получается дайджест – уникальным образом сжатый вариант исходного текста. Дайджест шифруется с помощью личного ключа и превращается в цифровую подпись, которая посылается вместе с самим сообщением. Получив послание, получатель расшифровывает цифровую подпись с помощью открытого ключа, и извлекает дайджест сообщения, применяя для сообщения ту же хэш-функцию он получает свой сжатый вариант текста и сравнивает его с дайджестом, восстановленным из подписи. Если они совпадают, то это значит, что подпись правильная.

6. Представлены используемые методы защиты информации в онлайн-магазине (zorbashop.com). Выделены следующие направления защиты: метод шифрования с цифровой подписью, использование брандмауэра, защищенный протокол Secure Sockets Layer (SSL), разрешение доступа. Использован алгоритм MD5 и кэш для хранения паролей, MD5 – это алгоритм, который, использует в качестве входных данных сообщение произвольной длины и выдает на выходе 128-битовое значение. Вводимые данные последовательно разбиваются на блоки по 512 бит.

Библиографический список

Список использованных источников

1. Балабанов, И.Т. Электронная коммерция / И.Т. Балабанов. – СПб: Питер, 2008. – 336 с.
2. Васильев В.И. Интеллектуальные системы защиты информации / В.И. Васильев. – М.: Машиностроение, 2013. – 172 с.
3. Вишняков, В.А. Электронный бизнес и коммерция: УМК / В.А. Вишняков, Ю.В. Бородаенко. – Минск, МИУ, 2010. – 186 с.
4. Вишняков, В.А. Основы электронной коммерции. Учеб. пособие с грифом МО РБ. Минск: Бестпринт. 2014. – 265 с.
5. Войтович, А.И. Электронная торговля: Курс лекций / А.И. Войтович. – Мн.: Академия управления при Президенте Республики Беларусь, 2005. – 117 с.
6. Климченя, Л.С. Электронная коммерция: Учеб. Пособие / Л.С. Климченя. – Мн.: Выш. шк., 2004. – 191 с.
7. Козье, Д. Электронная коммерция: Пер. с англ. / Д. Козье. – Москва: Издательско-торговый дом «Русская Редакция», 2008. – 288 с.
8. Панышин, Б.Н. Курс лекций «Электронная торговля: теория и практика» / Б.Н. Панышин. – Минск: БГУ 2008. – 450 с.
9. Старовойтова, Т.Ф. Электронный бизнес и коммерция / Т.Ф. Старовойтова. – М.: ТетраСистемс, 2006. – 304 с.
10. Цуканова О.А. Сетевая экономика: Учебное пособие. / О.А. Цуканова, А.В. Варзунов. – СПб.: ГУИТМО, 2008. – 64 с.
11. Интернет в цифрах. Мировая статистика за 2012 [Электронный ресурс]. – Режим доступа: [http://www. Adindex.ru](http://www.Adindex.ru). Дата доступа: 11 октября 2013.
12. Интернет-магазин amazon.com – [Электронный ресурс].– Режим доступа: <http://www. amazon.com>. Дата доступа: 11 октября 2013.
13. Интернет-магазин ebay.com [Электронный ресурс]. – 11 октября 2013. – Режим доступа: <http://www. eBuy.com>
14. Электронная безопасность. [Электронный ресурс]. – 11 октября 2013. – Режим доступа: <http://www. www.firebox.ru>
15. Stalling, W. Bussiness Data Communications. / W. Stalling, R.V. Styke Prentise Hall Int. 2008. – pp.558.

16. Актуальные тенденции: средства сетевой защиты. [Электронный ресурс]. – 10 января 2014. – Режим доступа: <http://www.firebox.ru>

17. Таненбаум Э. Компьютерные сети / Э.Таненбаум, Д.Уэзеролл. – СПб.: Питер, 2012. – 960 с.

Список публикаций соискателя

1-А. Вишняков, В.А. Обзор и анализ средств защиты информации в электронной коммерции / В.А. Вишняков, Храйба Мохаммед // Тез. докладов XII Белорусско-российской НТК «Технические средства защиты информации». Минск: БГУИР, 2014. – С. 24.

2-А. Вишняков, В.А. Анализ методов защиты информации в онлайн-магазине zorbashop.com / В.А. Вишняков, Храйба Мохаммед // Тез. докладов XIII Белорусско-российской НТК «Технические средства защиты информации». Минск: БГУИР, 2015. – С.100.