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

УДК 004.73:004.057.4

Киселёв
Дмитрий Владимирович

Моделирование защищённой территориально-распределённой сети предприятия

АВТОРЕФЕРАТ

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

_____

Научный руководитель
Астровский И. И.
к.т.н., доцент

_____

Минск 2019

КРАТКОЕ ВВЕДЕНИЕ

Безопасность данных – одна из главных задач, решаемых отделами информационных технологий (ИТ-отделами) компаний. Причем речь идет не только о предотвращении утечки корпоративной информации, снижении объемов паразитного трафика и отражении атак на ресурсы компании, но и об оптимизации работы системы в целом.

Найти универсальное решение в данном вопросе практически невозможно: неоднородность сфер деятельности и структур организаций переводит задачу в категорию требующих индивидуального подхода. Однако для грамотных специалистов неразрешимых проблем не существует.

Неоднородность сферы деятельности различных организаций, фирм, банков делает объективно необходимым конкретизацию стратегий защиты информации и управления ими в случае серьезного нарушения или кризиса. Такой подход побуждает разрабатывать различные концепции информационной безопасности в зависимости от размеров организации (малый, средний, крупный), сфер деятельности (финансовая, банковская, производственная, торговая), национальных и региональных особенностей. Анализ информационных рисков включает определение того, что нужно защищать, от кого и как защищаться. Рациональный уровень информационной безопасности выбирается в первую очередь из соображений экономической целесообразности.

Корпорация – это объединение организаций, лиц на основе совместных, профессиональных интересов, одна из форм акционерного общества для крупного бизнеса, в том числе банковского.

Для крупных корпораций характерна сложная, территориально-распределенная структура с многоуровневым и многозвенным построением. Масштабы деятельности и объемы выпускаемой продукции, услуг могут носить как региональный, так и глобальный характер.

Характерной и отличительной особенностью корпоративных вычислительных сетей является то, что их построение осуществляется, как правило, на протяжении нескольких лет. В таких сетях функционирует оборудование разных производителей и разных поколений, то есть. оборудование, как самое современное, так и устаревшее, не всегда изначально ориентированное на совместную работу, передачу и обработку данных. По мере количественного и качественного развития корпоративных сетей задача управления ими все более усложняется, требует новых средств управления сетями в масштабах всего предприятия. Такие средства должны быть независимы от протоколов, масштабируемы и должны обеспечивать централизованное управление сетью.

В настоящее время потребители ищут решения по объединению разрозненных филиалов не только в рамках одной корпорации, но и регионов по стране в целом. Основная цель объединения филиалов – создание единого информационного пространства и единых сервисных функций. Современные решения позволяют предоставить потребителям единую систему управления и контроля (мониторинга) ресурсов корпоративной сети, снижение затрат, объединение сетей передачи данных и телефонии, защиту от несанкционированного доступа.

Безопасность данных – одна из главных задач современных предприятий. Информационный ресурс корпоративного уровня особенно уязвим и требует качественной и надежной защиты, так как информационная структура организаций корпоративного типа разнородна, состоит из набора распределенных систем, технологий, баз и банков данных и локальных задач.

Целью магистерской диссертации является разработка программы моделирования защищённой сети предприятия.

Задачами магистерской диссертации являются:

– анализ методов и средств защиты информации в корпоративной сети;

– разработка территориально-распределённой сети предприятия;

– моделирование работы сети предприятия;

– моделирование способов защиты корпоративной сети.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Работа посвящена теоретическому исследованию протоколов безопасности для передачи данных через публичные сети, изучению технологий туннелирования для безопасного обмена данными в корпоративных сетях.

Для надёжной защиты информации в корпоративных сетях при передаче через публичные сети должны использоваться надёжные и проверенные технические решения. Для достижения качественной защиты необходимо исследовать известные уязвимости корпоративных сетей и, учитывая наиболее опасные и распространённые уязвимости, выбрать и обосновать технологию для построения безопасной корпоративной сети, а также используемые в этой технологии протоколы безопасности.

Актуальность настоящего исследования подтверждается тем, что безопасность данных – это одна из главных задач, решаемых всеми современными отделами информационных технологий компаний.

Развитие корпоративных сетей, то есть сетей, охватывающих несколько удалённых друг от друга офисов, взаимодействующих между собой через

публичные сети, становится одной из самых из современных тенденций. В настоящее время появляется все больше корпоративных сетевых организаций.

Ни одно современное предприятие не обходится без собственных систем и средств защиты информации. В связи с необходимостью обеспечивать конфиденциальность, целостность и доступность информации, а также гарантировать правильное её распределение, возникает потребность в защите информации.

На данный момент существует достаточно много исследований в области зашиты информации в корпоративных сетях, однако, не все методы и средства одинаково подходят для различных корпоративных сетей.

Содержание магистерской работы соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-45 81 01 «Инфокоммуникационные системы и сети».

Информационная база для анализа сформирована на основе данных, полученных из баз данных, распространяемых в свободном доступе в сети интернет.

Научная новизна магистерской работы заключается в том, что были проанализированы уязвимости корпоративных сетей, проанализированы и систематизированы методы и средства защиты информации в соответствии с современными тенденциями. Разработанная классификация выполнена на основе анализа современных работ как зарубежных так и отечественных авторов.

Теоретическая и практическая значимость работы заключается в том, что в ней описаны современные алгоритмы и методы для защиты информации в корпоративных сетях, а также смоделирована защищённая корпоративная сеть на основе выбранных технологий и даны рекомендации по применению выбранных технологий для настройки безопасной корпоративной сети.

Личный вклад автора заключается в том, что анализ материалов и программное моделирование сети были получены лично соискателем. Постановка задач и обсуждение результатов проводились совместно с научным руководителем.

Результаты исследования были представлены на 54-ой научной конференции аспирантов, магистрантов и студентов БГУИР 2018-го года. Результаты магистерской диссертации могут быть использованы в целях обучения.

Основные положения работы и результаты исследования изложены в докладе к 54-ой научной конференции аспирантов, магистрантов и студентов БГУИР 2018-го года (авторский объём 1 л.).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В введении обосновывается актуальность выбранной темы, даётся краткая характеристика её разработанности, определяются объект и предмет исследования.

Первая глава «Защита информации в корпоративной сети» включает общие положения по состоянию защищённости корпоративных сетей и состоит из группы подразделов.

В подразделах первой главы производится анализ наиболее актуальных уязвимостей в корпоративных сетях и рассматриваются современные способы организации защищённой корпоративной сети для устранения этих уязвимостей.

Также рассмотрена технология построения VPN и различные способы реализации VPN.

Вторая глава «Организация безопасности в сети» включает в себя рассмотрение конкретных протоколов для создания надёжной VPN и состоит из группы подразделов.

В подразделах второй главы рассматриваются виды протоколов туннелирования, используемых в VPN, протоколы безопасности, которые позволяют шифровать данные. Описывается протокол безопасности IPSec.

Также во второй главе рассмотрены протоколы маршрутизации и аутентификации.

Третья глава «Моделирование защищённой сети предприятия» описывает практическую часть диссертации и также состоит из группы подразделов.

В подразделах описывается структура выбранной корпоративной сети, её моделирование и проверка работоспособности при помощи программного обеспечения Cisco Packet Tracer, а также создание программного продукта, на основе выбранных технологий построения защищённой корпоративной сети и модели, созданной при помощи Cisco Packet Tracer. Целью созданного программного продукта является обучение и проверка знаний в области настройки защищённой территориально-распределённой корпоративной сети.

ЗАКЛЮЧЕНИЕ

Итогом работы является получение практических навыков построения и моделирования защищённой, территориально-распределенной корпоративной сети предприятия и создание программного продукта на основе полученных знаний.

В ходе работы были изучены технологии построения виртуальных сетей, а также протоколы туннелирования и маршрутизации. Проанализированы вероятные угрозы и предложены варианты защиты от них.

В соответствии с выбранной сетью была подобрана подходящая технология построения виртуальной сети VPN, а также на основе сравнительного анализа и топологии и конфигурации сети был выбран

протокол безопасности IPSec. На основе выбранной структура корпоративная сеть смоделирована и проверена на работоспособность при помощи программного обеспечения Cisco Packet Tracer. Также, на основе выбранных технологий построения защищённой корпоративной сети и модели, созданной при помощи Cisco Packet Tracer, создан программный продукт в виде веб-приложения, готовый для использования.

Поставленные цель и задачи были достигнуты в полном объёме.

Данная сеть может быть построена и сконфигурирована для использования, а созданный программный продукт может использоваться в целях обучения и проверки знаний в области настройки защищённой территориально-распределённой корпоративной сети.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 Комплексная защита информации в корпоративных сетях [Электронный ресурс]. – Режим доступа: http://www.kp.ru/.

2 Защита информации в корпоративных сетях [Электронный ресурс]. – Режим доступа: http:// window.edu.ru/.

3 Боченина, Е. Ю. Реализация атак на инфраструктурные сервисы и протоколы сети. / Челябинск, 2017. – 75 с.

4 Антивирусная защита [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/.

5 Антивирусная защита сетей [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/.

6 Межсетевые экраны [Электронный ресурс]. – Режим доступа: http://compress.ru/.

7 VPN [Электронный ресурс]. – Режим доступа: https://www.draytek.co.uk.

8 Что такое VPN [Электронный ресурс]. – Режим доступа: https://hide.me/.

9 Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы. 5-е издание. / В. Г. Олифер, Н. А. Олифер – СПб. : Питер, 2016. – 992 с.

10 DMVPN [Электронный ресурс]. – Режим доступа: http://network-lab.ru/.

11 VPN [Электронный ресурс]. – Режим доступа: https://knowpc.ru/.

12 Протоколы туннелирования [Электронный ресурс]. – Режим доступа: http://teacherbox.ru/.

13 Выбор протокола безопасности [Электронный ресурс]. – Режим доступа: http://mirznanii.com/.

14 Режимы работы IPSec [Электронный ресурс]. – Режим доступа: http://eucariot.livejournal.com/.

15 ODR (On-Demand Routing) [Электронный ресурс]. – Режим доступа: https://www.howtonetwork.org/.

16 RIP (Routing Information Protocol) [Электронный ресурс]. – Режим доступа: http://ru.bmstu.wiki/.

17 OSPF (Open Shortest Path First) [Электронный ресурс]. – Режим доступа: http://subnets.ru/.

18 EIGRP (Enhanced Interior Gateway Routing Protocol) [Электронный ресурс]. – Режим доступа: http://www.cisco.com/.

19 BGP (Border Gateway Protocol) [Электронный ресурс]. – Режим доступа: https://sites.google.com/.

20 RADIUS Types [Электронный ресурс]. – Режим доступа: http://www.iana.org/.

21 RADIUS (Remote Authentication in Dial-In User Service) [Электронный ресурс]. – Режим доступа: http://dic.academic.ru/.

22 An Analysis of the RADIUS Authentication Protocol [Электронный ресурс]. – Режим доступа: https://www.untruth.org/.

23 Настройка IPSec [Электронный ресурс]. – Режим доступа: https://learn.urfu.ru/.

24 Шифрование пакетов в IPSec [Электронный ресурс]. – Режим доступа: http://rti-mints.ru/.

Список собственных публикаций

1-А Киселёв, Д. В. Выбор протокола безопасности для организации VPN / Д. В. Киселёв // Инфокоммуникации: материалы 54-й научной конференции аспирантов, магистрантов и студентов, Минск, 23–27 апреля 2018 г. – Минск: БГУИР, 2018. – С. 57.