С.В.Запечников
Н.Г.Милославская
А.И.Толстой

ОСНОВЫ ПОСТРОЕНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

2-е издание, стереотипное

Рекомендовано УМО по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям «Компьютерная безопасность» и «Комплексное обеспечение информационной безопасности автоматизированных систем»

Москва
Горячая линия - Телеком
2011

Электронный архив библиотеки МГТУ им. Н.Э. Баумана

ББК 32.973.2-018.2я73
УДК 004.732.056(075.8)
З-31

Запечников С. В., Милославская Н. Г., Толстой А. И.

З-31 Основы построения виртуальных частных сетей. Учебное пособие для вузов. – 2-е изд., стереотип. – М.: Горячая линия–Телеком, 2011. – 248 с.: ил.

ISBN 978-5-9912-0215-2.

Рассматриваются основы построения виртуальных частных сетей (VPN). Даются основные определения. Описывается технология туннелирования в сетях. Подробно анализируются стандартные протоколы построения VPN и управление криптографическими ключами в VPN. Выделяются особенности различных вариантов и схем создания VPN. В качестве примеров реализации VPN приводятся различные российские продукты (по состоянию на момент выхода в свет первого издания книги).

Для студентов высших учебных заведений, обучающихся по специальностям «Компьютерная безопасность» и «Комплексное обеспечение информационной безопасности автоматизированных систем», и слушателей курсов повышения квалификации по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем».

ББК 32.973.2-018.2я73

Адрес издательства в Интернет WWW.TECHBOOK.RU

Учебное издание

Запечников Сергей Владимирович, **Милославская** Наталья Георгиевна, **Толстой** Александр Иванович

ОСНОВЫ ПОСТРОЕНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Учебное пособие

2-е издание, стереотипное

Обложка художника В. Г. Ситникова

Подписано в печать 15.08.11. Печать офсетная. Формат 60×88/16
Уч.-изд. л. 15,5. Тираж 100 экз. Изд. № 110215

ISBN 978-5-9912-0215-2

Цифровая версия книги доступна на сайте www.techbook.ru

Предисловие

Основой для учебного пособия послужил опыт преподавания технологий защиты в открытых сетях лично авторов и их коллег, подробные описания, сделанные разработчиками данных технологий и средств защиты, а также многочисленные отечественные и зарубежные публикации по рассматриваемой тематике.

В настоящее время специалистов-профессионалов по различным аспектам защиты информации готовит ряд вузов России. Обучение происходит на специализированных факультетах, ознакомительных курсах или курсах повышения квалификации. Но все эти учебные заведения испытывают острую нехватку узкопрофильной учебно-методической литературы, что, в первую очередь, сказывается на качестве обучения. Данное учебное пособие предлагается для обучающихся (студентов, аспирантов и повышающих квалификацию специалистов) по группе специальностей "Информационная безопасность".

Поскольку число атак на сети неизменно растет, а создать полностью защищенную информационную среду очень сложно, нужны специализированные средства, предназначенные для осуществления защиты информации, передаваемой по открытым каналам связи сетей передачи данных, и воплощения в жизнь выработанной организацией политики безопасности ее информационных и сетевых ресурсов. Специалист в области информационной безопасности должен владеть определенными теоретическими знаниями и практическими навыками в данной, очень важной области обеспечения информационной безопасности. На сегодняшний день учебной литературы по вопросам построения виртуальных частных сетей, к сожалению, пока не имеется.

Основная задача, которую призвано решить учебное пособие, — это представить обучающимся систематизированный подход к проблеме виртуальных частных сетей (VPN), ознакомить их с характерными признаками различных вариантов их построения, а также научить квалифицировано выбирать, применять и самостоятельно разрабатывать реализующие такие возможности средства. В пособии показано, что при условии грамотного использования VPN (совме-

стно с другими средствами обеспечения информационной безопасности, такими как средства аутентификации, средства обнаружения вторжений и т.п.) может быть реализована достаточно надежная защита информации от несанкционированного перехвата с различными целями во время ее передачи по открытым каналам связи. Такие знания особенно важны для специалистов-практиков по защите информации в современных сетях.

Важно подчеркнуть, что для приступающих к ознакомлению с учебным пособием есть определенные требования по предварительной подготовке. Например, следует знать протоколы и сервисы Internet, сетевые операционные системы, основные принципы безопасности сетей и технологий их защиты, иметь базовые знания по криптографии.

Учебное пособие состоит из введения, пяти разделов, заключения и приложений с полезной информацией.

Во введении отмечается своевременность рассмотрения заявленной в названии учебного пособия темы и решаемые на основе технологии виртуальных сетей задачи.

Первый раздел содержит основные определения, цели и задачи, а также описание специфики построения VPN и основного применяемого подхода — туннелирования. Выделены особенности построения VPN в различных типах сетей и рассмотрены разные схемы VPN. Вводится понятие политики безопасности для VPN и называются другие средства защиты информации, дополняющие VPN и реализующие комплексный подход к защите информации в корпоративных сетях.

Во втором разделе детально рассматриваются стандартные протоколы создания виртуальных частных сетей, реализующие функции VPN на различных уровнях модели взаимодействия открытых систем OSI/ISO (с указанием соотнесения их с уровнями стека протоколов TCP/IP) - канальном, сетевом и сеансовом.

Третий раздел посвящен управлению криптографическими ключами в VPN. Последовательно изучаются жизненный цикл криптографических ключей, особенности управления ключевой системой асимметричных криптосистем, концепция инфрастуктуры открытых

ключей, метод сертификации открытых ключей и модель инфраструктуры открытых ключей PKIX.

В четвертом разделе даются основы практического построения VPN, перечисляются и поясняются требования к VPN-продуктам, которые подразделяются на шлюзы и клиенты, рассматриваются варианты реализации VPN и решения для организации VPN на базе сетевой операционной системы, маршрутизаторов, межсетевых экранов, специализированного программного обеспечения и аппаратных средств. Также анализируются четыре основных вида VPN: Intranet VPN, Client/server VPN, Extranet VPN и Remote Access VPN и приводятся полезные рекомендации специалистов по выбору VPN-продуктов.

Пятый раздел описывает некоторые реализации VPN на основе таких российских разработок, как аппаратно-программный комплекс защиты информации "Континент-К", программные продукты компании "ЭЛВИС+", VPN-решения компании "Инфотекс", семейство продуктов "Net-PRO" компании "Сигнал-КОМ", продукты МО ПНИЭИ "ШИП" и "Игла-2" и аппаратно-программный комплекс "ФПСУ-IP" компании "Амикон". С целью определения лучших условий применения рассмотренных продуктов приводится их сравнение.

В заключение выделены основные проблемы, возникающие при использовании VPN-продуктов, и указаны возможные варианты их усовершенствования.

В приложениях представлена полезная информация справочного характера: сравнение зарубежных продуктов для создания VPN и документы, в которых содержится полное описание основных протоколов для VPN.

После каждого раздела приведены вопросы для самоконтроля.

Авторы признательны коллегам по факультету "Информационная безопасность" МИФИ, а также всем рецензентам.

Авторы, естественно, не претендуют на исчерпывающее изложение всех названных в работе аспектов проблемы построения VPN, поэтому с благодарностью внимательно изучат и учтут критические замечания и предложения читателей при дальнейшей работе над учебным пособием.

ОГЛАВЛЕНИЕ