

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

УДК 004.056

Сороко
Максим Викторович

Применение протокола IPSec для защиты сети

АВТОРЕФЕРАТ

на соискание степени магистра техники и технологии
по специальности 1-45 81 01 «Инфокоммуникационные системы и сети»

Научный руководитель
Астровский Иван Иванович
канд. техн. наук, доцент

Минск 2019

КРАТКОЕ ВВЕДЕНИЕ

В сегодняшнем мире с постоянно изменяющимися условиями, а также с темпом развития информационных технологий, сложно представить предприятие или организацию, которая не использовала бы в своей деятельности компьютерные информационные сети. Зачастую предприятия малого и среднего бизнеса пренебрегают вопросами, связанными с обеспечением безопасности своих информационных систем. Иногда владельцы компаний думают, что информационные ресурсы не очень ценятся, и, следовательно, компания не является вектором для атаки, но сегодня, когда деятельность киберпреступников возрастает с каждой секундой, любая организация является потенциальной жертвой разного рода атак. Реальность такова, что даже в настоящий момент компании теряют значительную сумму денег и терпят финансовые риски из-за небрежности или недостаточной осведомленности о проблемах безопасности.

В современном мире информационная безопасность является очень важным аспектом ведения любого бизнеса. Чтобы оставаться конкурентоспособным на рынке, организация должна сохранять в тайне свои информационные активы. Сегодня широко распространены разнообразные методы получения информации законными и незаконными средствами. Также с каждым днем на рынке информационных технологий появляются новейшие системы защиты информации.

Анализируя вышесказанные утверждения, можно прийти к выводу, что информационная безопасность является одной из самых актуальных тем не только на сегодняшний день, но будет актуальна и в будущем.

Актуальность данной магистерской диссертации заключается в том, что с помощью использования различных методов, связанных с информационной безопасностью, можно обеспечить защищенность распределенной корпоративной сети.

Объектом исследования работы является корпоративная сеть связи. Предметом исследования диссертационной работы является нахождение методов для построения распределенных защищенных корпоративных сетей.

Целью диссертации является обеспечение информационной безопасности корпоративной сети с помощью стека протоколов IPSec, а также создание обучающей программы по информационной безопасности.

Практическая ценность данного исследования позволяет использовать полученные результаты для обеспечения информационной безопасности корпоративной сети как на практике, так и в учебных целях.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Работа выполнялась по теме: «Применение протокола IPSec для защиты сети».

Проведенная работа по диссертационной тематике соответствует мировым тенденциям в области проектирования защищенных сетей связи. Рассмотренные модели взаимодействия протоколов позволяют осуществить надёжное построение и безопасность сетей связи.

Целью диссертации является обеспечение информационной безопасности корпоративной сети с помощью стека протоколов IPSec, а также создание обучающей программы по информационной безопасности.

Для достижения цели были решены следующие задачи:

- проведен обзор литературы и рассмотрены основные разновидности сетей связи;
- осуществлено исследование и проанализированы разновидности моделей построения защищенных корпоративных сетей;
- исследованы протоколы IP сетей, используемые для защиты и шифрования данных в корпоративных сетях;
- разработана защищенная корпоративная сеть связи с помощью исследуемых методов обеспечения информационной безопасности;
- разработана обучающая программа по информационной безопасности.

Научная новизна темы данной магистерской диссертации заключается в том, что результаты практического применения исследуемых способов, направленных на защиту информации, позволяют доказать их эффективность для обеспечения информационной безопасности.

Основные положения и результаты магистерской работы докладывались и обсуждались на 54–й научной конференции аспирантов, магистрантов и студентов; международном научно–техническом семинаре «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных».

Основные результаты и положения диссертации, выносимые на защиту, разработаны и получены лично автором. Соавтором опубликованных работ являлся научный руководитель кандидат технических наук, доцент И.И. Астровский, вклад которого связан с определением цели и задач исследований, выбором методов исследований, интерпретацией и обобщением результатов.

КРАТКОЕ СОДЕРЖАНИЕ

Во введении рассматривается проблема информационной безопасности в современном мире, обосновывается актуальность выбранной темы диссертационной работы, дается краткая характеристика ее разработанности, определяются объект и предмет исследования.

В общей характеристике работы сформирована цель, научная новизна, практическая ценность данной диссертационной работы, а также основные задачи, используемые для достижения поставленной цели.

Первая глава «Обзор общих сведений о системах передачи данных» включает в себя анализ систем и сетей передачи данных. Первая глава состоит из группы подразделов.

В подразделах первой главы осуществляется анализ основных систем и сетей передачи данных. Рассматриваются и описываются корпоративные сети. В конце даются основные выводы по первой главе.

Вторая глава «Анализ обеспечения безопасности корпоративных сетей» описывает основные средства, предназначенные для обеспечения безопасности корпоративной сети. Вторая глава состоит из группы подразделов.

В подразделах второй главы рассматриваются и описываются известные сетевые атаки: переполнение буфера, использование специализированных программ (вирусов, снифферов, троянских коней, почтовых червей, и т.д.), IP-спуфинг, man-in-the-middle, отказ в обслуживании, phishing-атаки. В конце даются основные выводы по второй главе.

Третья глава «Способы обеспечения безопасности корпоративной сети» включает в себя несколько подразделов, в которых описываются предлагаемые способы обеспечения информационной безопасности распределенной корпоративной сети, протоколы и методы обеспечения шифрования данных и обеспечения аутентификации, доказываются их эффективность для дальнейшего использования. В конце даются основные выводы по третьей главе.

Четвертая глава «Разработка защищенной распределенной корпоративной сети» состоит из нескольких подразделов, в которых осуществляется анализ выбора программных средств. Разрабатывается защищенная корпоративная сеть связи с использованием выбранного программного обеспечения. Разрабатывается обучающая программа тестирования. В конце даются основные выводы по четвертой главе.

ЗАКЛЮЧЕНИЕ

В результате магистерской диссертации сформированы основные выводы, с помощью которых можно существенно обезопасить корпоративную сеть. Рассмотрены самые распространенные сетевые атаки, используя которые злоумышленники могут получить конфиденциальную информацию, дестабилизировать корпоративную сеть организации, внедрить вредоносные программы в сеть и т.п. Проведен выбор программных средств, предназначенных для обеспечения информационной безопасности корпоративной сети. Разработана защищенная распределенная корпоративная сеть, логическая схема которой может быть использована как в учебных целях, так и на практике. Разработана программа тестирования по информационной безопасности, которая может быть использована как для обучения сотрудников организаций, так и для студентов, обучающихся в сфере сетевых технологий и защиты информации.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А Сороко, М.В. Применение протокола IPSEC для защиты сетевого трафика / М.В.Сороко // Инфокоммуникации : материалы 54-й научной конференции аспирантов, магистрантов и студентов, Минск, 23–27 апреля 2018 г. – Минск : БГУИР, 2018. – С. 137.

2–А Сороко, М. В. Система мониторинга безопасности корпоративной сети на основе анализа событий / М. В. Сороко // Инфокоммуникации: 55-я юбилейная конференция аспирантов, магистрантов и студентов, Минск, 22 – 26 апреля 2019 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2019. – С. 13.

3–А I.I.ASTROVSKY, V.S.DANILCHUK, M.V.SOROKO, L.M. AL-RUBAI DEVELOPMENT OF COMPUTER SOFTWARE AND TOOLS FOR ELECTRONIC DOCUMENT MANAGEMENT/ I.I.ASTROVSKY, V.S.DANILCHUK, M.V.SOROKO, L.M. AL-RUBAI // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы международного научно-технического семинара (Минск, ноябрь – декабрь 2018 г.) – Минск : БГУИР, 2018. – С. 83-86.