Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

Иванцов А.М.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ»

Для студентов специалитета по специальности 10.05.03 очной формы обучения

Ульяновск, 2019

Методические указания для самостоятельной работы студентов по дисциплине «Виртуальные частные сети» / составитель: А.М. Иванцов. - Ульяновск: УлГУ, 2019. Настоящие методические указания предназначены для студентов специалитета по специальности 10.05.03 очной формы обучения. В работе приведены литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля и тесты для самостоятельной работы. Студентам очной формы обучения они будут полезны при подготовке к лекциям, семинарам и к зачёту по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 2/19 от 19.03.2019 г.).

Содержание

1. Литература для изучения дисциплины…….……....…… 4
2. Методические указания …….……...…….....…5
2.1. Раздел 1. Виртуальная частная сеть как средство защиты информации.
Тема 1. Введение в технологию виртуальных частных сетей (VPN) ……..5
2.2. Раздел 1. Тема 2. Схема и политики безопасности VPN……..…. 6
2.3. Раздел 1. Тема 3. Стандартные протоколы создания VPN……7
2.4. Раздел 2. Управление криптографическими ключами в виртуальных частных сетях. Тема 4. Особенности управления ключевой системой асимметричных криптосистем. Инфрастуктура открытых ключей…….8
2.5. Раздел 2. Тема 5 Сертификация открытых ключей……. 9
2.6. Раздел 3. Построение виртуальной частной сети. Тема 6. Требования к продуктам построения виртуальных частных сетей. Варианты реализации ….……10
2.7. Раздел 3. Тема 7. Решения для построения виртуальных частных сетей….11
2.8. Раздел 3. Тема 8. Характеристика российских продуктов для создания виртуальных частных сетей……12

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1. Запечников С.В., Основы построения виртуальных частных сетей [Электронный ресурс]: Учебное пособие для вузов / Запечников С.В., Милославская Н.Г., Толстой А.И. - 2-е изд., стереотип. - М.: Горячая линия - Телеком, 2011. - 248 с. - ISBN 978-5-9912-0215-2 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991202152.html

2. Душкин А.В., Программно-аппаратные средства обеспечения информационной безопасности [Электронный ресурс]: Учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов. Под редакцией А.В. Душкина - М.: Горячая линия - Телеком, 2016. - 248 с. - ISBN 978-5-9912-0470-5 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991204705.html.

3. Некоммерческая интернет-версия СПС "КонсультантПлюс":

3.1 Доктрина информационной безопасности Российской Федерации (Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации") Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_208191/

3.2 Стратегия национальной безопасности Российской Федерации (Указ Президента Российской Федерации от 31 декабря 2015 года N 683 "О Стратегии национальной безопасности Российской Федерации") Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_191669/

3.3 Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи» Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/

4. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента. ГОСТ-Эксперт - единая база ГОСТов Российской Федерации для образования и промышленности. Режим доступа: http://gostexpert.ru/gost/gost-27002-2012

5. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", «Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", «Системный анализ и управление» / А.С. Андреев, С.М. Бородин, А.М. Иванцов. - Ульяновск: УлГУ, 2015. 54 с. Режим доступа http://lib.ulsu.ru/MegaPro/Download/MObject/297/Andreev2015.pdf.

6. Бирюков А.А. Информационная безопасность: защита и нападение / Бирюков А. А. - Москва: ДМК Пресс, 2017. - 434 с. - ISBN 978-5-97060-435-9. - Текст: электронный // ЭБС "Консультант студента": [сайт]. - URL: https://www.studentlibrary.ru/book/ISBN9785970604359.html

7. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»; ИНФРА-М, 2014. – 416 с. ил.

8. Чефранова А.О., Алабина Ю.Ф. Технология VPN ViPNet: курс лекций / Под ред. Доктора пед. Наук, профессора А.О. Чефрановой. – М.: Горячая линия – Телеком, 208. – 338 с. Ил.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ КАК СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ

ТЕМА 1. ВВЕДЕНИЕ В ТЕХНОЛОГИЮ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ (VPN)

Основные вопросы:

1. Понятие виртуальной частной сети (VPN)
2. Специфика построения VPN. VPN в публичных сетях. Туннелирование в VPN
3. Туннелирование в VPN

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 5-20.

Для самостоятельного изучения вопроса 1 следует обратиться к [2] на с. 157-160.

Вопрос 2 изложен в учебном пособии [1] на с. 21-25.

Для самостоятельного изучения вопроса 2 следует обратиться к [2] на с. 176-180.

Вопрос 3 изложен в учебном пособии [1] на с. 26-28.

Для самостоятельного изучения вопроса 3 следует обратиться к [7] на с. 218-223.

Контрольные вопросы по теме 1:

1. Что такое виртуальная частная сеть (VPN)?
2. Дать определение технологии VPN
3. Основные задачи технологии VPN
4. Специфика построения VPN
5. Туннелирование в VPN
6. Протоколы механизма туннелирования

Тесты для самостоятельной работы:

1. Суть туннелирования VPN состоит в том, что:

а) при туннелировании пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня

б) при туннелировании пакет протокола более высокого уровня помещается в поле данных пакета протокола более низкого уровня

2. Как называют протокол IPX, переносящий данные в интрасеть филиалов предприятия?

а) протокол-пассажир

б) несущий протокол

в) протокол туннелирования

3. Что, из перечисленного, понимается под термином частная виртуальная сеть?

а) Шифрованный туннель внутри обычной сети
б) Локальная сеть в здании
в) Программный комплекс для шифрования

2.2. РАЗДЕЛ 1. ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ КАК СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ

ТЕМА 2. СХЕМА И ПОЛИТИКИ БЕЗОПАСНОСТИ VPN

Основные вопросы:

1. Схема VPN. Алгоритм работы VPN-агентов
2. Политики безопасности в VPN

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 29-31.

Для самостоятельного изучения вопроса 1 следует обратиться к [7] на с. 217-224.

Вопрос 2 изложен в учебном пособии [1] на с. 32-37.

Для самостоятельного изучения вопроса 2 следует обратиться к [6] на с. 395-408, к [3.1-3.2, 4].

Контрольные вопросы по теме 2:

1. Пояснить основные элементы схемы VPN
2. Что такое VPN-агент
3. Алгоритм работы VPN-агентов
4. Политики безопасности в VPN. Примеры политик безопасности VPN
5. Критерии безопасности VPN
6. Варианты создания VPN (защищённые каналы, частные каналы, промежуточные каналы)

Тесты для самостоятельной работы:

1. Безопасность VPN будет равна:

а) безопасности наиболее защищённой интрасети
б) безопасности наименее защищённой интрасети
в) не зависит от безопасности отдельных интрасетей

2. Для варианта создания VPN под названием «защищённые каналы»:

а) шифруется и расшифровывается только трафик, передаваемый между хостами
б) шифруется и расшифровывается не весь трафик
в) шифруется и расшифровывается весь трафик

2.3. РАЗДЕЛ 1. ВИРТУАЛЬНАЯ ЧАСТНАЯ СЕТЬ КАК СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ

ТЕМА 3. СТАНДАРТНЫЕ ПРОТОКОЛЫ СОЗДАНИЯ VPN

Основные вопросы:

1. Семиуровневая модель взаимодействия открытых систем (OSI)
2. Протоколы защиты данных канального, транспортного и сеансового уровней

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [6] на с. 26-30.

Вопрос 2 изложен в учебном пособии [6] на с. 36-40, 108-111.

Контрольные вопросы по теме 3:

1. Уровни защищённых каналов
2. Семиуровневая модель взаимодействия открытых систем (OSI)
3. Протоколы защиты данных канального уровня (PPTP, L2F и L2TP)
4. Сравнительный анализ протоколов защиты на канальном уровне
5. Защита данных на сетевом уровне (Протокол IPSec)
6. Протоколы туннельного и транспортного режимов
7. Защита на сеансовом уровне (Протоколы SSL, TLS, SOCKS)

Тесты для самостоятельной работы:

1. Какой протокол используют для реализации частных виртуальных сетей?

а) RADIUS
б) TCP/UDP
в) SIP
г) NFS

2. К средствам VPN, как правило, относят протоколы модели OSI (выбрать 3 позиции):

а) канального уровня
б) физического уровня
в) сетевого уровня
г) прикладного уровня
д) транспортного уровня
е) сеансового уровня

3. Какой протокол, из перечисленных, используется для защиты данных на сетевом уровне?

а) PPTP
б) IPSec

в) L2F
г) L2TP

2.4. РАЗДЕЛ 2. УПРАВЛЕНИЕ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ В ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЯХ

ТЕМА 4. ОСОБЕННОСТИ УПРАВЛЕНИЯ КЛЮЧЕВОЙ СИСТЕМОЙ АСИММЕТРИЧНЫХ КРИПТОСИСТЕМ. ИНФРАСТУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

Основные вопросы:

1. Проблемы управления криптографическими ключами
2. Инфраструктура открытых ключей (ИОК). Модели APKI и PKIX

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 96-101.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [7] на с. 98-110.

Вопрос 2 изложен в учебном пособии [1] на с. 102-106.

Контрольные вопросы по теме 4:

1. Понятие управления криптографическими ключами
2. Жизненный цикл ключей
3. Компрометация ключей
4. Управление секретными и открытыми ключами
5. Инфраструктура открытых ключей (ИОК)
6. Модели APKI и PKIX

Тесты для самостоятельной работы:

1. Какая, из перечисленных, задач управления ключами наиболее проста?

а) управление открытыми ключами
б управление секретными ключами
в) являются идентичными

2. Какая фаза, из перечисленных, с точки зрения сложности реализации мер обеспечения безопасности ключей, является наиболее сложной?

а) генерация ключей
б) распространение ключей
в) хранение ключей
г) уничтожение ключей

3. Какие криптографические системы, из перечисленных, наиболее производительны?

а) асимметричные
б) симметричные

в) симметричные и асимметричные системы одинаковы по производительности

2.5. РАЗДЕЛ 2. УПРАВЛЕНИЕ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ В ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЯХ

ТЕМА 5. СЕРТИФИКАЦИЯ ОТКРЫТЫХ КЛЮЧЕЙ

Основные вопросы:

1. Основные подходы к обеспечению безопасности открытых ключей. Содержание метода сертификации открытых ключей
2. Закон РФ «Об электронной подписи»

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 107-114.

Для самостоятельного изучения вопроса 2 следует обратиться к [2] на с. 107-114.

Вопрос 2 изложен в учебном пособии [1] на с. 121-125.

Для самостоятельного изучения вопроса 2 следует обратиться к тексту Закона РФ «Об электронной подписи» [3.3].

Контрольные вопросы по теме 5:

3. Подходы к обеспечению безопасности открытых ключей
4. Содержание метода сертификации открытых ключей
5. Удостоверяющий центр
6. Сертификат открытого ключа
7. Формат сертификации открытого ключа
8. Аннулирование сертификатов
9. Модель инфраструктуры открытых ключей
10. Основные протоколы ИОК согласно модели PKIX
11. Закон РФ «Об электронной подписи»

Тесты для самостоятельной работы:

1. Какой подход обеспечения безопасности открытых систем, из перечисленных, наиболее распространён в VPN?

а) передача ключа через доверенный канал
б) прямой доступ в доверенную базу данных
в) использование криптосистем, основанных на идентификаторах
г) использование криптосистем с неявно сертифицированными открытыми ключами
д) использование метода сертификации открытых ключей

2. Сертификат открытого ключа – это?

а) специальная структура данных, состоящая из поля подписи
б) специальная структура данных, состоящая из полей данных и поля подписи
в) специальная структура данных, состоящая из полей данных

3. Какой из перечисленных стандартов относится к административным протоколам?
а) RFC 2585
б) RFC 2560
в) RFC 2511

4. Как генерируются данные для шифрования трафика?
а) Задаются вручную
б) С помощью специальных алгоритмов и библиотек
в) Берутся из открытой баз

2.6. РАЗДЕЛ 3. ПОСТРОЕНИЕ ВИРТУАЛЬНОЙ ЧАСТНОЙ СЕТИ

ТЕМА 6. ТРЕБОВАНИЯ К ПРОДУКТАМ ПОСТРОЕНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ. ВАРИАНТЫ РЕАЛИЗАЦИИ

Основные вопросы:

1. Характеристика основных средств построения VPN
2. Варианты реализации VPN

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 127-136.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [7] на с. 217-225.

Вопрос 2 изложен в учебном пособии [1] на с. 137-142.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [7] на с. 235-238.

Контрольные вопросы по теме 6:

1. Характеристика основных средств построения VPN
2. Производительность
3. Управляемость
4. Совместимость
5. Поддержка справочной службы
6. Надёжность защиты и функциональная полнота
7. Реализация алгоритмов скоростной криптозащиты
8. Варианты реализации VPN
9. Шлюзы и клиенты VPN

Тесты для самостоятельной работы:

1. Какой VPN-продукт, из перечисленных, обладает наиболее высокой производительностью?
а) выполненный на основе маршрутизатора
б) выполненный на основе специального процессора

в) выполненный на основе межсетевого экрана

2. Задержки какого типа, из перечисленных, начинают играть роль при использовании высокоскоростных каналов?
а) задержки при установлении защищённого соединения между VPN-устройствами
б) задержки, связанные с шифрованием и расшифрованием
в) задержки, связанные с добавлением нового заголовка к передаваемым пакетам

3. Какой протокол, из перечисленных, используется в VPN на базе сетевой операционной системы?
а) L2F
б) PPTP
в) UDP

2.7. РАЗДЕЛ 3. ПОСТРОЕНИЕ ВИРТУАЛЬНОЙ ЧАСТНОЙ СЕТИ

ТЕМА 7. РЕШЕНИЯ ДЛЯ ПОСТРОЕНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Основные вопросы:
1. Особенности VPN, построенных на различных базах
2. Виды виртуальных частных сетей

Рекомендации по изучению темы:
Вопрос 1 изложен в учебном пособии [1] на с. 141-166.
Вопрос 2 изложен в учебном пособии [1] на с. 167-182.

Контрольные вопросы по теме 7:
1. VPN на базе сетевых операционных систем
2. VPN на базе маршрутизаторов
3. VPN на базе межсетевых экранов
4. VPN на базе специализированного программного обеспечения
5. VPN на базе аппаратных средств
6. Виды виртуальных частных сетей

Тесты для самостоятельной работы:
1. Какой протокол, из перечисленных, используется в VPN на базе сетевой операционной системы?
а) L2F
б) PPTP
в) UDP

2. Что применяется в частных виртуальных сетях?
а) Кодирование
б) Балансировка нагрузки
в) Шифрование

3. Какая библиотека используется для шифрования частных сетей чаще всего?
а) DenLib
б) MD5
в) OpenSSL
г) CryptoPr

2.8. РАЗДЕЛ 3. ПОСТРОЕНИЕ ВИРТУАЛЬНОЙ ЧАСТНОЙ СЕТИ

ТЕМА 8. ХАРАКТЕРИСТИКА РОССИЙСКИХ ПРОДУКТОВ ДЛЯ СОЗДАНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Основные вопросы:

1. Аппаратно-программный комплекс «Континент»
2. Продукты комплекса «VipNet»
3. Сравнительный анализ российских продуктов

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [1] на с. 194-198.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [8] на с. 8-13, 232, 305.

Вопрос 2 изложен в учебном пособии [1] на с. 199-201.

Вопрос 3 изложен в учебном пособии [1] на с. 222-229.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [5].

Контрольные вопросы по теме 8:

1. Аппаратно-программный комплекс «Континент»
2. Программные продукты семейства «Застава»
3. Продукты комплекса «VipNet»
4. Семейство продуктов «Net-PRO»
5. Продукты «Шип» и «Игла-2»
6. Сравнительный анализ российских продуктов

Тесты для самостоятельной работы:

1. Какой стандарт шифрования, из перечисленных, вошёл в современный ГОСТ Р 34.12-2015?
а) DES
б) ГОСТ 28147- 89

в) RSA

2. Какой из российских продуктов для создания VPN использует ОС FreeBSD?

а) Континент
б) ШИП
в) VipNet
г) Застава

3. В каком из российских продуктов для создания VPN не используется идентификация и аутентификация сетевого трафика?

а) Континент
б) ШИП
в) VipNet
г) Застава

4. В каком из российских продуктов для создания VPN используется электронный замок «Соболь»?

а) Континент
б) ШИП
в) VipNet
г) Застава