Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.53

Мазуро
Андрей Павлович

Модель и средства защиты электронного магазина

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-40 80 02 "Системный анализ, управление
и обработка информации"

Научный руководитель
Шавель Александр Николаевич
доцент каф. ТД БНТУ, к.ф.-м.н., доцент

Минск 2020

ВВЕДЕНИЕ

Быстрое развитие информационных технологий и глобальной сети Интернет привели к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности.

Одним из основных инструментов управления бизнесом являются информационные системы.

Компании сталкиваются с огромным количеством различных угроз для информационной инфраструктуры. В качестве примера можно привести несанкционированный доступ, заражение вирусами. Таким образом, можно сделать вывод, что необходимо уделять внимание к информационной защите данных. Поэтому применение информационных технологий немыслимо без повышенного внимания к вопросам информационной безопасности.

Доступ к информации, являющейся «коммерческой тайной» компании, должен быть ограничен, т.к. несанкционированное использование этих данных может быть причиной вторжений сторонних участников рынка – конкурентов.

В связи с этим данная диссертация посвящена разработке информационной защиты локальной вычислительной сети на примере интернет-магазина.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность

Бурное развитие средств вычислительной техники открыло перед человечеством небывалые возможности по автоматизации умственного труда и привело к созданию большого числа разного рода автоматизированных информационных и управляющих систем, к возникновению принципиально новых, так называемых, информационных технологий.

Неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляюших системах наносят серьезный материальный и моральный урон многим субъектам (государству, юридическим и физическим лицам), участвующим в процессах автоматизированного информационного взаимодействия.

Жизненно важные интересы этих субъектов, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их экономических, политических и других сторон деятельности, конфиденциальная коммерческая и персональная информация, была бы постоянно легко доступна и в то же время надежно защищена от неправомерного ее использования: нежелательного разглашения, фальсификации, незаконного тиражирования, блокирования или уничтожения.

Цели и задачи исследования

Целью диссертационной работы является разработка модели защиты безопасности интернет-магазина.

Модель защита должна выполнять следующие функции:

1. Защита информации от угроз внешних нарушителей за счет шифрования исходящего трафика из ЛВС организации
2. Противодействие техническим средствам промышленного шпионажа
3. Защита информации от угроз внутренних нарушителей (инсайдеров)

Методы исследования

В ходе диссертации была изучена предметная область, проведены работы по пред проектному исследованию деятельности коммерческой фирмы. Анализ деятельности фирмы позволил определить необходимость в наличии процессов, нуждающихся в защите.

Опубликованные результаты

По теме диссертационной работы опубликована 1 печатная статья в научном журнале.

Структура и объем диссертации

Диссертация изложена на 87 страницах. Она состоит из введения (2 стр.), постановки задачи и определения концептуальной модели (16 стр.), исследования вопроса сетевой безопасности (22 стр.), практической реализации (24 стр.) и заключения (1 стр.). Работа содержит 14 иллюстраций, 10 таблиц а также список использованных источников.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первой главе была рассмотрена структура склада интернет - магазина, изучены возможные операции проходящие внутри организации. Также был произведен детальный анализ предметной области. В этой главе уделено много внимание таким понятиям как “модель нарушителя” и “факторы риска”. На основе анализа был сделан следующий вывод: минимизация рис-ков может быть достигнута путем подхода к вопросу с помощью комплексного решения, т. е. за счет использования программных, аппаратных и регламентирующих средств.

Вторая глава была посвящена вопросу сетевой безопасности и шифрования. Были проанализированы классификации угроз и возможные методы шифрования данных. Безопасная информационная система обладает следующими свойствами: конфиденциальность, доступности и целостность. Были выявлены основные направления защиты: защита данных в момент их передачи по линиям связи и защита от несанкционированного удаленного доступа в сеть. Установлены наиболее популярные стандарты: симметричным алгоритмом шифрования является DES, а из несимметричных криптоалгоритмов с открытым ключом — RSA.

В результате был сформирован следующий набор инструментов для обеспечения информационной безопасности: в качестве средства построения VPn канала был выбран криптомаршрутизатор «КриптоМ-2», в качестве средств защиты информации от НСД было выбрано комплексное решение, такое как СЗИ Sekret Net + АПМДЗ «Соболь» и был определен вариант установки и размещения оборудования и средств защиты информации от утечки по техническим каналам в трех этажном здании с оборудованным цокольным (подвальным) этажом. Весь этот набор имеет под собой также и экономическое обоснование приведенной в четвертой главе.

ЗАКЛЮЧЕНИЕ

Информационная безопасность - большая и очень важная проблема в современном мире. В результате выполнения диссертации была разработана модель информационной защиты интернет-магазина с использованием аппаратных, программных и регламентирующих средств.

В ходе диссертации была изучена предметная область, проведены работы по пред проектному исследованию деятельности коммерческой фирмы. Анализ деятельности фирмы позволил определить необходимость в наличии процессов, нуждающихся в защите.

Разработанная система обеспечивает выполнение определенных нами функций, таких как:

1. Защита информации от угроз внутренних нарушителей (инсайдеров)

2. Защита информации от угроз внешних нарушителей за счет шифрова- ния исходящего трафика из ЛВС организации

3. Противодействие техническим средствам промышленного шпионажа

Новизна данной работы заключается в том, что модель была разработана с использованием комбинации из аппаратных, программных и регламентирующих средств. Уникальность этой комбинации и составляет научно-прикладную новизну данной диссертации.