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

УДК 004.738.4:004.056

Семак
Александр Дмитриевич

Проектирование политики безопасности корпоративной сети предприятия

АВТОРЕФЕРАТ

на соискание степени магистра техники и технологии

по специальности 1-45 81 01 Инфокоммуникационные системы и сети

Научный руководитель
Селезнев Игорь Львович
к.т.н., доцент

Минск 2018

ВВЕДЕНИЕ

В наше время стремительного развития новых информационных технологий, всеобщей компьютеризации, постоянно обостряющейся конкуренции различных товаропроизводителей все более изощренными становятся методы взлома систем информационной безопасности.

Технические и интеллектуальные методы и средства несанкционированного доступа к информации различной физической природы, различной степени конфиденциальности и секретности, циркулирующей в информационных системах от локального до стратегического уровня, постоянно совершенствуются и становятся изощреннее. В работе применяется системный подход к проблеме анализа и синтеза технических средств и методов защиты информации от несанкционированного доступа.

Современная концепция безопасности, действующая в рамках эффективного управления любой современной организацией, оперирует в подавляющем большинстве случаев с автоматизированными информационными системами, т.е. с такими комплексами, каждый из которых включает в себя компьютерное и коммуникационное оборудование, программное обеспечение, диагностические средства, информационные ресурсы, а также системный персонал.

Под безопасностью информационной системы подразумевается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения ее компонентов, высокий уровень противостояния данной информационной системы различным возмущающим воздействиям.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Цель диссертационной работы заключается в разработке политики безопасности сети предприятия, обеспечении уровня безопасности, соответствующего нормативным документам.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1 Сформировать критерии для разработки политики безопасности сети предприятия.

2 Провести анализ основных проблем в безопасности локальной вычислительной сети

3 Проанализировать основные типы сетевых атак, их воздействие на сеть и возможные последствия.

4 Провести анализ методов и средств защиты сети от возможных атак.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 1 работа, в том числе 1 статья в сборниках материалов конференций.

Структура и объем диссертации

Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, трех глав и заключения, и библиографического списка. Общий объем диссертации – 55 страниц, работа содержит 24 рисунка, библиографический список включает 26 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрена проблематика защищенности информационной системы сети предприятия. Рассмотрено понятие информация с точки зрения ее характера, степени конфиденциальности. Показана значимость информационной безопасности как одной из важнейших характеристик информационной системы.

В **общей характеристике работы** сформулированы цель и задачи исследования, показана связь с современными задачами в области сетевой безопасности.

В первой главе рассматриваются основные положения информационной безопасности, виды сетевых атак, способы и методы противодействия несанкционированному доступу. Приведены основные задачи информационной безопасности, ее составляющие, а также некоторые государственные стандарты в области обеспечения безопасности сети. Обусловлена актуальность и важность проблемы обеспечения информационной безопасности.

Во второй главе рассматриваются способы, средства и методы решения задач по обеспечению безопасности сети их достоинства и недостатки. Представлен анализ технологии NAT. Приведен краткий обзор разновидностей межсетевых экранов. Перечислен примерный список инструктивных и нормативных документов, которые рекомендуется разработать на предприятии. Рассмотрен принцип работы таких технологий как аутентификация и авторизация пользователей, а также разграничение прав и доступа пользователей на основе применения групповых политик Active Directory.

В третей главе показана необходимость разработки политики безопасности сети, рассмотрены основные структурные элементы информационной безопасности.

Представлены некоторые аспекты конфигурации оборудования, позволяющие настроить правила взаимодействия сети, которые не будут угрожать безопасной работе сетевой инфраструктуры предприятия. Рассмотрены организационные методы защиты сети предприятия.

ЗАКЛЮЧЕНИЕ

1 Проведена систематизация знаний для понимания особенностей разработки политики безопасности сети. Рассмотрены основные положения информационной безопасности.

2 Предложены технологии защиты сети и информационных систем, нормативные документы, которым необходимо следовать при разработке политики безопасности сети предприятия.

3 Изучены особенности обеспечения сетевой безопасности, основные типы атак, их особенности и область воздействия. Проанализированы возможные меры и комплекс мероприятий для борьбы с данными типами атак.

4 Рассмотрены основные угрозы, которые могут помешать штатной работе сети и ее компонентов.

5 Проведен анализ методов и средств предотвращения несанкционированного доступа к ресурсам предприятия.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Пархомик, С.Ю. Автоматизация и масштабирование локальных вычислительных сетей с использование SDN / С.Ю. Пархомик, А.Д. Семак, И.Л. Селезнев// Алгебраическое кодирование и безопасность данных. – 2017 – С. 56-62.

2-А. Семак, А. Д. Проектирование политики безопасности корпоративной сети предприятия / А. Д. Семак // Телекоммуникационные системы и сети: материалы 53-й научной конференции аспирантов, магистрантов и студентов. – Минск: БГУИР, 2017. – С. 73-74.