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

Клочков А.Е.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ»

Для студентов специалитета по специальности 10.05.03 очной формы обучения

Ульяновск, 2019

Методические указания для самостоятельной работы студентов по дисциплине «Безопасность сетей ЭВМ» / составитель: А.Е. Клочков - 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

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.

9. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы,

технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер, 2014. — 944 с.

10. Шелухин О.И., Обнаружение вторжений в компьютерные сети (сетевые аномалии) [Электронный ресурс]: Учебное пособие для вузов / Под ред. профессора О.И. Шелухина. - М.: Горячая линия - Телеком, 2013. - 220 с. - ISBN 978-5-9912-0323-4 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991203234.html.

11.Основы информационной безопасности. Курс лекций. Часть 2 / А.М. Иванцов, В.Г. Козловский. – Ульяновск: УлГУ, 2020 – 103 с.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ТИПОВЫЕ УГРОЗЫ СЕТЕВОЙ БЕЗОПАСНОСТИ

ТЕМА 1. СЕТЕВЫЕ АТАКИ

Основные вопросы:

1. Классификация сетей ЭВМ
2. Сетевые угрозы уязвимости и атаки

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [9] на с. 124-134.

Вопрос 2 изложен в учебном пособии [7] на с. 26-48.

Для самостоятельного изучения вопроса 2 следует обратиться к [6] на с. 196-229.

Контрольные вопросы по теме 1:

1. Классификация сетей ЭВМ
2. Классификация сетевых угроз, уязвимостей и атак
3. Атаки на реализации сетевых протоколов, отдельные узлы и службы
4. Стадии проведения сетевой атаки
3. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI
4. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.

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. ТИПОВЫЕ УГРОЗЫ СЕТЕВОЙ БЕЗОПАСНОСТИ

ТЕМА 2. МЕХАНИЗМЫ РЕАЛИЗАЦИИ АТАК В СЕТЯХ TCP/IP

Основные вопросы:

1. Классификация атак
2. Этапы реализации атак

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [10] на с. 5-8.

Для самостоятельного изучения вопроса 1 следует обратиться к [9] на с. 829-844.

Вопрос 2 изложен в учебном пособии [10] на с. 8-15.

Контрольные вопросы по теме 2:

1. Стек протоколов Методы сканирования портов TCP/IP
2. Методы обнаружения пакетных сниферов
3. Методы обхода МЭ
4. Основные механизмы реализации атак

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. ТИПОВЫЕ УГРОЗЫ СЕТЕВОЙ БЕЗОПАСНОСТИ

ТЕМА 3. МЕТОДЫ ПЕРЕХВАТА СЕТЕВЫХ СОЕДИНЕНИЙ В СЕТЯХ TCP/IP

Основные вопросы:

1. Атаки, направленные на сетевую инфраструктуру
2. Методы защиты от атак на сетевую инфраструктуру

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [6] на с. 54-89.

Вопрос 2 изложен в учебном пособии [9] на с. 845-856.

Для самостоятельного изучения вопроса 2 следует обратиться к [2] на с. 45-60.

Контрольные вопросы по теме 3:

1. Имперсонация вслепую
2. Десинхронизация TCP-соединений
3. Характеристика атаки направленных на сетевую инфраструктуру
4. Основные методы защиты от атак на сетевую инфраструктуру

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 1. ТИПОВЫЕ УГРОЗЫ СЕТЕВОЙ БЕЗОПАСНОСТИ

ТЕМА 4. ПРИМЕРЫ СЕТЕВЫХ АТАК В СЕТЯХ TCP/IP. ТЕХНИЧЕСКИЕ МЕРЫ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК

Основные вопросы:

1. Атаки, направленные на отказ в обслуживании
2. Технические меры защиты от сетевых атак

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [9] на с. 831-844.
Вопрос 2 изложен в учебном пособии [9] на с. 845-856.

Контрольные вопросы по теме 4:

1. Принуждение к ускоренной передаче
2. Характеристики атак, направленные на отказ в обслуживании
3. Изменение конфигурации и состояния хостов
4. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации
5. Характеристика технических мер защиты от сетевых атак

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. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

ТЕМА 5. КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основные вопросы:

1. Протоколы аутентификации на прикладном и транспортном уровнях
2. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [7] на с. 293-307.

Для самостоятельного изучения вопроса 2 следует обратиться к [9] на с. 860-869.

Вопрос 2 изложен в учебном пособии [6] на с. 368-390.

Контрольные вопросы по теме 5:

1. Протоколы аутентификации на прикладном уровне
2. Протокол Kerberos
3. Протоколы аутентификации на транспортном уровне
4. Протокол SSL/TLS
5. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI

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 2. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

ТЕМА 6. ЗАЩИТА ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ (VPN)

Основные вопросы:

1. Принципы функционирования и варианты реализации VPN
2. Организация туннелирования на различных уровнях модели ISO/OSI

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, а также в учебном пособии [8] на с. 232-244.

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. Назначение, основные возможности, принципы функционирования и варианты реализации VPN
2. Организация туннелирования на различных уровнях модели ISO/OSI
3. Достоинства и недостатки применения VPN
4. Протокол IPSEC
5. Протоколы AH и ESP
6. Особенности работы протокола IP SEC в туннельном и транспортном режимах
7. Протокол управления ключами ISAKMP/Oakley
8. Использование протокола L2TP для организации виртуальных частных сетей

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 2. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

ТЕМА 7. РАЗРАБОТКА ЗАЩИЩЕННЫХ СЕТЕВЫХ ПРИЛОЖЕНИЙ

Основные вопросы:

1. Методы и стандарты шифрования
2. Обеспечение целостности с использованием программного интерфейса SSPI.

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [7] на с. 76-92.
Вопрос 2 изложен в учебном пособии [1] на с. 167-182.

Контрольные вопросы по теме 7:

3. Охарактеризовать процедуру аутентификации
4. Методы и стандарты шифрования
5. Обеспечение целостности с использованием программного интерфейса SSPI.
6. Программный интерфейс OpenSSL

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. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

ТЕМА 8. СРЕДСТВА ЗАЩИТЫ ЛОКАЛЬНЫХ СЕТЕЙ ПРИ ПОДКЛЮЧЕНИИ К ИНТЕРНЕТ

Основные вопросы:

1. Основные понятия технологии межсетевых экранов
2. Функции межсетевых экранов
3. Ориентация МЭ на уровни эталонной модели

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [11] на с. 83-84.
Вопрос 2 изложен в учебном пособии [11] на с. 85-89.
Вопрос 3 изложен в учебном пособии [11] на с. 90-101.

Контрольные вопросы по теме 8:

1. Межсетевые экраны (МЭ)
2. Классификация МЭ
3. Требования к МЭ
4. Основные возможности и схемы развертывания МЭ
5. Достоинства и недостатки МЭ
6. Построение правил фильтрации
7. Методы сетевой трансляции адресов (NAT)
8. Шлюзы уровня приложений
9. Методы обхода межсетевых экранов

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

2.9. РАЗДЕЛ 3. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

ТЕМА 9. ЗАЩИТА СЕРВЕРОВ И РАБОЧИХ СТАНЦИЙ

Основные вопросы:

1. Основные принципы построения систем обнаружения и предотвращения вторжений
2. Способы противодействия вторжениям

Рекомендации по изучению темы:

Вопрос 1 изложен в учебном пособии [10] на с. 15-41.

Для самостоятельного изучения вопроса 1 следует обратиться к учебному пособию [7] на с. 339-342.

Вопрос 2 изложен в учебном пособии [7] на с. 343-351.

Контрольные вопросы по теме 9:

1. Основные методы предотвращения и обнаружения вторжений
2. Характеристика системы обнаружения вторжений (СОВ)
3. Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы
4. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности
5. Классификация СОВ
6. Выявление атак на основе сигнатур атак и выявления аномалий
7. Аудит прикладных служб
8. Средства обнаружения уязвимостей сетевых служб
9. Системы виртуальных ловушек (Honey Pot и Padded Cell)
10. Основные способы противодействия вторжениям

Тесты для самостоятельной работы:

1. **Система обнаружения вторжений (СОВ) называется поведенческой, если она:**

а) работает с информацией о вторжениях (атаках)
б) использует информацию о нормальном поведении контролируемой системы
в) только выдает предупреждения

2. Система обнаружения вторжений (СОВ) называется интеллектуальной, если она:

а) работает с информацией о вторжениях (атаках)
б) использует информацию о нормальном поведении контролируемой системы
в) только выдает предупреждения

3. В чём основное преимущество систем обнаружения аномалий (СОА)?

а) обнаружение неизвестных атак