Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Н. Я. Великите

ПЕРЕДАЧА ДАННЫХ И СЕТЕВЫЕ ТЕХНОЛОГИИ

Учебно-методическое пособие по изучению дисциплины
для студентов специальности
10.05.03 «Информационная безопасность автоматизированных систем»,
специализация «Безопасность открытых информационных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2025

УДК 004.7(076)

Рецензент
кандидат технических наук, доцент кафедры теории машин и механизмов и деталей машин ФГБОУ ВО «Калининградский государственный технический университет» О. С. Витренко

Великите, Н. Я.
Передача данных и сетевые технологии: учебно-методическое пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем» / Н. Я. Великите. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2025. – 51 с.

Учебно-методическое пособие является руководством к изучению дисциплины «Передача данных и сетевые технологии» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». В нем представлен тематический план изучения дисциплины, содержание дисциплины по ее разделам и темам, темы практических занятий, указания к изучению каждой темы, рекомендации по выполнению практических заданий. Содержатся требования к текущей и промежуточной аттестации, определены условия получения положительной оценки.
Табл. 2, список лит. – 15 наименований

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в учебном процессе в качестве локального электронного методического материала методической комиссией института цифровых технологий 29 апреля 2025 г., протокол № 3

УДК 004.7(076)

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

В данном учебно-методическом пособии изложены основы теории передачи данных и сетевых технологий.

Целью освоения дисциплины «Передача данных и сетевые технологии» является: изучение теоретических основ передачи данных и сетевых технологий и приобретение практических навыков по построению локальных и глобальных сетей передачи данных для решения задач профессиональной деятельности.

В результате изучения передачи данных и сетевых технологий перед студентом ставятся следующие задачи: студент должен составить представление о компьютерных системах в терминах сетевых технологий, изучить стандарты передачи данных, а также уметь использовать теоретические знания в области передачи данных и сетевых технологий на практике.

В результате освоения дисциплины ожидается, что студенты получат целостное представление о широкой сфере проблем сетевых технологий и передачи данных и будут:

знать:

– историю развития, закономерности построения и функционирования компьютерных сетей и систем телекоммуникаций;

– сетевые технологии и основы построения сетевых протоколов;

– основные стандарты в области инфокоммуникационных систем и технологий;

– теоретические основы архитектурной и системотехнической организации вычислительных сетей;

уметь:

– проектировать и эксплуатировать компьютерные сети и системы телекоммуникаций;

– анализировать и выявлять причины сложных проблем, возникающих на сетевых устройствах информационно-коммуникационных систем;

– выявлять и устранять сложные инциденты, возникающие на сетевых устройствах информационно-коммуникационных систем;

– документировать предлагаемые решения;

владеть:

– навыками разработки и администрирования компьютерных сетей и систем телекоммуникаций.

Дисциплина «Передача данных и сетевые технологии» относится к Модулю «Естественнонаучный и инженерный модуль» и относится к блоку 1 обязательной части.

В учебно-методическом пособии по изучению дисциплины с практическими заданиями представлен тематический план, содержащий перечень изучаемых тем, обязательных практических работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана

на семестр следует оценивать рекомендуемое время на изучение дисциплины, возможно, вам потребует больше времени на выполнение отдельных самостоятельных заданий или проработку отдельных тем.

В разделе содержание дисциплины приведены подробные сведения об изучаемых вопросах по которым вы можете ориентироваться в случае пропуска каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки, каждая тема имеет ссылки на литературу (или иные информационные ресурсы), а также контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к промежуточной аттестации – экзамену.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделу ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную учебную группу.

2. ТЕМАТИЧЕСКИЙ ПЛАН

Тематический план изучения дисциплины «Передача данных и сетевые технологии» представлен в таблице 1.

Таблица 1 – Тематический план изучения дисциплины «Передача данных и сетевые технологии»

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объём самостоятельной работы, ч
		Лекции		
	Раздел 1.Основы передачи данных	Тема 1. Основы локальных сетей передачи данных. Описание функций сети. Модель взаимодействия устройств сети	4	3,5
		Тема 2. Введение в локальные сети. Базовая конфигурация коммутатора	4	3,5
		Тема 3. Сети Ethernet. MAC и IP-адресация. Работа протокола ARP. Принципы работы технологии Ethernet	4	3,5
		Тема 4. Устранение базовых проблем работы коммутатора	4	3,5
	Раздел 2. Сетевые технологии и сетевые протоколы	Тема 5. Понимание сетевого уровня стека TCP/IP. IP-адресация и подсети. Технология DHCP	4	3,5
		Тема 6. Понимание транспортного уровня стека TCP/IP. Описание функций маршрутизации	4	3,5
		Тема 7. Статическая и динамическая маршрутизация. Описание процесса доставки пакетов	4	3,5
		Тема 8. Технология NAT. Соединение локальной сети с сетью Internet. Управление трафиком с использованием ACL	4	3,5

			32	**28**
		Практические занятия		
		Занятие 1. Определение MAC-адреса рабочей станции различными способами	6	3,5
		Занятие 2. Определение IP-адреса, маски подсети и шлюза по умолчанию	6	3,5
		Занятие 3. Протокол ARP. Просмотр и изменение записей ARP-таблицы	6	3,5
		Занятие 4. Расчет пара-метров IP-сети	6	3,5
		Занятие 5. IP-маршрутизация. Просмотр и изменение таблицы маршрутизации	6	3,5
		Занятие 6. Протоколы транспортного уровня TCP и UDP. Номера портов	6	3,5
		Занятие 7. Локальные виртуальные сети (VLAN), магистральные (trunk) соединения между коммутаторами	6	3,5
		Занятие 8. Конфигурирование работы протокола STP	6	3,5
			48	**28**
		Рубежный (текущий) и итоговый контроль		
		Тестирование (ЭИОС)	8 (РЭ)	
		Экзамен (тест)	1,25 (КА)	
			56 (СР)	34,75 Контроль

Итого: 180

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

3.1 Раздел 1. Основы передачи данных

3.1.1 Тема 1.1 Основы локальных сетей передачи данных. Описание функций сети. Модель взаимодействия устройств сети

Перечень изучаемых вопросов

1.Определение и принципы локальных сетей

2.Топологии локальных сетей.

3. Компоненты локальной сети.

4. Протоколы и технологии

5. Модель OSI и ее уровни

6. Безопасность и защита данных.

Методические указания к изучению

В данной теме мы рассмотрим предмет и задачи дисциплины. Рассмотрим специфику, задачи обеспечения передачи данных. Ознакомимся с этапами развития теории локальных сетей передачи данных.

Изучение данной темы важно для понимания принципов работы современных компьютерных сетей, используемых как в домашних условиях, так и в крупных корпоративных инфраструктурах. Для успешного освоения материала необходимо понимать ключевые концепции сетевых технологий, такие как модели OSI и TCP/IP, функции различных уровней сети и взаимодействие между устройствами.

Для начала изучите базовые термины и понятия, относящиеся к компьютерным сетям:

– Компьютерная сеть: совокупность компьютеров и других устройств, соединенных между собой для обмена информацией.

– Топология сети: структура, определяющая физическое расположение узлов сети и способы их соединения.

– Модель OSI: семиуровневая эталонная модель взаимодействия открытых систем, используемая для описания сетевого взаимодействия.

– TCP/IP: набор протоколов, обеспечивающих передачу данных через Интернет.

Рассмотрите модель OSI, которая состоит из семи уровней:

1. Физический уровень: передача битов по физическим каналам связи.

2. Канальный уровень: управление доступом к среде передачи и формирование кадров.

3. Сетевой уровень: маршрутизация пакетов и управление адресами.

4. Транспортный уровень: обеспечение надежной доставки данных и контроль ошибок.

5. Сеансовый уровень: установление, поддержание и завершение сеансов связи.

6. Уровень представления: преобразование форматов данных.

7. Прикладной уровень: предоставление услуг пользователям и приложениям.

Изучите функции каждого уровня и взаимосвязь между ними.

Протокол TCP/IP является основным протоколом Интернета.

Изучите его архитектуру и функции:

– IP (Internet Protocol): отвечает за адресацию и маршрутизацию пакетов.

– TCP (Transmission Control Protocol): обеспечивает надежную доставку данных с контролем ошибок и управлением потоком.

– UDP (User Datagram Protocol): используется для быстрой передачи данных без гарантии доставки.

Понимание работы этих протоколов поможет вам лучше разобраться в принципах функционирования сетей.

Исследуйте, как различные устройства взаимодействуют друг с другом в рамках компьютерной сети:

– Клиент-серверная архитектура: взаимодействие между клиентом (например, компьютером пользователя) и сервером (центральным узлом).

– Пиринговая сеть (P2P): равноправное взаимодействие между участниками сети без центрального сервера.

– Маршрутизаторы: устройства, отвечающие за пересылку данных между различными сегментами сети.

– Коммутаторы: устройства, объединяющие несколько сегментов сети и обеспечивающие связь между ними.

Рекомендуемая литература: [4, ч. 1].

Контрольные вопросы для самопроверки

1. Что такое локальная сеть и каковы ее основные принципы?

2. Какие устройства могут быть частью локальной сети?

3. Что такое локальная сеть и каковы ее основные принципы?

4. Какие устройства могут быть частью локальной сети?

5. Какие типы топологий существуют для локальных сетей (звезда, кольцо, шина)?

6. Как каждая топология влияет на функционирование сети?

7. Какие основные компоненты составляют локальную сеть (серверы, рабочие станции, коммутаторы, маршрутизаторы)?

8. Какие функции выполняют каждый из этих компонентов?

9. Какие протоколы используются в локальных сетях (TCP/IP, Ethernet)

10. Как эти протоколы обеспечивают передачу и управление данными?

11. Какова модель OSI и как она используется в сетях?

12. Какие функции выполняют каждый из уровней модели OSI?

13. Какие меры безопасности применяются в локальных сетях для защиты от несанкционированного доступа?

14. Какие технологии используются для шифрования и защиты данных?

3.1.2 Тема 1.2 Введение в локальные сети. Базовая конфигурация коммутатора

Перечень изучаемых вопросов

1. Введение в локальные сети. Основные компоненты локальной сети: Сетевые карты, концентраторы, коммутаторы, маршрутизаторы.

2. Типы линий связи: Коаксиальный кабель, витая пара, оптоволоконный кабель.

3. Базовая конфигурация коммутатора. Настройка базовых параметров коммутатора: Присвоение имени, установка пароля, настройка IP-адреса Удаленное управление коммутатором: Настройка интерфейса VLAN и шлюза по умолчанию.

4. Безопасность коммутатора: Установка пароля для командного режима.

Методические указания к изучению

Изучение данной темы представляет собой первый шаг к пониманию принципов работы локальных сетей и настройке сетевого оборудования. Коммутатор (switch) играет ключевую роль в создании и управлении сетями, обеспечивая соединение между различными устройствами внутри одной сети. Правильная настройка коммутаторов необходима для обеспечения эффективной и безопасной работы сети.

Основные этапы изучения

Изучение основных терминов и понятий

Прежде всего, необходимо ознакомиться с основными терминами и понятиями, связанными с локальными сетями и коммутаторами:

– Локальная сеть (LAN): группа компьютеров и других устройств, связанных между собой в пределах одного здания или кампуса.

– Коммутатор (Switch): устройство, которое соединяет несколько устройств в одну сеть и позволяет им обмениваться данными.

– Порт коммутатора: интерфейс, через который подключаются устройства к коммутатору.

– VLAN (Virtual Local Area Network): виртуальная локальная сеть, позволяющая разделить физическую сеть на несколько логических сегментов.

– MAC-адрес: уникальный идентификатор устройства в сети.

– STP (Spanning Tree Protocol): протокол, предотвращающий петли в сетях с избыточными связями.

Изучение архитектуры и функций коммутатора

На данном этапе нужно изучить архитектуру коммутатора и его основные функции:

– Функционирование портов: как данные передаются между портами коммутатора.

– Таблица MAC-адресов: механизм, позволяющий коммутатору узнавать, какие устройства подключены к каким портам.

– Управление трафиком: методы приоритизации трафика и фильтрации нежелательных пакетов.

– Безопасность: базовые меры безопасности, такие как ограничение доступа к портам и защита от атак типа «man-in-the-middle».

Конфигурация коммутатора

Основной частью данного этапа будет изучение процесса базовой конфигурации коммутатора. Обычно процесс включает следующие шаги:

1. Подключение к коммутатору: использование консольного кабеля или Telnet/SSH для подключения к устройству.

2. Настройка интерфейсов: назначение IP-адресов и масок подсетей для управления интерфейсом.

3. Создание VLAN: разделение физической сети на несколько логических сегментов.

4. Настройка STP: активация и настройка протокола Spanning Tree для предотвращения петель в сети.

5. Безопасность: установка паролей администратора и ограничение доступа к определенным портам.

Рекомендуемая литература: [5, гл. 5].

Контрольные вопросы для самопроверки

1.Что такое локальная сеть и какие ее основные преимущества?

2. Какие топологии используются в локальных сетях и их особенности.

3. Какие основные компоненты входят в состав локальной сети?

4. Как подключить и настроить базовые параметры коммутатора?

5. Как обеспечить удаленное управление коммутатором?

6. Какие протоколы и модели используются в локальных сетях?

7. Какие меры безопасности следует принять при настройке коммутатора?

8. Какие типы кабелей используются для подключения устройств в локальной сети?

9. Какие основные протоколы используются для маршрутизации в локальных сетях?

10. Какие основные задачи решаются при помощи локальных сетей?

3.1.3 Тема 1.3 Сети Ethernet. MAC и IP-адресация. Работа протокола ARP. Принципы работы технологии Ethernet

Перечень изучаемых вопросов

1. MAC-адресация: Определение и назначение MAC-адресов. Структура MAC-адресов (48 бит, 12 шестнадцатеричных цифр). Использование MAC-адресов в локальных сетях.

2. IP-адресация: Определение и назначение IP-адресов. Структура IP-адресов (сеть и хост). Классы IP-адресов и их назначение.

3. Протокол ARP: Назначение и принцип работы протокола ARP. Процесс разрешения IP-адресов в MAC-адреса. ARP-таблицы и их типы (динамические и статические).

4.Технология Ethernet: Основные принципы работы Ethernet. Структура кадра Ethernet (MAC-адреса, EtherType, данные). Роль коммутаторов в сетях Ethernet.

5.Принципы работы Ethernet: Использование коммутаторов для маршрутизации пакетов. Таблицы MAC-адресов и их роль в коммутаторах. Скорости и методы пересылки данных в коммутаторах.

Методические указания к изучению

Тема охватывает ключевые аспекты работы сетей Ethernet, включая MAC и IP-адресацию, протокол ARP и принципы функционирования самой технологии Ethernet. Это важные знания для понимания сетевых технологий и построения локальных вычислительных сетей (LAN).

Целью является получение знаний о принципах работы сети Ethernet, способах адресации устройств в сетях, а также понимании механизмов передачи данных между устройствами с использованием протоколов ARP и Ethernet.

Перед началом изучения важно ознакомиться с основными терминами и понятиями:

1. Ethernet – технология передачи данных в компьютерных сетях, использующая кабельную инфраструктуру.

2. MAC-адрес – уникальный физический адрес устройства в сети.

3. IP-адрес – логический адрес устройства в сети, используемый для маршрутизации пакетов.

4. ARP (Address Resolution Protocol) – протокол, позволяющий преобразовывать IP-адреса в MAC-адреса.

5. Frame – кадр данных, передаваемый по сети Ethernet.

6. CSMA/CD (Carrier Sense Multiple Access with Collision Detection) – механизм управления доступом к среде передачи данных.

7. MTU (Maximum Transmission Unit) – максимальный размер кадра данных, который может быть передан через сеть.

8. Hub, Switch, Router – сетевые устройства, обеспечивающие коммутацию и маршрутизацию трафика.

Изучение основ технологии Ethernet

1. История развития технологии Ethernet.
2. Типы кабелей и топологии сети (звезда, шина, кольцо).
3. Стандарты Ethernet (10BASE-T, 100BASE-TX, Gigabit Ethernet идр.).
4. Формат кадра Ethernet (заголовок, данные, контрольная сумма).
5. Механизм CSMA/CD и его работа.

MAC-адресация

1. Что такое MAC-адрес?
2. Уникальность MAC-адресов и их назначение.
3. Как происходит отправка кадров данных с использованием MAC-адресов.
4. Таблицы коммутации (switching tables) и их роль в передаче данных.

IP-адресация

1. Основы TCP/IP модели.
2. Разница между физическим (MAC) и логическим (IP) уровнями.
3. Классы IP-адресов (A, B, C) и маски подсетей.
4. Протокол IPv4 и IPv6.
5. Динамическая и статическая IP-адресация.

Работа протокола ARP

1. Назначение протокола ARP.
2. Процесс преобразования IP-адресов в MAC-адреса.
3. Формат ARP-запросов и ARP-ответов.
4. Кэширование ARP-записей.
5. Проблемы и ограничения ARP.

Принципы работы технологии Ethernet

1. Кадры данных и процесс их передачи.
2. Коллизии и их разрешение.
3. Управление потоком данных.
4. Полудуплексный и полнодуплексный режимы работы.
5. Безопасность и аутентификация в Ethernet-сетях.

Рекомендуемая литература: [4, ч. 2].

Контрольные вопросы для самопроверки

1. В чем основное отличие между MAC-адресами и IP-адресами?
2. Как работает протокол ARP при передаче данных между устройствами в локальной сети?
3. Какие основные компоненты входят в состав кадра Ethernet?
4. Как коммутаторы Ethernet используют таблицы MAC-адресов для маршрутизации пакетов?
5. В чем состоит назначение статических записей в ARP-таблице?
6. Какие методы пересылки данных используются в коммутаторах Ethernet?
7. Какие преимущества использования Ethernet в локальных сетях?
8. Как происходит разрешение IP-адресов в MAC-адреса с помощью протокола ARP?
9. Какие типы MAC-адресов используются в сетях Ethernet (одноадресные, многоадресные, широковещательные)?
10. Какие преимущества и недостатки использования динамических и статических записей в ARP-таблице?

3.2. Раздел 2. Сетевые технологии и сетевые протоколы

3.2.1 Тема 2.1 Понимание сетевого уровня стека TCP/IP. IP-адресация и подсети. Технология DHCP

Перечень изучаемых вопросов

1. Понимание сетевого уровня стека TCP/IP.
2. IP-адресация и подсети.
3. Технология DHCP.

Методические указания к изучению

Данная тема охватывает ключевые аспекты работы сетевых протоколов на уровне сети в модели TCP/IP. Здесь вы познакомитесь с основами IP-адресации, изучите принципы деления сетей на подсети и разберетесь с технологией автоматического назначения IP-адресов – DHCP. Эти знания являются базовыми для понимания функционирования компьютерных сетей и необходимы для дальнейшего изучения сетевой архитектуры.

Понимание сетевого уровня стека TCP/IP

Стек TCP/IP – это набор протоколов, обеспечивающих связь между устройствами в сети. TCP/IP состоит из нескольких уровней, каждый из которых отвечает за определённые функции передачи данных. Сетевой уровень (или уровень интернета) отвечает за маршрутизацию пакетов от источника до получателя через сеть.

Основные протоколы сетевого уровня:

– IP (Internet Protocol) – основной протокол сетевого уровня, который обеспечивает адресацию и передачу данных по сети.

– ICMP (Internet Control Message Protocol) – используется для диагностики состояния сети и передачи сообщений об ошибках.

Ключевые моменты:

– Стек TCP/IP работает по принципу инкапсуляции данных: данные передаются в виде пакетов, содержащих заголовки каждого уровня.

– Протокол IP обеспечивает доставку данных по назначению, но не гарантирует надёжность доставки.

IP-адресация

Основы IP-адресации

IP-адрес – это уникальный идентификатор устройства в сети, состоящий из четырёх чисел, разделённых точками (например, 192.168.0.1). Существует два основных типа IP-адресов:

– IPv4 – 32-битный адрес, представленный в десятичной форме с точками.

– IPv6 – 128-битный адрес, используемый для расширения возможностей адресации.

Классы IP-адресов (для IPv4):

– Класс A: 1.0.0.0 – 126.255.255.255

– Класс B: 128.0.0.0 – 191.255.255.255

– Класс C: 192.0.0.0 – 223.255.255.255

– Специальные классы (D и E)

Маска подсети

Маска подсети определяет, какая часть IP-адреса относится к сети, а какая – к хосту. Например, маска 255.255.255.0 означает, что первые три октета относятся к сети, а последний – к хосту.

Подсети

Подсети позволяют разделить большую сеть на несколько меньших, что упрощает управление и повышает безопасность. Это достигается путём изменения маски подсети.

Технология DHCP

DHCP (Dynamic Host Configuration Protocol) – это протокол, позволяющий автоматически назначать IP-адреса устройствам в сети. Сервер DHCP выдаёт клиентам IP-адреса, маску подсети, шлюз по умолчанию и другие параметры конфигурации.

Процесс получения IP-адреса клиентом включает четыре этапа:

1. DHCPDISCOVER: Клиент отправляет широковещательное сообщение, чтобы найти сервер DHCP.

2. DHCPOFFER: Сервер DHCP предлагает клиенту свободный IP-адрес.

3. DHCPREQUEST: Клиент запрашивает предложенный IP-адрес.

4. DHCPACK: Сервер подтверждает назначение IP-адреса и отправляет дополнительные параметры конфигурации.

Рекомендуемая литература: [4, ч. 2].

Контрольные вопросы для самопроверки

1.Объясните основные различия между протоколами TCP и UDP.

2. Опишите процесс маршрутизации пакетов в сети TCP/IP.

3. Как определить, находится ли хост в одной подсети с другим хостом?

4. Приведите пример расчета подсети для заданного IP-адреса и маски подсети.

5. В чем разница между статической и динамической IP-конфигурацией? Когда лучше использовать каждую из них?

6. Какие действия предпринимает DHCP сервер при истечении срока аренды IP-адреса?

7. Почему использование IPv6 становится необходимым в современных сетях?

8. Какие проблемы могут возникнуть при неправильной настройке шлюза по умолчанию?

9. Опишите сценарий использования DHCP relay агента в сложной сети.

10. Какой тип сообщений использует клиент при запросе конфигурации от DHCP сервера?

11.Что такое стек протоколов TCP/IP? Какие уровни он включает?

12. Какова роль каждого из четырех уровней TCP/IP (прикладного, транспортного, интернет-уровня и уровня сетевого интерфейса)?

13. Чем отличаются протоколы IPv4 и IPv6? Какие преимущества предоставляет IPv6?

14. Как данные передаются через сеть с использованием TCP/IP? Что такое маршрутизация?

15.Что такое IP-адрес? Из каких частей он состоит?

16. Как работают классы IP-адресов (A, B, C)? Чем они отличаются?

17. Что такое маска подсети и как она используется для разделения сети на подсети?

18. Как рассчитать количество возможных подсетей и хостов в сети?

19. Что такое широковещательный адрес и адрес сети?

20. Какие ошибки могут возникнуть при неправильной настройке IP-адресации или маски подсети?

21. Что такое DHCP (Dynamic Host Configuration Protocol)? Для чего он используется?

22. Как работает процесс выдачи IP-адреса через DHCP (DORA – Discover, Offer, Request, Acknowledge)?

23. Какие существуют методы выделения IP-адресов в DHCP (динамическое, автоматическое и статическое распределение)?

24. Что такое DHCP lease и как осуществляется его обновление?

25. Какие преимущества предоставляет использование DHCP в больших сетях?

26. Как работают DHCP relay агенты и зачем они нужны?

3.2.2 Тема 2.2 Понимание транспортного уровня стека TCP/IP. Описание функций маршрутизации

Перечень изучаемых вопросов

1. Описание транспортного уровня стека TCP/IP.
2. Протоколы TCP и UDP.
3. Функции протокола TCP.
4. Функции протокола UDP.
5. Маршрутизация в стеке TCP/IP.
6. Протоколы маршрутизации.

Методические указания к изучению:

Транспортный уровень является одним из ключевых уровней модели TCP/IP, обеспечивающим надежную передачу данных между приложениями. Маршрутизация – процесс выбора оптимального пути передачи данных от источника до получателя через сеть. Оба эти аспекта играют важную роль в функционировании сети и обеспечивают целостность передаваемых данных.

Целью изучения данной темы является понимание принципов работы транспортного уровня и механизмов маршрутизации в сетях TCP/IP. Это включает следующие аспекты:

– Понимание назначения и функций транспортного уровня.

– Изучение протоколов транспортного уровня (TCP и UDP).

– Освоение основ маршрутизации пакетов данных в компьютерных сетях.

– Ознакомление с основными алгоритмами маршрутизации.

Транспортный уровень

1. Назначение транспортного уровня

Объясните назначение транспортного уровня в стеке TCP/IP. Опишите, какие функции он выполняет для обеспечения надежной доставки данных между приложениями.

2. Протоколы транспортного уровня

Рассмотрите два основных протокола транспортного уровня: TCP (Transmission Control Protocol) и UDP (User Datagram Protocol).

– TCP: Подробно изучите механизм надежной передачи данных с использованием подтверждения получения пакетов (ACK), контроля перегрузки и установления соединения (three-way handshake).

– UDP: Изучите особенности передачи данных без установки соединения и отсутствие гарантии доставки пакетов.

3. Порты и мультиплексирование

Поясните, какую роль играют порты в транспортных протоколах. Объясните принципы мультиплексирования и демультиплексирования данных.

4. Фрагментация и сборка пакетов

Обсудите процессы фрагментации и сборки пакетов на транспортном уровне. Каким образом осуществляется восстановление исходной последовательности данных?

Функции маршрутизации

1. Определение маршрутизации

Дайте определение маршрутизации и поясните её значение в сетевых технологиях. Опишите основные задачи, решаемые с помощью маршрутизации.

2. Маршрутизаторы и таблицы маршрутизации

Расскажите о роли маршрутизаторов в процессе передачи данных. Что такое таблица маршрутизации? Какие данные она содержит и как используется?

3. Алгоритмы маршрутизации

Изучите различные алгоритмы маршрутизации, такие как:

– Статическая маршрутизация.

– Динамическая маршрутизация.

– Протоколы маршрутизации (RIP, OSPF, BGP).

4. Метрики маршрутизации

Рассмотрим метрики, используемые для оценки качества маршрутов, такие как задержка, пропускная способность и стоимость маршрута.

5. Конвергентность и стабильность маршрутов

Определите понятия конвергентности и стабильности маршрутов. Почему важно поддерживать стабильную работу маршрутизации?

6. Управление маршрутизацией

Исследуйте методы управления маршрутизацией, включая политику маршрутизации и администрирование маршрутизаторов.

Рекомендуемая литература: [6, гл. 7].

Контрольные вопросы для самопроверки

1. Какие протоколы используются на транспортном уровне стека TCP/IP и каковы их основные функции?

2. В чем заключается основное различие между протоколами TCP и UDP? Какие приложения используют каждый из этих протоколов?

3. Как протокол TCP обеспечивает надежную доставку данных? Какие механизмы используются для восстановления после ошибок и управления потоком?

4. Какие приложения используют UDP и почему? Как UDP обрабатывает потерю пакетов и ошибки?

5. Как маршрутизация реализуется в стеке TCP/IP? Какие протоколы участвуют в маршрутизации и как они работают?

6. Опишите основные протоколы маршрутизации, такие как OSPF и RIP. Как они взаимодействуют с протоколом IP?

3.2.3 Тема 2.3 Статическая и динамическая маршрутизация. Описание процесса доставки пакетов

Перечень изучаемых вопросов

1. Статическая и динамическая маршрутизация.

2. Описание процесса доставки пакетов. Компоненты для настройки статического маршруту.

3. Таблицы маршрутизации.

Методические указания к изучению

Маршрутизация – это процесс выбора оптимального пути передачи данных между узлами сети. Она играет ключевую роль в обеспечении надежной и эффективной работы сетей, включая Интернет. Понимание принципов статической и динамической маршрутизации, а также механизма доставки пакетов является важным аспектом сетевого администрирования и разработки сетевых приложений.

1. Понимание основ маршрутизации: студенты должны уметь различать статическую и динамическую маршрутизацию, понимать принципы их работы и применять эти знания на практике.

2. Описание процесса доставки пакетов: студенты должны разбираться в процессе передачи данных через сеть, начиная от формирования пакета до его доставки получателю.

3. Применение знаний на практике: студенты должны научиться конфигурировать маршрутизаторы и управлять ими, используя полученные теоретические знания.

Основы маршрутизации

Определение маршрутизации

Маршрутизация – это процесс определения наилучшего маршрута для передачи данных от отправителя к получателю через сеть. Этот процесс включает в себя выбор наиболее эффективного пути среди множества возможных вариантов.

Статическая маршрутизация

Статическая маршрутизация подразумевает ручное добавление маршрутов в таблицу маршрутизации. Администратор вручную настраивает маршруты, указывая, каким образом данные будут передаваться между определенными сетями.

Преимущества:

– Простота настройки.

– Низкая нагрузка на процессор.

Недостатки:

– Отсутствие гибкости.

– Требует постоянного вмешательства администратора.

Динамическая маршрутизация

Динамическая маршрутизация основана на автоматическом обновлении таблицы маршрутизации в зависимости от изменений в топологии сети. Маршруты определяются с помощью специальных протоколов маршрутизации, таких как RIP, OSPF и BGP.

Преимущества:

– Автоматическое обновление маршрутов.

– Гибкость и адаптация к изменениям в сети.

Недостатки:

– Более сложная настройка.

– Повышенная нагрузка на процессор.

Процесс доставки пакетов

Формирование пакета

Передача данных в сетях осуществляется посредством передачи пакетов. Пакеты содержат заголовок, включающий адрес источника и назначения, а также полезную нагрузку (данные).

Передача пакета

Пакет передается от одного узла к другому через промежуточные устройства (маршрутизаторы). Каждый маршрутизатор принимает решение о том, куда направить пакет, основываясь на таблице маршрутизации.

Таблица маршрутизации

Таблица маршрутизации содержит информацию о возможных маршрутах и используется для принятия решений о передаче пакетов. В случае статиче-

ской маршрутизации таблица заполняется вручную, тогда как в динамической маршрутизации она обновляется автоматически.

Протоколы маршрутизации

Протоколы маршрутизации, такие как RIP, OSPF и BGP, используются для обмена информацией о маршрутах между маршрутизаторами и автоматического обновления таблиц маршрутизации.

Рекомендуемая литература: [6, гл. 5].

Контрольные вопросы для самопроверки:

1. Какие основные компоненты необходимы для настройки статического маршрута?
2. Какие протоколы динамической маршрутизации используются для построения таблиц маршрутизации?
3. В чем заключается основное преимущество статической маршрутизации в плане безопасности?
4. Как динамическая маршрутизация помогает в случае отказа одного из маршрутизаторов?

3.2.4 Тема 2.4 Технология NAT. Соединение локальной сети с сетью Internet. Управление трафиком с использованием ACL

Перечень изучаемых вопросов

1. Определение и основная функция NAT.
2. Типы NAT. Опишите статический, динамический NAT и PAT (Port Address Translation).
3. Применение NAT. Преобразование адресов. Роль NAT в подключении к Интернету. Преимущества использования NAT.
4. Управление трафиком с использованием ACL
5. Типы ACL. Настройка ACL. Применение ACL.

Методические указания к изучению

Изучение технологии NAT (Network Address Translation), её роли в соединении локальных сетей с глобальной сетью Интернет, а также принципов управления трафиком с помощью списков контроля доступа (ACL).

Данная тема охватывает три ключевых аспекта работы сетей: NAT (Network Address Translation), соединение локальных сетей с Интернетом и управление трафиком с помощью списков контроля доступа (ACL). Эти технологии являются важными элементами современных сетевых инфраструктур и используются для обеспечения безопасности, экономии IP-адресов и управления потоками данных.

После освоения данной темы вы сможете:

1. Понимать принципы работы технологии NAT и её применение в корпоративных сетях.

2. Настраивать подключение локальной сети к глобальной сети (Интернет).

3. Управлять сетевым трафиком с использованием списков контроля доступа (ACL).

4. Разбираться в вопросах безопасности и оптимизации сетевого трафика.

Основные аспекты изучения:

1. Понимание технологии NAT
   – Что такое NAT?
   – Принцип работы NAT.
   – Виды NAT (статический, динамический).
   – Преимущества и недостатки NAT.
2. Применение NAT для соединения локальной сети с Интернетом
   – Конфигурация NAT на маршрутизаторе.
   – Различия между PAT (Port Address Translation) и обычным NAT.
   – Примеры настройки NAT для различных сценариев.
3. Управление трафиком с использованием ACL
   – Определение ACL.
   – Типы ACL (стандартные и расширенные).
   – Применение ACL для фильтрации трафика.
   – Настройка ACL на маршрутизаторах и коммутаторах.

Network Address Translation – технология преобразования сетевых адресов.

Типы NAT:

– Static NAT: Статическое преобразование адресов.
– Dynamic NAT: Динамическое преобразование адресов.
– Port Address Translation (PAT): Преобразованиепортов.

Применение NAT:

– Экономия публичных IP-адресов.
– Скрытие внутренней структуры сети от внешних пользователей.
– Повышение уровня безопасности.

Управление трафиком с использованием ACL.

Access Control List – списки контроля доступа.Позволяют фильтровать пакеты на основе различных критериев (IP-адрес, протокол, порт и др.).

Типы ACL:

– Стандартные ACL (фильтрация по IP-адресу источника).

– Расширенные ACL (фильтрация по множеству параметров).

Применение ACL:

– Ограничение доступа к определённым сервисам.

– Блокировка нежелательного трафика.

– Повышение безопасности сети.

Рекомендуемая литература: [4, гл. 5].

Контрольные вопросы для самопроверки

1. Какие основные функции выполняет NAT в современных сетях?
2. Опишите разницу между статическим и динамическим NAT.
3. Как PAT (Port Address Translation) помогает в экономии IP-адресов?
4. Как NAT влияет на безопасность сети?
5. Какие преимущества и недостатки использования NAT в локальных сетях?
6. Что такое ACL и как он используется для управления трафиком?
7. Как настроить ACL для ограничения входящего трафика в сети?
8. Как NAT и ACL взаимодействуют для обеспечения безопасности и управления трафиком в сети?
9. Что такое NAT и для чего он используется?
10. Опишите статический, динамический NAT и PAT (Port Address Translation).
11. Как NAT помогает в экономии IP-адресов и обеспечении безопасности сети?
12. Как NAT преобразует внутренние (приватные) IP-адреса в внешние (публичные) и наоборот?
13. Как NAT позволяет нескольким устройствам в локальной сети подключаться к Интернету через один публичный IP-адрес?
14. Как NAT помогает решить проблему дефицита IP-адресов в IPv4?
15. Как NAT повышает безопасность и сокращает расходы на IP-адреса?
16. Что такое Access Control List (ACL) и для чего он используется?
17. Опишите основные типы ACL (входящие и исходящие списки).
18. Как настраиваются списки контроля доступа для управления трафиком в сети?
19. Как ACL помогает в ограничении доступа к определенным ресурсам сети?

4. ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

Практические занятия направлены на углубление знаний и закрепление основных понятий и методов, изучаемых в рамках дисциплины.

Основная цель занятий – научиться применять теоретические знания для решения прикладных задач.

Цель практических занятий по дисциплине: освоение и закрепление на практических занятиях основных положений теории передачи данных и сетевых технологий.

Практикум содержит 8 работ.

Практические занятия проводятся в компьютерных классах института цифровых технологий.

В результате выполнения практических работ ожидается, что студенты приобретут навыки по реализации и эксплуатации компьютерные сети и системы телекоммуникаций; анализировать и выявлять причины сложных проблем, возникающих на сетевых устройствах информационно-коммуникационных систем; выявлять и устранять сложные инциденты, возникающие на сетевых устройствах информационно-коммуникационных систем; документировать предлагаемые решения. Будут владеть навыками разработки и администрирования компьютерных сетей и систем телекоммуникаций.

Тематический план практических занятий приведён в таблице 1 .

Методические указания к изучению

1. Изучение лекционного материала и конспектов:

– Перед практическими занятиями необходимо проработать соответствующие разделы лекционного материала.

– Рекомендуется вести конспект занятий и дополнительно пересмотреть его перед началом практического занятия.

2. Проработка учебной литературы:

– Используйте основные учебники и методические пособия, рекомендованные преподавателем.

– Для глубокого понимания теории рекомендуется обращаться к дополнительной литературе.

3. Подготовка вопросов:

– Составьте список вопросов по материалу, вызвавшему затруднения.

– Обсуждение этих вопросов на практическом занятии поможет устранить пробелы в знаниях.

4. Вопросы для самоконтроля:

– Перед каждым занятием рекомендуется проверять себя с помощью вопросов для самоконтроля из методических указаний к лекционным занятиям. Это позволит оценить уровень своей подготовки.

Рекомендуется в ходе выполнения задания на практическую работу использовать доступные в компьютерном классе средства компьютеризации и электронного доступа к информационным ресурсам кафедры, сети Интернет. Подготовка отчета по выполненной практической работе осуществляется в соответствии с рекомендованной преподавателем формой отчета.

Рекомендуется прикрепить отчёт по каждой практической работе в контейнер в ЭИОС. В этой же системе можно посмотреть требования преподавателя по форме отчёта и по срокам выполнения заданий.

ПРАКТИЧЕСКИЕ ЗАНЯТИЕ № 1
Определение MAC-адреса рабочей станции различными способами

Цель работы: научиться определять физический адрес сетевого интерфейса (MAC-адрес) на различных операционных системах, используя встроенные инструменты и утилиты командной строки.

Этапы выполнения:

Определение MAC-адреса на Windows:

1. Откройте командную строку (cmd):
   – Нажмите сочетание клавиш Win + R.
   – Введите команду cmd и нажмите Enter.
2. Выполните команду:
   ipconfig /all
3. Найдите строку Physical Address – это и есть ваш MAC-адрес.

Определение MAC-адреса на Linux:

1. Откройте терминал.
2. Выполните одну из команд:

ifconfig | grep ether

Или:

ip link show

3. Найдите строку с ether или link/ether – это и есть ваш MAC-адрес.

Определение MAC-адреса через графический интерфейс:

1. Для Windows:

– Откройте Панель управления → Центр управления сетями и общим доступом.

– Выберите активное подключение и перейдите в Свойства подключения → Сведения.

– Посмотрите значение параметра Физический адрес.

Для Linux:

– Зайдите в настройки сети через графический интерфейс вашего дистрибутива.

– Перейдите в свойства активного подключения и найдите там параметр Hardware Address.

Этот практический урок поможет вам освоить базовые навыки работы с сетевыми параметрами и лучше понимать работу сетевых протоколов на уровне физического адреса.

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения в методических указаниях.

2. Выполнить задание по пунктам.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– этапы выполнения;

– ответить на контрольные вопросы.

Критерий оценки

Выполнение задания оценивается по следующим критериям:

– Правильность определения MAC-адреса на всех указанных платформах.

– Ответы на контрольные вопросы.

– Полнота и корректность описания процесса поиска MAC-адреса.

Контрольные вопросы

1. Что такое MAC-адрес?

2. Каково назначение MAC-адреса в сетях?

3. Какие команды используются для определения MAC-адреса в разных ОС?

4. Почему важно уметь находить MAC-адрес разными способами?

5. Можно ли изменить MAC-адрес? Если да, то зачем это нужно?

6. Какие существуют способы изменения MAC-адреса?

7. Чем отличается MAC-адрес от IP-адреса?

8. Где используется информация о MAC-адресе в локальной сети?

9. Как узнать MAC-адрес удалённого устройства в сети?

10. Может ли MAC-адрес использоваться для идентификации устройств в интернете?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 2
Определение IP-адреса, маски подсети и шлюза по умолчанию

Цель работы: научиться определять сетевые параметры компьютера (IP-адрес, маску подсети и шлюз по умолчанию), используя командную строку операционной системы Windows.

Этапы выполнения:

1. Открытие командной строки

– Нажмите комбинацию клавиш Win + R.

– Введите команду cmd и нажмите Enter.

2. Получение сетевых параметров

– В открывшейся командной строке выполните следующую команду:

```
ipconfig /all
```

– Эта команда выведет полную информацию обо всех сетевых интерфейсах вашего компьютера.

3. Поиск необходимых параметров

– Найдите сетевой интерфейс, который вас интересует (например, Ethernet или Wi-Fi).

– Обратите внимание на следующие параметры:

– IPv4-адрес: Это ваш локальный IP-адрес в сети.

– Маска подсети: Определяет размер вашей подсети.

– Основной шлюз: Адрес маршрутизатора, через который осуществляется доступ в Интернет.

4. Запись результатов

– Запишите значения найденных параметров в удобном формате.

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения в методических указаниях.

2. Выполнить задание по пунктам.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– этапы выполнения

– ответить на контрольные вопросы.

Критерий оценки

Оценка «Отлично»

– Студент правильно выполнил все этапы задания.

– Безошибочно определил и записал IP-адрес, маску подсети и адрес шлюза по умолчанию.

– Ответил на все контрольные вопросы без ошибок.

– Демонстрировал глубокое понимание темы.

Оценка «Хорошо»

– Задание выполнено почти без ошибок.

– Возможно допущено несколько незначительных неточностей при определении параметров или записи значений.

– Ответы на контрольные вопросы даны верно, но могли содержать небольшие ошибки или недопонимания.

Оценка «Удовлетворительно»

– Выполнены основные этапы задания, однако есть значительные ошибки.

– Определённые параметры содержат ошибки или пропуски.

– Ответы на контрольные вопросы неполные или содержат серьёзные ошибки.

Оценка «Неудовлетворительно»

– Задание выполнено с большим количеством ошибок.

– Параметры определены неверно или вовсе отсутствуют.

– Ответы на контрольные вопросы демонстрируют слабое знание материала.

Эти критерии помогут объективно оценить уровень подготовки студента и выявить области, требующие дополнительного изучения.

Контрольные вопросы

1. Что такое IPv4-адрес?

2. Каково назначение маски подсети?

3. Для чего нужен основной шлюз?

4. Какие команды можно использовать для получения сетевых параметров в Linux?

5. Какая информация выводится командой ipconfig /all?

6. Можно ли изменить IP-адрес вручную? Если да, то как это сделать?

7. Какие еще команды используются для диагностики сети в Windows?

8. Как узнать MAC-адрес устройства?

9. Чем отличается динамический IP от статического?

10. Какие дополнительные инструменты существуют для анализа сетевого трафика?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3
Протокол ARP. Просмотр и изменение записей ARP-таблицы

Цель задания: научиться просматривать и изменять записи ARP-таблицы на компьютере, а также понимать принципы работы протокола ARP в локальной сети.

Этапы выполнения:

1. Просмотр текущей ARP-таблицы

– Откройте командную строку Windows (cmd).

– Введите команду arp -a. Это позволит вам просмотреть текущие записи ARP-таблицы вашего компьютера.

– Запишите результаты вывода команды в файл или блокнот.

2. Добавление статической записи в ARP-таблицу

– Определите IP-адрес и MAC-адрес устройства в вашей сети, которому вы хотите добавить статическую запись. Например, это может быть ваш роутер.

– Используйте следующую команду для добавления статической записи:

arp -s [IP-адрес] [MAC-адрес]

Пример:

arp -s 192.168.0.1 00-11-22-33-44-55

– Проверьте, добавилась ли запись в таблицу, выполнив снова команду arp -a.

3. Удаление записи из ARP-таблицы

– Найдите динамически добавленную запись в таблице командой arp -a.

– Удалите эту запись с помощью следующей команды:

arp -d [IP-адрес]

Пример:

arp -d 192.168.0.1

– Убедитесь, что запись удалена, повторно проверив таблицу командой arp -a.

4. Очистка всей ARP-таблицы

– Очистите всю ARP-таблицу с помощью команды:

arp -d *

– Проверьте результат командой arp -a, чтобы убедиться, что таблица пустая.

5. Заполнение таблицы заново

– Перезагрузите компьютер или отключите/включите сетевой интерфейс, чтобы увидеть, как заполняется ARP-таблица автоматически при взаимодействии с устройствами в сети.

– Через несколько минут проверьте состояние таблицы командой arp -a.

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения в методических указаниях.

2. Выполнить задание по пунктам.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

–этапы выполнения

– ответить на контрольные вопросы.

Критерии оценки:

– Понимание темы: Студент демонстрирует понимание принципов работы протокола ARP и назначения ARP-таблицы.

– Выполнение этапов: Все шаги задания выполнены корректно, без ошибок.

– Анализ результатов: Способность объяснить полученные данные и результаты выполненных действий.

– Ответы на вопросы: Ответы на контрольные вопросы полные и правильные.

Контрольные вопросы

1. Что такое протокол ARP?

2. Какую роль играет ARP-таблица в работе сети?

3. Какие типы записей существуют в ARP-таблице? Опишите разницу между ними.

4. Почему важно уметь управлять ARP-записями?

5. Каковы возможные причины очистки ARP-таблицы?

6. Какие команды используются для просмотра, добавления, удаления и очистки ARP-таблицы?

7. Как вручную добавить статическую запись в ARP-таблицу?

8. Какие проблемы могут возникнуть при наличии неправильных записей в ARP-таблице?

9. Можно ли использовать ARP для атак типа «ARP-spoofing»? Если да, то как?

10. Как проверить, изменилась ли запись в ARP-таблице после внесения изменений?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 4
Расчет параметров IP-сети

Цель работы: научиться рассчитывать параметры IP-сети (сетевую маску, диапазон адресов сети, широковещательные адреса), используя различные классы сетей и CIDR-нотацию.

Этапы выполнения:

1. Теоретическая подготовка:

– Повторение основ работы IP-протокола (IPv4).

– Изучение классов сетей (A, B, C) и CIDR-нотации.

– Понимание принципов расчёта сетевой маски, диапазона адресов сети и широковещательного адреса.

2. Практические вычисления:

– Рассчитать сетевые параметры для заданного IP-адреса и маски.

– Проверить корректность полученных результатов с помощью онлайн-калькуляторов.

3. Документирование:

– Заполнить таблицу с результатами расчетов.

– Описать ход решения задач и пояснить каждый шаг.

Задание

1. Вам выдано несколько заданий, каждое содержит один IP-адрес и соответствующую маску. Например:

– IP-адрес: 192.168.0.10, маска: /24

– IP-адрес: 172.16.15.20, маска: /22

– IP-адрес: 10.50.25.30, маска: /18

2. Для каждого задания выполните следующие шаги:

– Определите класс сети.

– Переведите маску в десятичную форму.

– Найдите сетевой адрес.

– Определите первый и последний возможные адреса хостов.

– Укажите широковещательный адрес.

3. Результаты оформите в виде таблицы, где столбцы будут содержать:

– Номер задания,

– Класс сети,

– Маска в десятичной форме,

– Сетевой адрес,

– Диапазон адресов хостов,

– Широковещательный адрес.

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения в методичке.

2. Выполнить задание.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– выполнение задания по пунктам

– ответить на контрольные вопросы

Критерии оценки

1. Правильность расчётов: Все параметры рассчитаны верно (сетевая маска, диапазон адресов, широковещательный адрес).

2. Полнота оформления: Таблица заполнена правильно, включены все необходимые данные.

3. Логика решений: Описание хода решения показывает понимание процесса расчёта.

4. Грамотность: Отсутствие ошибок в оформлении текста и таблиц.

5. Ответы на контрольные вопросы.

Контрольные вопросы

1. Что такое сетевая маска?

2. Какие существуют классы сетей IPv4? В чём их различия?

3. Как рассчитать диапазон адресов хостов для заданной сети?

4. Что такое широковещательный адрес и как его определить?

5. В чём заключается разница между маской в формате CIDR и десятичным представлением?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5
IP-маршрутизация. Просмотр и изменение таблицы маршрутизации

Цель работы: научиться просматривать и изменять таблицу маршрутизации на устройствах под управлением операционных систем семейства Linux и Windows. Изучить команды и принципы работы с таблицей маршрутизации.

Этапы выполнения:

1. Просмотр текущей таблицы маршрутизации

– Windows:

route print

– Linux:

ip route show

описание:

Используйте указанные команды для просмотра текущих маршрутов на вашем устройстве. Обратите внимание на структуру вывода: интерфейс, шлюз, метрика и другие параметры.

2. Добавление маршрута вручную

– Windows:

route add 192.168.0.0 mask 255.255.255.0 192.168.10.1 metric 20

– Linux:

sudo ip route add 192.168.0.0/24 via 192.168.10.1 dev eth0

Описание:

Добавьте новый статический маршрут для сети 192.168.0.0/24 через шлюз 192.168.10.1. В случае с Windows также указана метрика маршрута (metric 20), а в Linux – интерфейс устройства (dev eth0).

3. Удаление маршрута

– Windows:

route delete 192.168.0.0

– Linux:

sudo ip route del 192.168.0.0/24

Описание:

Удалите добавленный ранее маршрут. Важно помнить, что после удаления маршруты будут восстановлены автоматически только в случае динамической маршрутизации.

4. Проверка изменений

Повторите команду просмотра маршрутов (route print или ip route show) и убедитесь, что изменения были внесены корректно.

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения в методических указаниях.

2. Выполнить задание по пунктам.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– этапы выполнения

– ответить на контрольные вопросы.

Критерии оценки

1. Правильность выполнения этапов:

– Успешный просмотр текущей таблицы маршрутизации.

– Правильное добавление нового маршрута.

– Верная команда удаления маршрута.

– Проведение проверки внесенных изменений.

2. Понимание принципов маршрутизации:

– Ответы на контрольные вопросы демонстрируют понимание базовых концепций IP-маршрутизации и работы с таблицами маршрутизации.

3. Аккуратность и внимательность:

– Отсутствие ошибок в синтаксисе команд.

– Четкое выполнение всех шагов задания.

4. Дополнительные баллы:

– Использование расширенного функционала команд (например, указание метрики или интерфейсов).

– Дополнительные исследования и эксперименты с различными параметрами маршрутизации.

Таким образом, данное практическое задание позволяет закрепить знания о работе с таблицей маршрутизации и приобрести практические навыки в этой области.

Контрольные вопросы

1. Что такое таблица маршрутизации?

2. Какие команды используются для просмотра таблицы маршрутизации в Windows и Linux?

3. Как добавить статический маршрут в Windows и Linux?

4. Для чего используется параметр metric в команде добавления маршрута в Windows?

5. Чем отличается синтаксис команд управления маршрутизацией в Windows и Linux?

6. Какие интерфейсы участвуют в маршрутах и зачем нужно указывать их в командах?

7. Почему важно правильно настроить маршрутизацию в сети?

8. Какие дополнительные параметры могут использоваться при настройке маршрутов?

9. Что произойдет, если неправильно указать шлюз или маску сети при добавлении маршрута?

10. Какие существуют способы автоматической настройки маршрутизации?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 6
Протоколы транспортного уровня TCP и UDP. Номера портов

Цель работы: изучение принципов работы протоколов TCP и UDP, понимание назначения номеров портов и их роли в сетевых коммуникациях.

Определение характеристик протокола:

– Определите, какой протокол используется для передачи файлов (например, HTTP, FTP), и почему выбран именно этот протокол.

– Объясните, какие номера портов используются стандартно для этих протоколов.

Работа с утилитами диагностики сети:

– Используйте команду netstat или аналогичную утилиту для просмотра активных соединений на вашем компьютере.

– Проанализируйте вывод команды и определите, какие приложения используют TCP и UDP соединения.

– Найдите и объясните назначение портов, используемых этими приложениями.

Создание простого сервера и клиента:

– Напишите простую программу на Python (или другом языке программирования), реализующую сервер и клиент на основе TCP или UDP.

– Протестируйте работу программы, передавая данные между клиентом и сервером.

– Обсудите преимущества и недостатки выбранного протокола для вашей реализации.

Анализ результатов:

– Подготовьте отчет, включающий:

– Описание выполненной работы.

– Результаты анализа сетевой активности.

– Код написанной программы и пояснения к нему.

– Выводы относительно выбора протокола и использования номеров портов.

Защита работы:

– Представьте результаты своей работы перед преподавателем или группой.

– Ответьте на вопросы, касающиеся выбранной темы.

Критерии оценки

1. Понимание теоретического материала: правильность ответов на контрольные вопросы, глубина понимания темы.

2. Качество практической части: корректность написания программы, успешная передача данных между клиентом и сервером.

3. Анализ и выводы: полнота отчета, наличие обоснованных выводов и рекомендаций.

4. Презентация и защита: умение ясно и структурированно представить свою работу, отвечать на дополнительные вопросы.

Контрольные вопросы

1. В чем основное различие между протоколами TCP и UDP?

2. Какие типы приложений чаще всего используют TCP? А UDP?

3. Что такое номер порта и зачем он нужен?

4. Как вы определяли активные соединения и используемые порты на своем компьютере?

5. Почему вы выбрали тот или иной протокол для своей программы?

6. Какие проблемы могут возникнуть при передаче данных через UDP? Как их избежать?

7. Как обеспечивается надежность передачи данных в TCP?

8. Назовите стандартные номера портов для популярных сервисов (HTTP, SSH, DNS).

9. Можно ли использовать один и тот же порт для разных приложений одновременно? Если да, то при каких условиях?

10. Каковы основные шаги установления TCP-соединения (handshake)?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №
Локальные виртуальные сети (VLAN), магистральные (trunk) соединения между коммутаторами

Цель работы: познакомиться с принципами работы VLAN и научиться настраивать их на коммутаторах, а также освоить настройку trunk-соединений для передачи трафика нескольких VLAN через одно физическое соединение.

Этапы выполнения:

1. Подготовка оборудования

Убедитесь, что у вас есть доступ к коммутатору Cisco или другому оборудованию, поддерживающему работу с VLAN и trunk-соединениями. В случае отсутствия физического оборудования можно использовать симуляторы сетевого оборудования, такие как Packet Tracer или GNS3.

2. Создание VLAN

Настройте два VLAN на одном коммутаторе:

– Создайте VLAN с номером 10 и назовите его Sales.

– Создайте VLAN с номером 20 и назовите его Marketing.

Используйте следующие команды на интерфейсе командной строки (CLI):

```
Switch(config)# vlan 10
Switch(config-vlan)# name Sales
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name Marketing
Switch(config-vlan)# exit
```

3. Назначение портов коммутаторов в VLAN

Назначьте порты коммутатора в соответствующие VLAN:

– Порты FastEthernet0/1 и FastEthernet0/2 — в VLAN 10 (Sales).

– Порт FastEthernet0/3 — в VLAN 20 (Marketing).

Для этого выполните следующие команды:

```
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit

Switch(config)# interface FastEthernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit

Switch(config)# interface FastEthernet0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit
```

4. Настройка trunk-соединения

Настройте trunk-соединение между двумя коммутаторами на портах GigabitEthernet0/1. Этот интерфейс будет передавать трафик обоих VLAN.

На первом коммутаторе выполните:

```
Switch1(config)# interface GigabitEthernet0/1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# end
```

На втором коммутаторе:

```
Switch2(config)# interface GigabitEthernet0/1
Switch2(config-if)# switchport mode trunk
Switch2(config-if)# end
```

5. Проверка конфигурации

Проверьте правильность настройки VLAN и trunk-соединений с помощью команд:

– Просмотрите список настроенных VLAN:

Switch#show vlan brief

– Убедитесь, что trunk-порт корректно передает данные всех VLAN:

Switch#show interfaces trunk

6. Тестирование связи

Подключите устройства к соответствующим портам и убедитесь, что устройства внутри одного VLAN могут общаться друг с другом, но не могут обмениваться данными с устройствами из другого VLAN.

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения в методических указаниях.

2. Выполнить задание по пунктам.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– этапы выполнения

– ответить на контрольные вопросы.

Критерии оценки:

– Полнота выполнения задания: Все шаги выполнены согласно инструкции.

– Правильность настройки: VLAN созданы и назначены на правильные порты, trunk-соединение работает корректно.

– Умение проверять конфигурацию: Использованы команды для проверки правильности настроек.

– Понимание принципов работы: Ответы на контрольные вопросы показывают понимание темы.

Контрольные вопросы

1. Что такое VLAN? Каковы преимущества использования VLAN?

2. Какие типы портов существуют в контексте VLAN: access и trunk? Чем они отличаются?

3. Как настроить порт коммутатора в режим access и назначить его в определенный VLAN?

4. Как правильно настроить trunk-порт для передачи трафика нескольких VLAN?

5. Какие команды используются для проверки настроек VLAN и trunk-соединений?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 8
Конфигурирование работы протокола STP

Цель работы: научиться конфигурированию протокола Spanning Tree Protocol (STP) на коммутаторах Cisco для предотвращения петель в сети Ethernet и обеспечения отказоустойчивости сетевой инфраструктуры.

Этапы выполнения:

1. Подготовка оборудования:

– Убедитесь, что у вас есть доступ к лабораторному оборудованию или симулятору сетей (например, Cisco Packet Tracer).

– Подключите три коммутатора между собой через порты FastEthernet0/1–FastEthernet0/3.

2. Настройка базовых параметров:

– Задайте IP-адреса на всех устройствах.

– Включите VLANs и назначьте интерфейсы соответствующим VLAN'ам.

3. Активация STP:

– Активируйте протокол STP на всех коммутаторах командой spanning-tree mode pvst.

– Проверьте статус STP командой show spanning-tree.

4. Определение корневого моста:

– Настройте один из коммутаторов как корневой мост с помощью команды spanning-tree vlan x root primary, где x — номер VLAN.

– Проверяйте изменения в топологии STP после настройки.

5. Оптимизация конфигурации:

– Измените приоритет коммутаторов для выбора резервного корневого моста.

– Используйте команду spanning-tree portfast для ускорения активации портов.

6. Проверка работоспособности:

– Создайте виртуальные машины и подключите их к разным VLAN'ам.

– Проведите пинг-тесты между машинами для проверки связности сети.

7. Документирование результатов:

– Запишите все выполненные команды и результаты проверок.

– Сделайте выводы о работе STP и его влиянии на сеть.

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения в методических указаниях.

2. Выполнить задание по пунктам.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– этапы выполнения;

– ответить на контрольные вопросы.

Критерии оценки:

– Полнота выполнения задания: Все этапы выполнены корректно и последовательно.

– Правильность настроек: Отсутствие ошибок в конфигурациях устройств.

– Результативность: Сеть функционирует согласно заданной топологии.

– Документация: Подробный отчет с командами и результатами тестов.

– Анализ и выводы: Грамотные объяснения принципов работы STP и влияния настроек на сеть.

Контрольные вопросы

1. Что такое STP и зачем он нужен?

2. Какие существуют режимы работы STP? В чём их различия?

3. Как выбрать корневой мост в сети?

4. Какие параметры влияют на выбор корневого порта?

5. Для чего используется команда spanning-tree portfast?

6. Опишите процесс пересчета топологии STP при изменении состояния портов.

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОЙ ПОДГОТОВКЕ

Внеаудиторная самостоятельная работа в рамках данной дисциплины включает в себя:

• подготовку к аудиторным занятиям (лекциям, практическим занятиям) и выполнение соответствующих заданий;

• самостоятельную работу над отдельными темами учебной дисциплины в соответствии с тематическим планом;

• подготовку к экзамену.

Подготовка к лекционным занятиям

При подготовке к лекции рекомендуется повторить ранее изученный материал, что дает возможность получить необходимые разъяснения преподавателя непосредственно в ходе занятия. Рекомендуется вести конспект, главное требование к которому быть систематическим, логически связанным, ясным и кратким. По окончанию занятия обязательно в часы самостоятельной подготовки, по возможности в этот же день, повторить изучаемый материал и доработать конспект.

Подготовка к практическим занятиям

Подготовка к практическим занятиям предусматривает:

• изучение теоретических положений по изучаемой теме;

• детальную проработку учебного материала, рекомендованной литературы и методической разработки на предстоящее занятие.

Самостоятельная работа над отдельными темами учебной дисциплины:

При организации самостоятельного изучения ряда тем лекционного курса обучаемый работает в соответствии с указаниями, выданными преподавателем. Указания по изучению теоретического материала курса составляются дифференцированно по каждой теме и включают в себя следующие элементы: название темы; цели и задачи изучения темы; основные вопросы темы; характеристику основных понятий и определений, необходимых обучаемому для усвоения данной темы; список рекомендуемой литературы; наиболее важные фрагменты текстов рекомендуемых источников, в том числе таблицы, рисунки, схемы и т.п.; краткие выводы, ориентирующие обучаемого на определенную совокупность сведений, основных идей, ключевых положений, систему доказательств, которые необходимо усвоить; контрольные вопросы, предназначенные для самопроверки знаний.

Подготовка к экзамену

При подготовке к экзамену большую роль играют правильно подготовленные заранее записи и конспекты. В этом случае остается лишь повторить пройденный материал, учесть, что было пропущено, восполнить пробелы, закрепить ранее изученный материал.

В ходе самостоятельной подготовки к экзамену при анализе имеющегося теоретического и лабораторного материала студенту также рекомендуется проводить постановку различного рода задач по изучаемой теме, что поможет в дальнейшем выявлять критерии принятия тех или иных решений, причины совершения определенного рода ошибок. При ответе на вопросы, поставленные в ходе самостоятельной подготовки, обучающийся вырабатывает в себе способность логически мыслить, искать в анализе событий причинно-следственные связи.

Вопросы и задачи для самоподготовки

ЗАДАЧА 1

Настройте простую локальную сеть дома или в лаборатории.

Используйте инструменты диагностики сети, такие как ping, traceroute и nslookup.

Исследуйте конфигурационные файлы сетевых устройств и протоколов.

ЗАДАЧА 2

Создание простой локальной сети с использованием коммутатора.

– Настройку VLAN и проверку работы сегментов сети.

– Применение базовых мер безопасности, таких как изменение пароля администратора и отключение неиспользуемых портов.

ЗАДАЧА 3

1. Создать схему небольшой Ethernet-сети, включающей несколько компьютеров, коммутатор и маршрутизатор.

2. Определить IP-адреса и маски подсетей для каждого устройства.

3. Смоделировать процесс передачи данных от одного компьютера к другому с использованием ARP.

4. Построить таблицу коммутации для коммутатора.

ЗАДАЧА 4

Практическое задание:

– Рассчитайте диапазон IP-адресов для заданной сети с использованием маски подсети.

– Определите, какие части IP-адреса относятся к сети и хосту.

Пример:

Для сети класса C (192.168.1.0/24) с маской подсети 255.255.255.224:

– Количество подсетей: ____

– Количество хостов в каждой подсети: ____

Практическое задание:

– Разделите заданную сеть на подсети с указанным количеством хостов.

– Рассчитайте диапазоны IP-адресов для каждой подсети.

ЗАДАЧА 5

1. Настройка маршрутизатора

Настройте виртуальный маршрутизатор (например, используя Cisco Packet Tracer или другой симулятор) для реализации статической и динамической маршрутизации.

2. Анализ трафика

Проведите анализ сетевого трафика с использованием Wireshark или аналогичного инструмента. Определите типы пакетов, передающихся по сети, и проследите процесс их маршрутизации.

3. Моделирование сети

Создайте простую топологию сети и смоделируйте передачу данных между узлами. Отслеживайте маршруты следования пакетов и исследуйте влияние различных факторов на выбор маршрута.

ЗАДАЧА 6

1. Настройка Static NAT:

– Выбрать два устройства: одно будет имитировать внутреннюю сеть, другое – внешнюю.

– Установить статический маршрут между устройствами.

– Создать правила NAT для преобразования внутренних IP-адресов во внешние.

2. Настройка Dynamic NAT:

– Использовать пул IP-адресов для динамического назначения внешним устройствам.

– Применять ACL для ограничения доступа к определённым ресурсам.

3. Анализ работы NAT:

– Отслеживание пакетов с помощью утилит вроде Wireshark или tcpdump.

– Проверка корректности работы правил NAT через ping и traceroute.

Подключение локальной сети к Интернету

Подключение через роутер:

– Роль маршрутизатора в соединении локальной сети с глобальной.

– Настройка DHCP-сервера для автоматической раздачи IP-адресов внутри локальной сети.

Безопасность подключения:

– Использование межсетевых экранов (firewalls).

– Применение VPN-технологий для шифрования передаваемых данных.

Маршрутизация:

– Принципы работы протоколов маршрутизации (например, RIP, OSPF, BGP).

– Настройка статической и динамической маршрутизации.

1. Настройка маршрутизатора:

– Конфигурация интерфейсов WAN и LAN.

– Назначение внешнего IP-адреса и настройка DNS-серверов.

2. Тестирование соединения:

– Проведение тестов скорости интернета.

– Анализ работы сетевой инфраструктуры с помощью SNMP-мониторинга.

3. Диагностика проблем:

– Решение возможных ошибок соединения с помощью команд ping, tracert и nslookup.

Вопросы для самоподготовки

1. Что такое компьютерная сеть? Какие бывают типы сетей?

2. В чём разница между локальной сетью (LAN), глобальной сетью (WAN) и Metropolitan Area Network (MAN)?

3. Объясните принцип работы протокола TCP/IP. Каковы его основные функции?

4. Чем отличается маршрутизация от коммутации? Приведите примеры устройств, выполняющих эти функции.

5. Что такое IP-адрес? Как классифицируются IPv4 и IPv6 адреса?

6. Что такое доменное имя и система DNS? Как происходит разрешение имен?

7. Опишите уровни модели OSI. Каково назначение каждого уровня?

8. Как работает протокол HTTP/HTTPS? Какие преимущества имеет HTTPS перед HTTP?

9. Что такое Wi-Fi и как он функционирует? Какие существуют стандарты беспроводной связи?

10. Объясните принципы шифрования данных. Какие алгоритмы используются чаще всего?

11. В чём заключается разница между VPN и прокси-сервером?

12. Что такое облачные вычисления? Какие виды облаков вы знаете?

13. Что такое файрволл? Для чего он нужен и какие функции выполняет?

14. Объясните разницу между проводными и беспроводными технологиями передачи данных.

15. Что такое топология сети? Какие топологии наиболее распространены?

16. Какие существуют методы управления доступом к среде передачи данных?

17. Что такое QoS (Quality of Service)? Какие механизмы используются для обеспечения качества обслуживания?

18. Что такое виртуализация сетей? Какие её основные преимущества?

19. Что такое контент-фильтрация? Какие способы фильтрации контента вы знаете?

20. Объясните, как работают антивирусные программы и системы обнаружения вторжений (IDS).

21. Что такое маршрутизатор и коммутатор? Как они взаимодействуют друг с другом?

22. Что такое широковещательная рассылка и многоадресная рассылка? Когда они применяются?

23. Что такое NAT (Network Address Translation)? Каковы его основные цели и применение?

24. Что такое туннелирование? Как оно используется в сетях?

25. Что такое аутентификация и авторизация? Какие методы используются для реализации этих процессов?

26. Что такое шифрование симметричным ключом и асимметричным ключом? В каких случаях применяется каждый метод?

27. Что такое DHCP и ARP? Как они функционируют?

28. Что такое DDoS атака? Какие меры защиты от неё существуют?

29. Что такое SDN (Software Defined Networking)? Какие возможности она предлагает?

30. Что такое VLAN? Каковы её основные цели и использование?

31. Что такое протокол RIP и OSPF? Как они различаются?

32. Что такое SNMP? Как он используется для мониторинга и управления сетями?

33. Что такое Power over Ethernet (PoE)? Какова его роль в современных сетях?

34. Что такое MPLS? Как она используется в телекоммуникационных сетях?

35. Что такое IGP и EGP? В чём их отличие?

36. Что такое технология 5G? Какие новые возможности она привносит в передачу данных?

37. Что такое сеть Интернет вещей (IoT)? Какие вызовы и перспективы связаны с этой технологией?

38. Что такое VoIP? Как эта технология используется для передачи голосовых данных через интернет?

39. Что такое BYOD (Bring Your Own Device)? Какие проблемы безопасности возникают при внедрении такой политики?

40. Что такое IPSec? Как он обеспечивает безопасность данных в сетях?

41. Что такое WPA и WEP? В чём их различия и недостатки?

42. Что такое потоковая передача данных? Какие технологии используются для потокового вещания?

6. КОНТРОЛЬ И АТТЕСТАЦИЯ

Критерии оценки результатов освоения дисциплины

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100-балльную/процентную систему и правило перевода оценок в пятибалльную систему (таблица 2).

Таблица 2 – Система оценок и критерии выставления оценки

Система оценок / Критерий	2	3	4	5
	0–40 %	**41–60 %**	**61–80 %**	**81–100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
1 Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно-корректно связывать между собой (только некоторые из которых может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект
2 Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3 Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно-корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые	В состоянии осуществлять научно-корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации,	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает

Система оценок / Критерий	2	3	4	5
	0–40 %	41–60 %	61–80 %	81–100 %
	«неудовлетворительно»	«удовлетворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
	из имеющихся у него сведений		вовлекает в исследование новые релевантные задаче данные	в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4 Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/не зачтено («зачтено» – 41–100 % правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» – менее 40 % правильных ответов; оценка «удовлетворительно» – от 41 до 60 % правильных ответов; оценка «хорошо» – от 61 до 80 % правильных ответов; оценка «отлично» – от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

Задание открытого и закрытого типа приведены в ФОС (приложении к рабочему модулю).

Типовые контрольные задания и иные материалы, необходимые для оценки результатов освоения дисциплин модуля (в том числе в процессе освоения), а также методические материалы, определяющие процедуры этой оценки приводятся в приложении к рабочей программе модуля. Оценивание результатов обучения проводится с применением электронного обучения, дистанционных образовательных технологий.

7. СПИСОК ЛИТЕРАТУРЫ

Основная литература

1. Иванова, С. М. Теория информации. Хранение и передача данных: учеб. пособие / С. М. Иванова, З. В. Ильиченкова. – Москва: РТУ МИРЭА, 2022. – 75 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/256583 (дата обращения: 07.12.2024). – Текст : электронный

2. Баланов, А. Н. Цифровое понимание. Создание, влияние и будущее технологий: учебник для вузов / А. Н. Баланов. – Санкт-Петербург: Лань, 2024. – 452 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/417800 (дата обращения: 10.07.2024). – ISBN 978-5-507-49416- 3. – Текст : электронный.

3. Хабаров, С. П. Основы моделирования беспроводных сетей. Среда OMNeT++: учеб. пособие / С. П. Хабаров. – Санкт-Петербург: Лань, 2022. – 260 с. – Режим доступа: для авториз. пользователей. – Лань : электроннобиблиотечная система. – URL: https://e.lanbook.com/book/206681 (дата обращения: 03.12.2024). – ISBN 978-5-8114-3658-3. – Текст : электронный

4. Васин, Н. Н. Технологии пакетной коммутации: учебник / Н. Н. Васин. – Санкт-Петербург: Лань, 2022. – 284 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/207083 (дата обращения: 10.07.2024). – ISBN 978-5-8114-3866- 2. – Текст : электронный.

5. Пуговкин, А. В. Основы построения инфокоммуникационных сетей и систем: учеб. пособие для вузов / А. В. Пуговкин, Д. А. Покаместов, Я. В. Крюков. – 2-е изд., перераб. и доп. – Санкт-Петербург: Лань, 2021. – 176 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/156402 (дата обращения: 10.07.2024). – ISBN 978-5-8114- 5905-6. – Текст : электронный.

Дополнительная литература

6. Истратова, Е. Е. Информационные сети. Основы передачи данных: учеб. пособие / Е. Е. Истратова, И. Н. Томилов. – Новосибирск: НГТУ, 2023. – 68 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/404681 (дата обращения: 10.07.2024). – ISBN 978-5-7782-4909-7. – Текст : электронный.

7. Сетевые технологии: учеб. пособие / А. В. Коротких, Л. В. Бунина, Д. А. Аминев, А. П. Титов. – Москва: РТУ МИРЭА, 2024. – 79 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/420971 (дата обращения: 26.07.2024). – ISBN 978-5-7339-2149-5. – Текст : электронный.

8. Васин, Н. Н. Сетевые технологии: учебник / Н. Н. Васин. – Самара: ПГУТИ, 2019. – 265 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/223364 (дата обращения: 10.07.2024). – Текст : электронный.

9. Информационные технологии. Базовый курс: учебник для вузов / А. В. Костюк, С. А. Бобонец, А. В. Флегонтов, А. К. Черных. – 3-е изд., стер. – Санкт-Петербург: Лань, 2021. – 604 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/180821 (дата обращения: 10.07.2024). – ISBN 978-5-8114-8776-9. – Текст : электронный.

10. Бражук, А. И. Сетевые средства Linux / А. И. Бражук. – 2-е изд., исправ. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 148 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=428794 (дата обращения: 03.12.2024). – Текст : электронный.

11. Гладких, А. А. Развитие сетевых технологий и сети нового поколения: учеб. пособие с описанием комплекса лабораторных работ / А. А. Гладких. – Ульяновск: Ульяновский государственный технический университет, 2017. – 124 с. – Режим доступа: для авторизир. пользователей. – Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/106114.html (дата обращения: 03.12.2024). – ISBN 978-5-9795-1657-8. – Текст : электронный.

Учебно-методические пособия по дисциплине

12. Скворцова, Т. И. Компьютерные коммуникации и сети: учеб.-метод. пособие / Т. И. Скворцова. – Москва: РТУ МИРЭА, 2020. 223 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/163825 (дата обращения: 07.12.2024). – Текст : электронный

13. Лысиков, А. А. Учебно-методические рекомендации по выполнению практических работ по дисциплине «Пакетные сети передачи данных»: учебно-методическое пособие / А. А. Лысиков, Е. В. Глушак. – Самара: ПГУТИ, 2023. – 28 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/411785 (дата обращения: 07.12.2024). – Текст : электронный.

14. «ГОСТ Р 56205-2014/IEC/TS 62443-1-1:2009. Национальный стандарт Российской Федерации. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели» (утв. и введен в действие Приказом Росстандарта от 10.11.2014 N 1493-ст) (в действующей редакции). – Режим доступа: для ав-

ториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

15. «ГОСТ Р МЭК 62443-2-1-2015. Национальный стандарт Российской Федерации. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики» (утв. и введен в действие Приказом Росстандарта от 22.06.2015 N 774-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

Локальный электронный методический материал

Наталья Яронимо Великите

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 3,6. Печ. л. 3,2.

Издательство федерального государственного бюджетного
образовательного учреждения высшего образования
«калининградский государственный технический университет»
236022, Калининград, Советский проспект, 1