МИНОБРНАУКИ РОССИИ
Федеральное государственные бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__4__» ____04____ 2022 г.

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Методические рекомендации для самостоятельной подготовки к занятиям студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Защита информации в компьютерных сетях» очной формы обучения

Курск 2022

УДК 004.056.5

Составитель М.А. Ефремов

Рецензент
Кандидат технических наук, доцент *А.Л. Марухленко*

Защита информации в компьютерных сетях: методические рекомендации для самостоятельной подготовки к занятиям студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Защита информации в компьютерных сетях» / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2022. - 19 с.

Содержат информацию, необходимую студентам в процессе самостоятельной подготовки к занятиям по дисциплине.

Методические рекомендации соответствуют требованиям программы, утвержденной учебно-методическими объединениями по специальностям.

Предназначены для студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Защита информации в компьютерных сетях», очной формы обучения.

Текст печатается в авторской редакции

Подписано в печать Формат 60х84 1/16
Усл.печ.л. 1,10 Уч.-изд.л. 1,00 Заказ 902 Тираж 100 экз. Бесплатно
Юго-Западный государственный университет
305040, г. Курск, ул. 50 лет Октября, 94

ПРЕДИСЛОВИЕ

Методические рекомендации разработаны с целью оказания помощи студентам направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Защита информации в компьютерных сетях», очной формы обучения, при самостоятельной подготовке к занятиям по дисциплине.

Методические рекомендации разработаны в соответствии с Федеральными государственными образовательными стандартами высшего образования соответствующих направлений подготовки.

Предлагаемые методические рекомендации содержат краткое содержание рассматриваемых тем дисциплины и задания для самоконтроля в форме вопросов.

Студентам предлагается список учебной литературы по дисциплине и перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для самостоятельной подготовки к занятиям.

Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы обучающихся являются лекции и практические занятия.

В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на практическое занятие и указания на самостоятельную работу.

Практические занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности студентов по изучаемой дисциплине.

Практические занятия предполагают свободный обмен мнениями по избранной тематике. Занятие начинается со вступительного слова преподавателя, формулирующего цель занятия и характеризующего его основную проблематику. Затем, как правило, заслушиваются сообщения студентов. Обсуждение сообщения совмещается с рассмотрением намеченных вопросов. Сообщения, предполагающие анализ публикаций по отдельным вопросам семинара, заслушиваются обычно в середине занятия. Поощряется выдвижение и обсуждение альтернативных мнений. В заключительном слове преподаватель подводит итоги обсуждения и объявляет баллы выступавшим студентам. В целях контроля подготовленности студентов и привития им навыков краткого письменного изложения своих мыслей преподаватель в ходе практических занятий может осуществлять текущий контроль знаний в виде тестовых заданий.

При подготовке к занятию студенты имеют возможность воспользоваться консультациями преподавателя. Кроме указанных тем, студенты вправе, по согласованию с преподавателем, избирать и другие интересующие их темы.

Качество учебной работы студентов преподаватель оценивает в конце занятия.

При освоении данного курса студент может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой.

В процессе *подготовки к экзамену* студенту следует руководствоваться следующими рекомендациями:

- необходимо стремиться к пониманию всего материала, чтобы еще до экзамена не оставалось непонятных вопросов;
- необходимо строго следить за точностью своих выражений и правильностью употребляемых терминов;
- не следует опасаться дополнительных вопросов – чаще всего преподаватель использует их как один из способов помочь студенту или сэкономить время;
- прежде чем отвечать на вопрос, необходимо сначала правильно его понять.

Содержание дисциплины, структурированное по темам (разделам)

Таблица 1–Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Настройка компьютерной сети	Общие сведения о компьютерных сетях, состав и и оборудование компьютерных сетей. Технические характеристики
2.	Организация защиты совместно используемых сетевых ресурсов	Виды совместно используемых ресурсов, задачи совместного использования сетевых ресурсов. Методы обращения к сетевым ресурсам. Штатные средства защиты совместных сетевых ресурсов операционных систем. Решения сторонних производителей
3.	Анализ кадров ethernet	Задачи анализа пакетов данных, передаваемых по сети. Угрозы, которые несёт анализ кадров со стороны злоумышленника. Средства анализа трафика, их функциональные возможности

4.	Технологии маршрутизации	Задачи маршрутизации сообщений и кадров. Средства маршрутизации, особенности маршрутизации пакетов различных типов.
5.	Работа протоколов транспортного уровня udp и tcp	Структура кадров протоколов транспортного уровня. Угрозы информации на транспортном уровне. Области применения протоколов, преимущества и ндостатки протоколов
6.	Сертификаты для безопасного сетевого взаимодействия	Назначение сертификатов при сетевом взаимодействии. Принципы работы цифровых сертификатов. Жизненный цикл сертификата. Протоколы проверки сертификатов, используемые при сетевом взаимодействии
7.	Защита соединений	Стандарт IPsec. Режимы тунеллирования данных, Структура кадра пакета защищённого соединения. Алгоритмы установления защищённого соединения. Виртуальные частные сети: назначение, иольуемые технологии, используемые алгоритмы
8.	Брандмауэры	Назначение и принципы работы МСЭ. Виды МСЭ. Реализация МСЭ средствами операционных систем. МСЭ сторонних разработчиков. Уязвимости и ограничения примения МСЭ
9.	Протоколы аутентификации	Общая схема аутентификации пользователей компьютерных сетей. Протоколы аутентификации, используемые в компьютерных сетях. Используемые криптографические схемы аутентификации. Протокол Kerberos

Задания для самоконтроля по темам курса

Тема 1. Настройка компьютерной сети.

1. Перечислите действия, необходимые для организации локальной компьютерной сети.

2. Назовите основные компоненты, входящие в состав сетевого адаптера.

3. Назовите известные Вам скорости и режимы передачи данных, используемые в сетевых адаптерах, поддерживающих тот либо иной вариант технологии Ethernet.

4. Перечислите системные ресурсы, потребляемые сетевыми адаптерами.

5. Опишите отличия работы сетевого коммутатора и сетевого маршрутизатора.

6. Охарактеризуйте режим инфраструктуры беспроводной локальной сети.

7. Назовите порядок раскладки проводов в разъѐме RJ-45 согласно стандарту TIA/EIA-568B.

8. Поясните, в каких случаях и почему применяются прямой и пере- крѐстный кабели UTP.

9. Назовите параметры стек сетевых протоколов TCP/IP, конфигурируемые для компьютеров сети.

10. Опишите формат IP-адреса 4-й версии протокола IP. Почему максимальное значение любого из чисел IP-адреса ограничено 255?

11. Опишите формат вывода работы утилиты ping.

12. Что называют шлюзом сети?

13. Какие дополнительные возможности при связи компьютеров даѐт организация в сети DNS-сервера?

14. Какие дополнительные возможности даѐт организация в сети DHCP- сервера?

15. Чем сетевой принтер отличается от обычного принтера, подключѐнного к компьютеру, входящему в локальную сеть?

16. Что такое Cisco IOS?

17. Опишите возможности технологии VLAN и способы организации VLAN в сетевых устройствах.

Тема 2. Организация защиты совместно используемых сетевых ресурсов.

1. Назовите основные сетевые компоненты, обеспечивающие работу се- тевого подключения в операционных системах семейства Windows.

2. Что называют драйвером устройства, каковы его основные функции?

3. Что называют сетевым протоколом и стеком сетевых протоколов? Назовите основные задачи протокола сетевого уровня.

4. Назовите задачи клиентского и серверного компонентов сетевого подключения. Поясните, что собой представляет одноранговая сеть.

5. Опишите способ организации общего доступа компьютеров локальной сети к Интернет, доступный в современных версиях Windows.

6. Объясните, для чего пользователи операционной системы объединяются в группы. Как в операционной системе Windows добавить пользователя в ту или иную группу?

7. Какие типы ресурсов могут быть выделены в совместное использование по сети?

8. Охарактеризуйте типы разрешений сетевого доступа к файловым ре- сурсам. Чем разрешение Полный доступ отличается от разрешения Изменение?

9. Назовите известные Вам имена пользователей и групп, зарегистрированные в Windows по умолчанию. Для чего существует учѐтная запись

10. Гость? Какие пользователи входят в группу Все?

11. Сможет ли пользователь с правами Администратора на удалѐнном компьютере подключиться к папке, специально не выделенной в совместное использование по сети? Если сможет, то как?

12. Что собой представляет технология доменов фирмы Microsoft, какова роль контроллера домена? Можно ли для определѐнного перечня пользователей выделить сетевые ресурсы на разных компьютерах сети с возможностью использования этих ресурсов этими пользователями, зарегистрировавшимися на любом из компьютеров?

13. В чем различие назначения разрешений на вкладках Доступ и Безопасность окна Свойства папки/диска?

14. В чем состоит опасность постоянной работы с учѐтной записью с правами Администратора?

15. Назовите последовательность действий при выделении в общее пользование по сети папки в операционной системе Windows.

16. Назовите последовательность действий, выполняемых при подключении к сетевой папке на удалѐнном компьютере.

17. Охарактеризуйте разрешения, выбираемые при выделении принтера в совместное использование по сети.

18. Назовите последовательность действий при выделении в общее пользование по сети принтера в операционной системе Windows.

19. Назовите последовательность действий, выполняемых при подключении на своѐм компьютере сетевого принтера.

20. Приведите net-команду, позволяющую просмотреть перечень имѐн компьютеров Вашей локальной сети.

21. Приведите net-команду, позволяющую просмотреть перечень сетевых ресурсов на конкретном удалѐнном компьютере.

22. Приведите net-команду, позволяющую подключить на своѐм компьютере удалѐнный файловый ресурс как локальный диск.

23. Приведите net-команду, позволяющую просмотреть сконфигурированные сетевые ресурсы на Вашем компьютере, и команду, позволяющую отключить указанный сетевой файловый ресурс?

24. Назовите протокол прикладного уровня, используемый в операционных системах Windows и Linux/Unix для организации сетевого доступа к файловым ресурсам и принтерам и программное обеспечение, обычно реализующее его в Linux/Unix.

25. Выделите каталог (папку) в качестве сетевого ресурса на компьютере, работающем под управлением Linux, и подключитесь к нему с компьютера, работающего под управлением Windows.

26. Настройте сетевой принтер на компьютере, работающем под управлением Linux, и подключитесь к нему с компьютера, работающего под управлением Windows.

27. Повторите задания предыдущих двух пунктов, выбрав в качестве сервера компьютер, работающий под управлением Windows.

Тема 3. Работа протоколов транспортного уровня.

1. Укажите, на каких уровнях модели взаимодействия открытых систем работает технология Ethernet.

2. Укажите название организации, разрабатывающей стандарты технологии Ethernet.

3. Укажите наиболее распространѐнные версии технологии Ethernet в настоящее время и скорости передачи данных этими технологиями.

4. Укажите наиболее скоростные в настоящее время и перспективные версии технологии Ethernet и скорости передачи данных этими технологиями.

5. Что собой представляет технология Wi-Fi, кто является разработчиком стандартов этой технологии?

6. Опишите обобщѐнный формат кадра Ethernet и укажите размеры его полей в байтах.

7. Что представляет собой контрольная сумма кадра Ethernet, какой алгоритм используется для еѐ расчѐта?

8. Опишите формат MAC-адреса. Дайте характеристику его полям.

9. Укажите типы MAC-адресов, каким образом выполняется идентификация типа по значению MAC-адреса?

10. Опишите форматы кадров Ethernet: Ethernet II (DIX) и Ethernet Raw 802.3/Novell 802.3, что обозначает аббревиатура DIX?

11. Опишите форматы кадров Ethernet 802.3/LLC и Ethernet SNAP. Какие функции выполняют подзаголовки LLC и SNAP?

12. Опишите алгоритм определения типа кадра Ethernet.

13. Перечислите основные функции анализаторов сетевых протоколов и опишите интерфейс и способы работы с анализатором

Wireshark. Как осуществляется работа интерфейса в неразборчивом режиме?

14. Опишите назначение и алгоритм работы протокола ARP. Что собой представляет ARP-кэш и какой командой можно его просмотреть на рабочей станции?

15. Укажите, в каких пределах распространяются широковещательные кадры.

16. Опишите принцип работы коммутатора Ethernet. Что собой представляет таблица MAC-адресов и каким образом она заполняется?

17. Укажите, как коммутатор Ethernet передаѐт широковещательные кадры и кадры с MAC-адресом получателя, для которого отсутствует запись в таблице MAC-адресов.

18. Приведите команду фильтров захвата: а) для захвата кадров с сообщениями, высылаемыми утилитой ping; б) для захвата кадров, отправляемых/получаемых рабочей станцией с IP-адресом 192.168.1.1; в) для захвата кадров с ARP-пакетами.

19. Опишите возможности, предоставляемые программой Packet Tracer в режиме симуляции. Что называют протокольной единицей данных (PDU)?

20. Назовите режимы работы Cisco IOS с сетевыми устройствами и команды перехода из режима в режим.

21. Приведите последовательность команд Cisco IOS для просмотра MAC-таблицы коммутатора Ethernet.

Тема 4. Технологии маршрутизации.

1. Опишите основное назначение протокола IP. Сравните пределы передачи IP-дейтаграмм и Ethernet-кадров.

2. Опишите формат IP-адреса протокола IP v4, назовите его принципиальное отличие от MAC-адреса.

3. Дайте определение технологии маршрутизации.

4. Что называют шлюзом сети/подсети. В каком случае пакеты проходят через шлюз?

5. Что представляет собой фрагментация/дефрагментация дейтаграмм? В каком случае она выполняется? Что такое MTU?

6. Оцените объем пространства адресов IP v4 и опишите, как организовано их выделение конечным пользователям.

7. Назовите классы IP адресов и их характеристики. Каким образом маршрутизаторы определяют принадлежность IP-адреса получателя к тому или иному классу?

8. Опишите особые (выделенные под специальные нужды) IP адреса и их назначение.

9. Что представляют собой локальные IP-адреса, назовите диапазоны сетей таких адресов. Для чего служит технология сетевой трансляции адресов?

10. Опишите формат и использование маски подсети. Как по значению маски определить количество адресов, которое она выделяет? Перечислите известные Вам маски и их характеристики для сети класса C.

11. Определите, входят ли два IP-адреса (например, 192.168.1.67 и

12. 192.168.117) в одну и ту же подсеть с маской 255.255.255.192.

13. Что представляет собой технология бесклассовой междоменной маршрутизации? Запишите адрес и маску суперсети для 2000 хостов.

14. Опишите структуру таблицы маршрутизации и способ нахождения маршрута маршрутизатором по IP-адресу получателя.

15. Что представляет собой маршрут по умолчанию, для чего он используется? Каким образом маршрут по умолчанию указывается в таблице маршрутизации?

16. Что такое метрика маршрута, какие параметры могут служить метрикой?

17. Чем отличается статическая маршрутизация от динамической? Приведите названия популярных протоколов динамической маршрутизации.

18. Опишите алгоритм нахождения маршрутизаторами следующего от них шага маршрута. Каким образом адресуется интерфейс, на который необходимо переслать пакет, на следующем шаге маршрута?

19. Выведите на экран Вашего компьютера таблицу маршрутизации для его интерфейсов.

20. Опишите формат заголовка IP и назначение его полей. Какова минимальная и максимальная длина IP пакета?

21. Опишите, каким образом выполняется фрагментация и дефрагментация пакетов при пересечении ними сетей с различным значением MTU.

22. Что такое время жизни пакета и для чего служит этот параметр?

23. Укажите идентификаторы наиболее популярных протоколов, пакеты которых переносятся в поле данных IP.

Тема 5. Работа протоколов транспортного уровня

1. Назовите назначение портов транспортного уровня и приведите примеры портов.

2. Назовите диапазон портов, закреплѐнный за стандартными серверными службами.

3. Приведите примеры портов служб, обычно использующих UDP и портов служб, обычно использующих TCP.

4. Назовите сходство и отличие функций протоколов UDP и TCP.

5. Что называют адресом сокет? Назовите команду, позволяющую отобразить пары сокетов, образующих коммуникации.

6. Опишите заголовок UDP. Как вычисляется контрольная сумма заголовка?

7. Перечислите механизмы обеспечения протоколом TCP надежности передачи данных.

8. Что называют максимальным размером сегмента и как он рассчитывается?

9. Опишите алгоритм позитивного подтверждения с ретрансляцией и его использование TCP.

10. Опишите процедуру установления соединения протоколом TCP. Какие поля заголовка транспортного уровня при этом задействованы?

11. Опишите алгоритмы передачи данных и завершения соединения протоколом TCP. Какие поля заголовка транспортного уровня при этом задействованы?

12. Каким образом протокол TCP может регулировать поток поступающих хосту-получателю данных?

13. Опишите механизмы выталкивания данных из выходного буфера и пересылки срочных данных, поддерживаемых TCP. Приведите примеры их использования.

14. Опишите формат заголовка TCP.

Тема 6. Сертификаты для безопасного сетевого взаимодействия

1. Какие средства обеспечивают поддержку инфраструктуры цифровых сертификатов

2. Существуют ли национальные стандарты для цифровых сертификатов

3. Опишите основные этапы жизненного цикла цифровых сертификатов

4. Опишите основные этапы проверки сертификата

5. Назначение удостоверяющего центра

6. Опишите процесс распространения информации, подлинность которой подтверждена цифровым сертификатом

Тема 7. Защита соединений

1. На каком уровне модели OSI происходит тунеллирование

2. Какие поля кадра предназначены для организации безопасного сетевого соединения

3. От каких угроз обеспечивает защиту использование тунелирования

4. Предложите модель угроз для сетевого протокола IPSec

5. Охарактеризуйте метод, использующий код идентификации хэшированного сообщения для установления защищённого соединения

6. Для чего используется технология виртуальных частных сетей

Тема 8. Брандмауэры

1. Охарактеризуйте основные виды МСЭ

2. Назовите виды угроз, против которых используются МСЭ

3. Предложите вариант реализации МСЭ для варианта политики ограничения использования сетевых ресурсов (доступ к одному хосту, использование или неиспользование аутентификации, возможность логгирования)

4. Предложите вариант, как с помощью журнала МСЭ можно

Тема 9. Протоколы аутентификации

1. Предложите протокол аутентификации для варианта организации системы подтверждения подлинности пользователей

2. Предложите вариант реализации системы при котором происходит /не происходит дополнительная нагрузка на сеть,

система становится / не становится чувствительна к надёжности центров аутентификации

Учебная литература, необходимая для самостоятельной подготовки к занятиям

1) Баканов В.М. Сетевые технологии: Учебное пособие. - М.: МГУПИ, 2008. - 105 с. [Электронный ресурс]: http://window.edu.ru/resource/182/58182

2) Комагоров В.П. Архитектура сетей и систем телекоммуникации: учебное пособие / В.П. Комагоров; Томский политехнический университет. - Томск: Изд-во Томского политехнического университета, 2011. - 154 с. [Электронный ресурс]: http://window.edu.ru/resource/074/79074

3) Олифер В. Г., Компьютерные сети. Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - Санкт-Петербург : Питер, 2015. - 943 с. - (Учебник для вузов). - Библиогр.: с. 917 . - Алф. указ.: с. 918

4) Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.: ил.

5) Хорев А.А. Способы и средства защиты информации. Учебн. пособие. – М.: МО РФ, 2000. – 316 с.

6) Грибунин В. Г., Чудовский В. В. Комплексная защита информации на предприятии: Учебн. пособие.- М.: Академия, 2009.- 416 с.

7) Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебн. пособие.- М.: Форум: Инфра-М, 2010.- 592 с.

8) Чепиков О. Средства аутентификации – выбор между рисками, удобством и стоимостью //Информационная безопасность. – 2004. №3

9) Применение сканеров для анализа защищенности компьютерных сетей: Материалы курса. – М.: Учебный центр «Информзащита», 2009.

10) Ньюман Д. Системы предотвращения сетевых атак //Сети. №16. – 2006.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для самостоятельной подготовки к занятиям по дисциплине

1. Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/

2. Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

3. Википедия. Свободная энциклопедия [официальный сайт]. Режим доступа: https://ru.wikipedia.org/