

МИНОБРНАУКИ РОССИИ

**Филиал федерального государственного бюджетного образовательного
учреждения высшего образования
«ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» в г. Находке
(ФИЛИАЛ ФГБОУ ВО «ВВГУ» В Г. Находке)**

**РАБОЧАЯ ПРОГРАММА
УЧЕБНОЙ ДИСЦИПЛИНЫ**

ОП.11 Компьютерные сети

программы подготовки специалистов среднего звена
09.02.07 Информационные системы и программирование

Форма обучения: *очная*

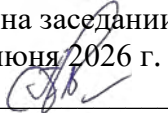
Находка 2026

Рабочая программа учебной дисциплины *ОП.11 Компьютерные сети* разработана в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности / профессии *09.02.07 Информационные системы и программирование* утвержденного приказом Минобрнауки России от *09.12.2016 № 1547*, *примерной образовательной программой*.

Разработчик(и): Вайтулевич М.В. преподаватель ОСПО филиала ФГБОУ ВО «ВВГУ» в г. Находке

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № 10 от «29» июня 2026 г.

Председатель ЦМК  Плахотина В.В.

СОДЕРЖАНИЕ

**1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
УЧЕБНОЙ ДИСЦИПЛИНЫ**

2 СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

3 УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

**4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
УЧЕБНОЙ ДИСЦИПЛИНЫ**

1. Общие сведения

1.1. Общая характеристика программы учебной дисциплины

По государственному образовательному стандарту среднего профессионального образования дисциплина «Компьютерные сети» включена в профессиональный учебный цикл общепрофессиональных дисциплин (ОП.11)

1.2. Цель и планируемые результаты освоения дисциплины:

В результате освоения дисциплины формируются компетенции:

Код	Умения	Знания
ОК 1 ОК 2 ОК 4 ОК 5 ОК 9 ОК 10 ПК 5.3 ПК 6.1 ПК 6.5 ПК 7.1 ПК 7.2 ПК 7.3	Организовывать и конфигурировать компьютерные сети; Строить и анализировать модели компьютерных сетей; Эффективно использовать аппаратные и программные компоненты компьютерных сетей при решении различных задач; Выполнять схемы и чертежи по специальности с использованием прикладных программных средств; Работать с протоколами разных уровней (на примере конкретного стека протоколов: TCP/IP, IPX/SPX); Устанавливать и настраивать параметры протоколов; Обнаруживать и устранять ошибки при передаче данных.	Основные понятия компьютерных сетей: типы, топологии, методы доступа к среде передачи; Аппаратные компоненты компьютерных сетей; Принципы пакетной передачи данных; Понятие сетевой модели; Сетевую модель OSI и другие сетевые модели; Протоколы: основные понятия, принципы взаимодействия, различия и особенности распространенных протоколов, установка протоколов в операционных системах; Адресацию в сетях, организацию межсетевого воздействия.

2. Структура и содержание учебной дисциплины

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем учебной дисциплины	70
Работа обучающихся во взаимодействии с преподавателем	68
в том числе:	
теоретическое обучение	34
практические занятия	34
Консультации	-
Самостоятельная работа	2
Итоговая аттестация в форме: дифференцированного зачета – 3 семестр.	

2.2. Тематический план и содержание учебной дисциплины «ОП.11 Компьютерные сети»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	5
	Содержание учебного материала	2	
Введение	Содержание учебного материала: учебная дисциплина «Компьютерные сети», ее основные задачи и связь с другими дисциплинами. Роль и место знаний по дисциплине в сфере профессиональной деятельности. История развития вычислительных сетей. Назначение компьютерных сетей. Основные проблемы и перспективы развития компьютерных сетей.	2	ОК 1 ОК 2 ОК 4 ОК 5 ОК 9 ОК 10 ПК 5.3 ПК 6.1 ПК 6.5 ПК 7.1 ПК 7.2 ПК 7.3
Раздел 1. Локальные сети		50	
Тема 1.1 Основные принципы построения компьютерных сетей	Содержание учебного материала: принципы централизованной и распределенной обработки данных. Системы «терминал-хост». Обобщенная структура компьютерной сети. Классификация компьютерных сетей. Функциональные типы компьютерных сетей: локальные, глобальные, корпоративные. Типы глобальных сетей. Характеристика процесса передачи данных. Режимы и коды передачи данных. Синхронная и асинхронная передача данных. Оценка качества коммуникационной сети.	4	ОК 1 ОК 2 ОК 4 ОК 5 ОК 9
	Практическое занятие 1: произвести компрессия данных, используя разные варианты (практическая работа №1).	2	ОК 10 ПК 5.3
	Практическое занятие 2: провести анализ компьютерных сетей (практическая работа №2).	2	ПК 6.1 ПК 6.5
	Самостоятельная работа обучающихся: проработать и проанализировать конспекты занятий, учебной и специальной литературы. Выполнить обобщенную структуру компьютерной сети с использованием прикладных программных средств. Сделать анализ классификации компьютерных сетей.	1	ПК 7.1 ПК 7.2 ПК 7.3

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	5
Тема 1.2 Сетевые архитектуры	Содержание учебного материала: организация сетей различных типов. Типы сетей: одноранговые, серверные, гибридные. Архитектура «клиент-сервер». Типы серверов: файловые, печати, приложений, сообщений, баз данных.	2	ОК 1 ОК 2 ОК 4 ОК 5
	Практическое занятие 3: проанализировать структуру компьютерных сетей, архитектура «клиент-сервер». Рассмотреть типы серверов: файловые, печати, приложений, сообщений, баз данных.	2	ОК 9 ОК 10
	Самостоятельная работа обучающихся: проработка конспектов, учебной и специальной литературы. Подготовить доклады по темам «Типы серверов», «Топология сети».	1	ПК 5.3 ПК 6.1 ПК 6.5 ПК 7.1 ПК 7.2 ПК 7.3
Тема 1.3 Технологии локальных сетей	Содержание учебного материала: базовые технологии локальных сетей: Ethernet, ArcNet, Token. Ограничения для сетей ArcNet и Token Ring.	2	ОК 1 ОК 2 ОК 4 ОК 5 ОК 9
	Практическое занятие 4: рассмотреть базовую технологию Ethernet (практическая работа №3). Составить таблицу по стандартам IEEE 802.x. Подготовить сообщения на темы «Технология Gigabit Ethernet», «Технология 100VG-AnyLAN».	2	ОК 10 ПК 5.3 ПК 6.1 ПК 6.5 ПК 7.1 ПК 7.2 ПК 7.3

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	5
Тема 1.4 Аппаратные компоненты компьютерных сетей	Содержание учебного материала: проводные и беспроводные компьютерные сети. Физическая передающая среда локальной вычислительной сети: коаксиальный кабель, витая пара, оптоволокно. Стандарты кабелей. Беспроводные каналы и их характеристики. Сетевые адаптеры. Функции и характеристики сетевых адаптеров. Классификация сетевых адаптеров. Драйверы сетевых адаптеров. Коммуникационное оборудование сетей: концентраторы, мосты, коммутирующие мосты, маршрутизаторы, шлюзы, их назначение, основные функции и параметры. Аналоговые и цифровые выделенные телефонные линии. Модемы: назначение, виды, характеристики. Протоколы модуляции, коррекции ошибок, сжатия данных. Программное обеспечение поддержки модемной связи. Подключение и настройка модема.	4	ОК 1 ОК 2 ОК 4 ОК 5 ОК 9 ОК 10 ПК 5.3 ПК 6.1 ПК 6.5 ПК 7.1 ПК 7.2 ПК 7.3
	Практическое занятие 5: разобраться с подключением и настройкой сетевого адаптера; подключением и настройкой модема	2	
	Практическое занятие 6: рассмотреть разновидности мостов: назначение, виды, функции, монтаж, обслуживание; коммутаторов: назначение, виды, функции, монтаж, обслуживание; концентраторов: принцип работы, монтаж, обслуживание. Подготовить сообщение на тему «Беспроводная технология Wi-Fi». Составить сводную таблицу сетевых кабелей.	3	
Тема 1.5 Сетевые модели	Содержание учебного материала: понятие «открытая архитектура». Семиуровневая модель взаимодействия открытых систем (OSI). Характеристика уровней взаимодействия модели OSI. Принципы пакетной передачи данных. Модель TCP/IP. Основные понятия TCP/IP. Характеристика уровней модели TCP/IP.	4	ОК 1 ОК 2 ОК 4 ОК 5 ОК 9 ОК 10 ПК 5.3 ПК 6.1 ПК 6.5 ПК 7.1 ПК 7.2 ПК 7.3

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	5
Тема 1.6 Протоколы	Содержание учебного материала: протоколы: основные понятия и принципы взаимодействия. Стеки протоколов. Стандартные стеки коммуникационных протоколов: OSI, IPX/SPX, TCP/IP, NetBIOS. Принцип работы протоколов. Протоколы сетевого уровня: IP, IPX, RIP, NLSP. Характеристика и применение протоколов сетевого уровня. Протоколы транспортного уровня UDP и TCP, их характеристика и применение. Установка протокола TCP/IP в операционных системах.	4	ОК 1 ОК 2 ОК 4 ОК 5 ОК 9 ОК 10 ПК 5.3 ПК 6.1 ПК 6.5 ПК 7.1 ПК 7.2 ПК 7.3
	Практическое занятие 7: рассмотреть и проанализировать протоколы, принципы взаимодействия; протоколы транспортного уровня UDP и TCP. Составить сводную таблицу по стекам протоколов. Подготовить презентацию по настройке протокола TCP/IP в операционной системе Windows XP Pro.	3	
Тема 1.7 Адресация в сетях	Содержание учебного материала: адресация в IP-сетях. Форматы IP-адресов и их преобразование. Разделение сети: подсети и маски подсетей. Адресация подсетей. Реализация архитектуры подсетей. Определение маски подсети. Реализация IP-маршрутизации. Процесс маршрутизации. Определение IP-адресов. Организация доменов и доменных имен. Определение имен узлов. Службы формирования имен узлов (DNS). Имена NetBIOS. Протокол динамической конфигурации узла (DHCP). Служба определения имен Интернета (WINS).	2	ОК 1 ОК 2 ОК 4 ОК 5 ОК 9 ОК 10 ПК 5.3 ПК 6.1 ПК 6.5 ПК 7.1 ПК 7.2 ПК 7.3
	Практическое занятие 8: определить номер сети и узла по IP-адресу и маске (практическая работа №4). Составить и проанализировать таблицу классов сетей. Подготовить сообщения по темам «Сервер DNS» и «Сервер DHCP».	4	

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	5
Тема 1.8 Межсетевое взаимодействие	Содержание учебного материала: принципы объединения сетей на основе протоколов сетевого уровня. Настройка протокола ТСР/IP в операционных системах. Применение диагностических утилит протокола ТСР/IP. Организация межсетевого взаимодействия. Протоколы маршрутизации. Фильтрация пакетов. Функции маршрутизатора. Сетевой шлюз. Брандмауэр. Принципы объединения сетей на основе протоколов сетевого уровня. Настройка протокола ТСР/IP в операционных системах. Применение диагностических утилит протокола ТСР/IP.	2	ОК 1 ОК 2 ОК 4 ОК 5 ОК 9 ОК 10 ПК 5.3 ПК 6.1 ПК 6.5
	Практическое занятие 9: настройка протокола ТСР/IP в операционных системах. Работа с диагностическими утилитами протокола ТСР/IP. Решение проблем с ТСР/IP. Промежуточное тестирование. Рассмотреть обзор программных средств защиты компьютерных сетей. Подготовить сводную таблицу по командам, применяемым при диагностике протокола ТСР/IP.	4	ПК 7.1 ПК 7.2 ПК 7.3
Раздел 2 Глобальные сети		18	
Тема 2.1 Основные понятия	Содержание учебного материала: организация виртуальных каналов информационного обмена. Протокол X.25. Характеристика уровней протокола. Достоинства и недостатки сетей X.25. Схема конструкции «IP поверх несущего протокола». Протокол Frame Relay: назначение и общая характеристика. Использование сетей Frame Relay. Технология ATM (Asynchronous Transfer Mode). Основные принципы технологии ATM. Соотношение уровней сервиса и типов трафика сети ATM. Передача трафика IP через сети ATM.	4	ОК 1 ОК 2 ОК 4 ОК 5 ОК 9 ОК 10 ПК 5.3 ПК 6.1 ПК 6.5
	Практическое занятие 10: рассмотреть работу модема на коммутируемых аналоговых линиях. Проанализировать и разобраться со схемой организации виртуального канала между двумя компьютерами глобальной сети.	4	ПК 7.1 ПК 7.2 ПК 7.3

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Осваиваемые элементы компетенций
1	2	3	5
Тема 2.2 Информационные ресурсы Интернет и протоколы прикладного уровня	Содержание учебного материала: протоколы уровня приложений. Различия и особенности распространенных протоколов. Протокол эмуляции удаленного терминала Telnet. Концепция сетевого виртуального терминала. Согласование параметров взаимодействия. Симметрия связи «терминал-процесс». Программа-клиент Telnet. Удаленный доступ через промежуточную сеть. Электронная почта: формат, почтовые клиенты, протоколы. Протоколы SMTP, POP3, IMAP. Их характеристика, назначение и отличие. Почтовая программа Outlook Express. Настройка программы почтового клиента. Протоколы распределенных файловых систем: FTP, Gopher, NNTP. Протокол пересылки гипертекста HTTP. Web-браузеры.	4	ОК 1 ОК 2 ОК 4 ОК 5 ОК 9 ОК 10 ПК 5.3 ПК 6.1 ПК 6.5
	Практическое занятие 11: разобраться с настройкой удаленного доступа к компьютеру с помощью модема. Рассмотреть работу программы Outlook Express. Разобраться с настройками и свойствами Web-браузера. Итоговое тестирование.	6	ПК 7.1 ПК 7.2 ПК 7.3
ИТОГО часов		70	
Теоретические занятия		34	
Практические занятия		34	
Самостоятельная работа		2	

3. Условия реализации учебной дисциплины

3.1. Для реализации программы учебной дисциплины «ОП.11 Компьютерные сети» образовательной организации, предусмотрено наличие следующих специальных помещений:

Учебная аудитория для проведения учебных занятий (уроки, лекции, практические занятия, лабораторные занятия, семинарские занятия, курсовое проектирование), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Кабинет информатики. Лаборатория программного обеспечения и сопровождения компьютерных систем (ауд 1410).

Компьютерные столы 33 шт., стулья 35 шт., автоматизированные рабочие места обучающихся - сетевые терминалы LG 23CAV42K 32 шт., стол для преподавателя 1 шт., автоматизированное рабочее место преподавателя, экран, мультимедийный проектор, маркерная доска 1 шт., маркерная доска 1 шт.

Помещение для самостоятельной работы обучающихся (ауд 1406)

Рабочие места на базе вычислительной техники с установленным офисным пакетом с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации. а также комплектом оборудования для печати: персональные компьютеры; посадочных мест – 30 шт. Стол преподавателя -

1 шт;

Стул преподавателя - 1 шт; Доска маркерная - 1 шт; Мультимедийный проектор с экраном

3.2. Информационное обеспечение реализации программы

Для реализации программы учебной дисциплины библиотечный фонд образовательной организации укомплектован печатными и электронными изданиями.

Основная литература:

1. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч.

Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2024. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/452574>

2. Карташевский, В.Г., Лихтциндер, Б.Я., Киреева, Н.В., Буранова, М.А. Компьютерные сети [Электронный ресурс] : Учебник /.— Самара : Изд-во ПГУТИ, 2025. — 267 с. : ил. — Режим доступа: <https://lib.rucont.ru/efd/565102>

3. Кузин, А. В. Компьютерные сети [Электронный ресурс]: Учебное пособие / Кузин А.В., Кузин Д.А. - 4-е изд., перераб. и доп. - Москва: Форум, НИЦ ИНФРА-М, 2025. - 192 с. Режим доступа: <https://znanium.com/catalog/product/536468>.

Дополнительная литература:

1. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч.

Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2024. — 351 с. — (Профессиональное образование). — ISBN 978-5-534-04635-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/453065>

2. Замятина, О. М. Инфокоммуникационные системы и сети. Основы моделирования : учебное пособие для среднего профессионального образования / О. М. Замятина. — Москва : Издательство Юрайт, 2024. — 159 с. — (Профессиональное образование). — ISBN 978-5534-10682-4. — Текст : электронный // ЭБС Юрайт [сайт]. —

URL: <https://urait.ru/bcode/456799>

3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита

программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 20205. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449548>

Интернет-ресурсы:

1. <http://www.ccc.ru> – архив журнала о компьютерных сетях и телекоммуникационных технологиях
2. http://www.sd-company.su/sd_base_xp/jurnals/other_network.php - все о компьютерных сетях
3. <http://psbatishev.narod.ru/internet/11.htm> - информация о глобальной сети Интернет.
4. <http://mir.it-karma.ru/set-internet/lekcii/struktura-i-osnovnye-principy-raboty-seti-internet> - Структура и основные принципы работы сети Интернет
5. https://ru.qwe.wiki/wiki/Computer_network - все о компьютерной сети
6. http://edu.tltsu.ru/er/book_view.php?book_id=218&page_id=2840 – лекции о компьютерных сетях

4. Контроль и оценка результатов освоения дисциплины

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися типовых индивидуальных заданий.

Результаты обучения	Критерии оценки	Методы оценки
Перечень умений, осваиваемых в рамках дисциплины: • Организовывать и конфигурировать компьютерные сети • Строить и анализировать модели компьютерных сетей • Эффективно использовать аппаратные и программные компоненты компьютерных сетей при решении различных задач • Работать с протоколами разных уровней • Устанавливать и настраивать параметры протоколов • Проверять правильность передачи данных • Обнаруживать и устранять ошибки при передаче данных	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками.	Устный опрос. Тестирование. Оценка решения ситуационных задач. Правильное выполнение практических заданий. Анализ способностей обучающегося к поиску различных нестандартных приемов решения задач. Практические занятия Внеаудиторная самостоятельная работа. Дифференцированный зачет
Перечень знаний, осваиваемых в рамках дисциплины: • Основные понятия компьютерных сетей: типы, топологии, методы доступа к среде передачи • Аппаратные компоненты компьютерных сетей; принципы пакетной передачи данных • Понятие сетевой модели • Сетевую модель OSI и другие сетевые модели • Протоколы: основные понятия, принципы взаимодействия, различия и особенности распространения протоколов, установка протоколов в операционных системах • Адресацию в сетях, организацию межсетевого воздействия	«Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с основным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Вопросно-ответная беседа с целью выявления способностей к поиску и использованию информации, необходимой для выявления эффективного выполнения задач.

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля и промежуточной аттестации
по учебной дисциплине
ОП.11 Компьютерные сети

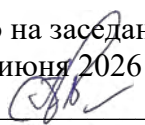
программы подготовки специалистов среднего звена /
квалифицированных рабочих и служащих

09.02.07 Информационные системы и программирование

Форма обучения: очная

Контрольно-оценочные средства для проведения текущего контроля и промежуточной аттестации по учебной дисциплине *ОП.11 Компьютерные сети* разработана в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности / профессии *09.02.07 Информационные системы и программирование* утвержденного приказом Минобрнауки России от 09.12.2016 № 1547, примерной образовательной программой, рабочей программой учебной дисциплины.

Разработчик(и): Вайтулевич М.В. преподаватель ОСПО филиала ФГБОУ ВО «ВВГУ» в г. Находке

Рассмотрено и одобрено на заседании цикловой методической комиссии
Протокол № 10 от «29» июня 2026 г.
Председатель ЦМК  Плахотина В.В.

1 Общие сведения

Контрольно-оценочные средства (далее – КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины *ОП.11 Компьютерные сети*.

КОС включают в себя контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине, которая проводится в форме дифференцированного зачёта.

2 Планируемые результаты обучения по дисциплине, обеспечивающие результаты освоения образовательной программы

Код ОК, ПК	Код результата обучения	Наименование результата обучения
ОК 01 ОК 02	31	создание компьютерных программ в современных концепциях программирования
	32	особенности и возможности языка программирования Python и области его применения
	33	основы функционального программирования на языке Python
	34	основы объектно-ориентированного программирования на языке Python
	35	базовые элементы языка Python
	У1	составлять алгоритмы для решения задач и реализовывать эти алгоритмы на компьютере в виде программ, написанных на языке Python
	У2	работать в интерактивной среде программирования и использовать её основные возможности для отладки и тестирования программ
	У3	создавать и отлаживать несложные приложения на языке программирования Python
	У4	использовать важнейшие стандартные структуры данных

3 Соответствие оценочных средств контролируемым результатам обучения

3.1 Средства, применяемые для оценки уровня практической подготовки

Краткое наименование раздела (модуля) / темы дисциплины	Код результата обучения	Показатель овладения результатами обучения	Наименование оценочного средства и представление его в КОС	
			Текущий контроль	Промежуточная аттестация
Раздел 1. Искусство программирования				
Тема 1.1. Введение в дисциплины	31	Способность создать простейшие программы с помощью языка программирования Python	Устный опрос (п. 5.1, вопросы 1-3) ⁵	Вариант 1 тест (п. 6.1) ⁵
	35	Способность оперировать операциями ввод-вывода	Устный опрос (п. 5.1, вопросы 4-7) Реферат (п. 5.2, темы 1-7)	Вариант 2 тест (п. 6.1)
	У1	Способность создавать программы в интерактивной среде разработки	Тест № 1 (п.5.3, варианты 1-3)	Практическое задание к экзамену 1 (...)
	У2	Способность организовывать работу в среде разработки	Вариант 2 тест (п. 6.1)	
Тема 1.2.	32	Способность создавать и манипулировать переменными	Контрольная работа № 1	

Основные элементы программиро- вания	У1	Способность использовать логические операторы и операторы сравнения	(п.5.4, задания 1 3)	Практическое задание к экзамену 1 (...)
	У3	Способность использовать встроенные функции Python		
Тема 1.3. Практическая работа	32	Способность создавать компьютерные программы	Конспект (чего)	Вопросы на экзамен 9-14 (п. 6.1)
	У1	Способность работы с консольным интерфейсом	Устный опрос (п. 5.1, вопросы 1-3) ⁵	Вариант 1 тест (п. 6.1) ⁵
	У2	Способность оперировать операциями ввод-вывода	Устный опрос (п. 5.1, вопросы 4-7)	Вариант 2 тест (п. 6.1)
Тема 1.4. Как писать программы	33	Способность использовать циклы и функции при написании программ	Тест № 1 (п.5.3, варианты 1-3)	Вариант 1 тест (п. 6.1) ⁵
	У1	Способность использовать функциональный подход в программировании	Вариант 2 тест (п. 6.1)	Вариант 2 тест (п. 6.1)
	У4	Способность устанавливать различные модули и пакеты	Контрольная работа № 1	Вариант 1 тест (п. 6.1) ⁵
Тема 1.5. Сложные типы данных	35	Способность использовать встроенные структуры данных	Устный опрос (п. 5.1, вопросы 1-3) ⁵	Вариант 2 тест (п. 6.1)
	У2	Способность создавать списки, кортежи и словари с помощью языка программирования Python	Устный опрос (п. 5.1, вопросы 4-7) Реферат (п. 5.2,	Вариант 1 тест (п. 6.1) ⁵
	У3	Способность оперировать методами множеств	Тест № 1 (п.5.3, варианты 1-3)	Вариант 2 тест (п. 6.1)
Тема 1.6. Работа с файлами	32	Способность работать с файлами в рамках программы	Вариант 2 тест (п. 6.1)	Вариант 1 тест (п. 6.1) ⁵
	У1	Способность читать и записывать данные в файл	Контрольная работа № 1	Вариант 2 тест (п. 6.1)
	У2	Способность работать с бинарными файлами	Устный опрос (п. 5.1, вопросы 1-3) ⁵	Вариант 1 тест (п. 6.1) ⁵
Тема 1.7. Работа над ошибками	35	Способность обрабатывать ошибки при написании программы	Устный опрос (п. 5.1, вопросы 4-7)	Вариант 2 тест (п. 6.1)
	У2	Способность создавать конструкции try-except-finally	Тест № 1 (п.5.3, варианты 1-3)	Вариант 1 тест (п. 6.1) ⁵
	У3	Способность обработки исключений	Вариант 2 тест (п. 6.1)	Вариант 2 тест (п. 6.1)
Тема 1.8. Регулярные выражения	33	Способность использовать регулярные выражения при написании программ	Контрольная работа № 1	Вариант 1 тест (п. 6.1) ⁵
	У1	Способность использовать функции модуля re	Устный опрос (п. 5.1, вопросы 1-3) ⁵	Вариант 2 тест (п. 6.1)
	У4	Способность создавать флаги для регулярных выражений	Устный опрос (п. 5.1, вопросы 4-7) Реферат (п. 5.2,	Вариант 1 тест (п. 6.1) ⁵
Тема 1.9. Элементы функциональ- ного программиро- вания	33	Способность создавать функции	Тест № 1 (п.5.3,	Вариант 2 тест
	У1	Способность использовать функции и lambda-функции	Вариант 2 тест (п. 6.1)	Вариант 1 тест (п. 6.1) ⁵
	У2	Способность каррировать функции, использовать вложенные функции	Контрольная работа № 1	Вариант 2 тест (п. 6.1)
Тема 1.10. Объектно- ориентирован- ное	34	Способность проектировать программу в соответствии с ООП	Устный опрос (п. 5.1, вопросы 1-3) ⁵	Вариант 1 тест (п. 6.1) ⁵
	У1	Способность использовать классы и объекты	Устный опрос (п. 5.1, вопросы 4-7)	Вариант 2 тест (п. 6.1)

программирование	У2	Способность использовать принципы ООП при написании программ	Устный опрос (п. 5.1, вопросы 1-3) ⁵	Вариант 1 тест (п. 6.1) ⁵
Тема 1.11. Практическая работа	32	Создание консольной игры с помощью ООП	Устный опрос (п. 5.1, вопросы 4-7) Реферат (п. 5.2,	Вариант 2 тест (п. 6.1)
Тема 1.12. Объектно-ориентированный дизайн	32	Способность создавать программы по принципам SOLID	Тест № 1 (п.5.3, варианты 1-3)	Вариант 1 тест (п. 6.1) ⁵
	У1	Способность обеспечивать взаимосвязи между классами внутри программы	Вариант 2 тест (п. 6.1)	Вариант 2 тест (п. 6.1)
	У2	Способность работать с классами и объектами	Контрольная работа № 1	Вариант 1 тест (п. 6.1) ⁵
Тема 1.13. Практическая работа	32	Способность следовать принципам ООП	Устный опрос (п. 5.1, вопросы 1-3) ⁵	Вариант 2 тест (п. 6.1)
	У1	Способность работать в абстрактными классами	Устный опрос (п. 5.1, вопросы 4-7)	Вариант 1 тест (п. 6.1) ⁵
Тема 1.14. Сложность алгоритмов	32	Способность применять асимптотический анализ	Тест № 1 (п.5.3, варианты 1-3)	Вариант 2 тест (п. 6.1)
	У1	Способность применять линейный и бинарный поиск	Вариант 2 тест (п. 6.1)	Вариант 1 тест (п. 6.1) ⁵
	У2	Способность обрабатывать предельное поведение функций	Контрольная работа № 1	Вариант 2 тест (п. 6.1)
Тема 1.15. Рекурсия	32	Способность применять рекурсивные алгоритмы	Устный опрос (п. 5.1, вопросы 1-3) ⁵	Вариант 1 тест (п. 6.1) ⁵
	У1	Способность подсчета факториала	Устный опрос (п.	Вариант 2 тест
	У2	Способность использовать сортировку слиянием	Тест № 1 (п.5.3, варианты 1-3)	Вариант 1 тест (п. 6.1) ⁵
Тема 1.16. Связный список	32	Способность применять связные списки	Вариант 2 тест (п. 6.1)	Вариант 2 тест (п. 6.1)
	У1	Способность использования связных списков в рамках программы	Контрольная работа № 1	Вариант 1 тест (п. 6.1) ⁵
Тема 1.17. Стек и очереди	32	Способность использовать стек и его операции	Устный опрос (п. 5.1, вопросы 1-3) ⁵	Вариант 2 тест (п. 6.1)
	У1	Способность реализовывать очередь	Устный опрос (п. 5.1, вопросы 4-7)	Вариант 1 тест (п. 6.1) ⁵
	У2	Способность реализовывать операции очереди	Тест № 1 (п.5.3, варианты 1-3)	Вариант 2 тест (п. 6.1)
Тема 1.18. Практическая работа	У4	Способность писать программы с использованием различных типов данных	Вариант 2 тест (п. 6.1)	Вариант 1 тест (п. 6.1) ⁵
Тема 1.19. Практическая работа	У3	Способность писать программы с использованием стека и очереди	Контрольная работа № 1	Вариант 2 тест (п. 6.1)

4 Описание процедуры оценивания

Результаты обучения по дисциплине, уровень сформированности компетенций оцениваются по четырём бальной шкале оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Текущая аттестация по дисциплине проводится с целью систематической проверки достижений обучающихся. Объектами оценивания являются: степень усвоения теоретических знаний, уровень овладения практическими умениями и навыками по всем видам учебной работы, качество выполнения самостоятельной работы, учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине).

При проведении промежуточной аттестации оценивается достижение студентом запланированных по дисциплине результатов обучения, обеспечивающих результаты освоения образовательной программы в целом.

Критерии оценивания письменной работы

(оценочные средства: практическая работа).

5 баллов - студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Проблема раскрыта полностью, выводы обоснованы. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент владеет навыком самостоятельной работы по заданной теме; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно.

4 балла - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Проблема раскрыта. Не все выводы сделаны и/или обоснованы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы.

3 балла - студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы. Проведен анализ проблемы без привлечения дополнительной литературы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы.

2 балла - работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Проблема не раскрыта. Выводы отсутствуют. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии выставления оценки студенту на зачете/ экзамене

(оценочные средства: практическая работа)

Оценка по промежуточной аттестации	Характеристика качества сформированности компетенций
«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций на продвинутом уровне: обнаруживает всестороннее, систематическое и глубокое знание учебного материала, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций на базовом уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности,

	затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на пороговом уровне: имеет знания только основного материала, но не усвоил его деталей, в ходе контрольных мероприятий допускаются значительные ошибки, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, при оперировании знаниями и умениями при их переносе на новые ситуации.
«не зачтено» / «неудовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже порогового: выявляется полное или практически полное отсутствие знаний значительной части программного материала, студент допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, умения и навыки не сформированы.

5. Примеры оценочных средств для проведения текущей аттестации

5.1 Примеры заданий для выполнения практических работ:

1. Дайте определение компьютерной сети. Опишите её назначение, основные преимущества и примеры использования в организации.
2. Опишите классификацию компьютерных сетей по территориальному охвату. Сравните PAN, LAN, MAN и WAN. Приведите примеры.
3. Что такое топология сети? Сравните топологии «шина», «звезда», «кольцо», «дерево» и «ячеистая сеть». Какая топология наиболее распространена в современных офисных сетях?
4. Назовите и характеризуйте активное и пассивное сетевое оборудование. В чём заключается их различие?
5. Опишите семь уровней эталонной модели OSI. Для каждого уровня укажите основные функции и приведите примеры протоколов или устройств.
6. Сравните модели OSI и TCP/IP. Назовите уровни TCP/IP и объясните, почему именно эта модель используется в реальных сетях.
7. Сравните MAC-адрес и IP-адрес. Для чего нужен каждый из них и в каких случаях они используются?
8. Объясните структуру IPv4-адреса. Что такое маска подсети, адрес сети, адрес узла, широковещательный адрес и шлюз по умолчанию?
9. Какие IPv4-адреса называются частными? Назовите диапазоны частных адресов, объясните их назначение и роль NAT.
10. Для сети 192.168.20.0/24 необходимо создать минимум шесть подсетей. Определите новый префикс, маску, количество доступных узлов и первые шесть подсетей.
11. Сравните статическую настройку IP-адресов и DHCP. В каких случаях следует использовать каждый способ?
12. Что такое DNS? Опишите, как компьютер получает IP-адрес сайта по его доменному имени.
13. Объясните функции маршрутизатора. Что такое шлюз по умолчанию и почему компьютер не сможет выйти в Интернет без правильно настроенного шлюза?
14. Что такое таблица маршрутизации? Рассмотрите записи ниже и объясните, куда будет направлен пакет для адресов 192.168.1.50, 10.10.5.20 и 8.8.8.8.

192.168.1.0/24 — напрямую через интерфейс LAN
10.10.0.0/16 — через шлюз 192.168.1.2
0.0.0.0/0 — через шлюз 192.168.1.1

15. Сравните концентратор (hub) и коммутатор (switch). Почему концентраторы практически не применяются в современных сетях?
16. Что такое VLAN? Объясните, как VLAN помогает разделить сеть организации и повысить уровень безопасности.
17. Опишите принцип работы беспроводной сети Wi-Fi. Назовите основные угрозы Wi-Fi и меры защиты.
18. Сравните протоколы TCP и UDP. Приведите примеры задач, в которых предпочтительно использовать каждый из них.
19. Что такое сетевой порт? Объясните различие между IP-адресом, портом и сокетом. Назовите распространённые номера портов.
20. Сравните HTTP и HTTPS. Почему современным сайтам требуется HTTPS и что делает протокол TLS?
21. Опишите устройство витой пары. Назовите стандарты T568A и T568B, объясните различие прямого и кроссового кабелей.
22. Опишите назначение команд ipconfig, ping, tracert и nslookup в Windows. Составьте пример последовательности диагностики, если компьютер не открывает сайт.

23. Что такое межсетевой экран? Назовите основные правила безопасной настройки сети организации.
24. Что такое VPN? Опишите основные сценарии применения VPN, преимущества и ограничения технологии.
25. Предложите схему сети для офиса на 25 сотрудников. В офисе есть компьютеры, Wi-Fi, сетевой принтер, файловый сервер и IP-камеры. Опишите оборудование, адресацию и правила сегментации.
26. Компьютер пользователя не открывает сайты. Значок сети показывает подключение, но доступ в Интернет отсутствует. Опишите подробный алгоритм поиска неисправности.
27. Зачем был создан IPv6? Сравните IPv4 и IPv6, приведите пример IPv6-адреса и объясните его основные преимущества.
28. Что такое QoS? Почему качество обслуживания особенно важно для IP-телефонии, видеоконференций и онлайн-обучения?
29. Для чего нужен мониторинг компьютерной сети? Какие показатели необходимо контролировать и какие средства можно использовать?
30. Разработайте концепцию защищённой сети для учебного заведения, в котором есть администрация, преподаватели, компьютерные классы, серверы, Wi-Fi, камеры и гостевой доступ. Опишите логическую структуру, меры защиты и порядок администрирования.

5.1 Ключи к заданиям для практических работ

Ответ 1

Компьютерная сеть — это система взаимосвязанных устройств, предназначенная для передачи, обработки и совместного использования информации. В состав сети могут входить персональные компьютеры, ноутбуки, серверы, смартфоны, принтеры, коммутаторы, маршрутизаторы, точки доступа Wi-Fi, IP-камеры, системы хранения данных и другие цифровые устройства. Соединение между ними может быть проводным — по витой паре или оптоволоконному кабелю — либо беспроводным, например через Wi-Fi.

Главная цель создания компьютерной сети заключается в организации обмена данными между пользователями и устройствами. Благодаря сети сотрудники могут работать с общими документами, использовать единый принтер, получать доступ к базам данных, обмениваться электронной почтой, подключаться к образовательной платформе или использовать корпоративные сервисы. Без сети каждому пользователю пришлось бы хранить документы только на своём компьютере и передавать файлы вручную, например через флеш-накопитель.

К основным преимуществам компьютерных сетей относятся совместное использование ресурсов, быстрый обмен данными, централизованное управление пользователями, резервное копирование и контроль доступа. Например, в колледже на сервере могут храниться учебные материалы, электронные журналы, документы администрации и резервные копии. Преподаватели получают доступ к своим ресурсам, студенты — к образовательной информации, а системный администратор управляет учётными записями и правами пользователей.

Компьютерная сеть позволяет подключить организацию к Интернету через единый канал связи. Также она обеспечивает работу систем видеонаблюдения, IP-телефонии, удалённого доступа, сетевых хранилищ и облачных сервисов. При правильной настройке сеть делает работу организации быстрее, удобнее и безопаснее.

Таким образом, компьютерная сеть является не просто набором соединённых компьютеров. Это важная информационная инфраструктура, от которой зависит работа сотрудников, доступ к данным,

связь с внешними сервисами и защита информации. Основы сетевых технологий включают изучение устройств, протоколов, адресации и среды передачи данных.

Ответ 2

Компьютерные сети классифицируют по территориальному охвату, то есть по расстоянию между подключёнными устройствами. Наиболее распространёнными видами являются PAN, LAN, MAN и WAN. Каждый тип сети применяется для решения разных задач и использует разные технологии связи.

PAN — Personal Area Network, персональная сеть. Она действует на небольшом расстоянии вокруг одного пользователя, обычно в пределах нескольких метров. Примером PAN является подключение беспроводных наушников к смартфону по Bluetooth, синхронизация фитнес-браслета с телефоном, соединение ноутбука с мышью или передача файлов между мобильными устройствами. Такие сети обычно создаются автоматически и не требуют сложного сетевого оборудования.

LAN — Local Area Network, локальная вычислительная сеть. Она объединяет устройства в пределах квартиры, офиса, компьютерного класса, этажа, здания или небольшого кампуса. Примером LAN является сеть учебного кабинета, в которой компьютеры подключены к коммутатору, а затем к маршрутизатору и Интернету. В локальных сетях чаще всего применяются Ethernet и Wi-Fi. LAN отличается высокой скоростью передачи данных и принадлежит одной организации или владельцу.

MAN — Metropolitan Area Network, городская сеть. Она соединяет несколько локальных сетей в пределах города или крупной агломерации. Например, у образовательной организации могут быть несколько корпусов в разных районах города, соединённых оптоволоконными каналами. Также MAN может строиться интернет-провайдерами для предоставления услуг пользователям в пределах населённого пункта.

WAN — Wide Area Network, глобальная сеть. Она объединяет устройства и локальные сети, расположенные на больших расстояниях: в разных городах, регионах, странах и континентах. Самый известный пример WAN — Интернет. Крупные предприятия используют WAN для соединения филиалов, складов, офисов и дата-центров. Для этого применяются VPN, выделенные каналы, мобильная связь, спутниковые технологии и сети операторов связи.

Таким образом, PAN предназначена для личных устройств, LAN — для ограниченной территории, MAN — для города, а WAN — для связи на больших расстояниях. На практике все типы могут использоваться одновременно. Например, смартфон подключается к наушникам через PAN, затем к домашнему Wi-Fi через LAN, а через маршрутизатор получает доступ к Интернету, который является WAN.

Ответ 3

Топология сети — это способ организации соединений между устройствами. Она показывает, как компьютеры, серверы, коммутаторы и маршрутизаторы связаны между собой физически или логически. Физическая топология описывает реальное расположение кабелей и оборудования, а логическая — направление передачи данных в сети.

Топология «шина» предполагает подключение всех устройств к одному общему кабелю. В старых Ethernet-сетях использовался коаксиальный кабель, к которому подключались компьютеры. Преимуществом такой схемы было небольшое количество кабеля. Однако выход из строя общего кабеля мог привести к прекращению работы всей сети. Кроме того, при одновременной передаче данных несколькими компьютерами возникали коллизии.

Топология «звезда» является наиболее распространённой в современных сетях. Каждое устройство подключается отдельным кабелем к центральному устройству, обычно к коммутатору. Если кабель одного компьютера повреждён, остальные рабочие места продолжают работать. Недостаток состоит в том, что отказ центрального коммутатора может нарушить работу всех подключённых устройств. Несмотря на это, топология «звезда» удобна для обслуживания, диагностики и расширения сети.

Топология «кольцо» предполагает, что каждое устройство соединено с двумя соседними, а данные передаются по кругу. Ранее такая схема использовалась в сетях Token Ring. Если в кольце нет резервирования, повреждение кабеля или одного устройства может нарушить работу всей сети.

Топология «дерево» представляет собой иерархическую структуру. Например, компьютеры подключаются к коммутаторам на этажах, эти коммутаторы подключаются к центральному коммутатору здания, а он — к маршрутизатору и серверам. Такая структура удобна для крупных организаций, колледжей, бизнес-центров и предприятий.

Ячеистая топология предполагает наличие нескольких путей между узлами. Если один канал выходит из строя, данные могут пойти по резервному маршруту. Полная ячеистая сеть является дорогой, поэтому чаще применяется частичная ячеистая топология между критически важными узлами.

В современных офисах чаще всего применяется топология «звезда» или иерархическая структура «звезда-дерево». Она обеспечивает удобство эксплуатации, возможность централизованного управления, высокую скорость и сравнительно простой поиск неисправностей.

Ответ 4

Сетевое оборудование принято делить на активное и пассивное. Основное различие состоит в том, что активное оборудование требует электропитания и участвует в передаче, обработке или управлении трафиком, а пассивное оборудование не обрабатывает данные и предназначено для организации физической кабельной инфраструктуры.

К активному сетевому оборудованию относятся коммутаторы, маршрутизаторы, точки доступа Wi-Fi, межсетевые экраны, модемы, медиаконвертеры, сетевые карты, контроллеры беспроводной сети и другие устройства. Коммутатор соединяет устройства в локальной сети и передаёт Ethernet-кадры на нужные порты. Маршрутизатор объединяет различные IP-сети и направляет пакеты между ними. Точка доступа создаёт беспроводную сеть и обеспечивает подключение клиентов Wi-Fi к проводной инфраструктуре.

Межсетевой экран относится к активному оборудованию, поскольку он анализирует трафик и принимает решения о его разрешении или блокировке. Например, firewall может запретить доступ гостевого Wi-Fi к внутренним серверам, но разрешить пользователям выход в Интернет. Маршрутизаторы и межсетевые экраны также могут выполнять NAT, VPN, DHCP и другие функции.

К пассивному оборудованию относятся витая пара, оптоволоконный и коаксиальный кабель, патч-корды, коннекторы, розетки, патч-панели, кабель-каналы, монтажные шкафы, стойки, органайзеры кабелей и кроссы. Эти устройства не требуют питания и не принимают решений о передаче информации.

Например, в телекоммуникационном шкафу компьютерного класса кабели от рабочих мест могут приходить на патч-панель. От патч-панели короткими патч-кордами линии соединяются с коммутатором. Патч-панель — пассивный элемент, а коммутатор — активный. Если требуется

подключить IP-камеры и точки доступа, может применяться коммутатор PoE, который одновременно передаёт данные и питание по Ethernet-кабелю.

Для надёжной работы сети важны обе группы оборудования. Хорошо настроенный маршрутизатор не компенсирует плохую кабельную систему, повреждённые коннекторы или отсутствие маркировки. В то же время качественно проложенные кабели не обеспечат защиту и маршрутизацию без правильно настроенного активного оборудования.

Ответ 5

Модель OSI, Open Systems Interconnection, — это эталонная семиуровневая модель взаимодействия сетевых систем. Она используется для описания того, как данные передаются от одного устройства к другому. Модель помогает разделить сетевые функции на уровни, чтобы проще проектировать сети, искать неисправности и понимать назначение протоколов.

Первый уровень — физический. Он отвечает за передачу битов по среде связи. На физическом уровне рассматриваются кабели, коннекторы, радиоволны, оптические сигналы, напряжение, скорость интерфейса и состояние линка. Примеры: витая пара, оптоволокно, разъём RJ-45, сетевой адаптер, радиоканал Wi-Fi.

Второй уровень — канальный. Он отвечает за передачу кадров в пределах локальной сети. На этом уровне используются MAC-адреса, Ethernet-кадры, VLAN, коммутаторы и механизмы контроля ошибок. Коммутатор анализирует MAC-адрес назначения и отправляет кадр на нужный порт.

Третий уровень — сетевой. Его задача — логическая адресация и маршрутизация. Здесь работают IP-адреса, маршрутизаторы и протоколы IPv4, IPv6, ICMP. Маршрутизатор определяет, через какой интерфейс отправить пакет, чтобы он достиг удалённой сети.

Четвёртый уровень — транспортный. Он отвечает за передачу данных между приложениями. TCP обеспечивает надёжную доставку, контроль порядка сегментов и повторную передачу потерянных данных. UDP передаёт данные быстрее, но без гарантии доставки. На этом же уровне применяются номера портов.

Пятый уровень — сеансовый. Он отвечает за создание, управление и завершение сеансов связи между приложениями. Шестой уровень — представления. Он отвечает за кодирование, шифрование, сжатие и преобразование данных. Седьмой уровень — прикладной. Здесь работают пользовательские протоколы и сервисы: HTTP, HTTPS, DNS, SMTP, FTP, SSH.

Модель OSI особенно полезна при диагностике. Если компьютер не подключается к сети, сначала проверяют физический уровень: кабель, индикаторы порта, Wi-Fi. Затем проверяют IP-адрес и шлюз, после этого DNS, доступность сервера и работу конкретного приложения. Такой поэтапный подход позволяет быстрее найти источник неисправности.

Ответ 6

Модель TCP/IP — это практическая модель взаимодействия сетевых протоколов, которая лежит в основе Интернета и большинства современных локальных сетей. В отличие от модели OSI, которая включает семь уровней, модель TCP/IP обычно состоит из четырёх уровней: прикладного, транспортного, интернет-уровня и уровня сетевого доступа.

Прикладной уровень TCP/IP объединяет функции трёх верхних уровней OSI: сеансового, уровня представления и прикладного. На нём работают протоколы, с которыми непосредственно

взаимодействуют пользовательские программы. Например, браузер использует HTTP или HTTPS, электронная почта использует SMTP, IMAP или POP3, удалённое управление сервером выполняется по SSH, а DNS преобразует доменные имена в IP-адреса.

Транспортный уровень TCP/IP соответствует транспортному уровню OSI. Здесь применяются TCP и UDP. TCP обеспечивает надёжную передачу данных: устанавливает соединение, нумерует сегменты, подтверждает их получение и повторно отправляет потерянные части. UDP не устанавливает соединение и не гарантирует доставку, но работает быстрее и даёт меньшие задержки.

Интернет-уровень соответствует сетевому уровню OSI. Главным протоколом является IP. Он отвечает за адресацию и передачу пакетов между различными сетями. На этом уровне также работают ICMP, IPv4, IPv6 и некоторые другие протоколы. Маршрутизаторы используют IP-адреса для выбора пути передачи данных.

Уровень сетевого доступа объединяет физический и канальный уровни OSI. Он включает Ethernet, Wi-Fi, MAC-адреса, сетевые адаптеры, коммутаторы, кабели и способы передачи кадров.

Главное отличие моделей состоит в том, что OSI является подробной теоретической схемой, а TCP/IP — практической моделью, основанной на реально работающих технологиях. OSI удобно использовать в обучении и диагностике, а TCP/IP используется при настройке реальных сетей, серверов, маршрутизаторов и клиентских устройств.

Модель TCP/IP стала основной потому, что протоколы IP, TCP, UDP, DNS, HTTP и другие получили широкое распространение и обеспечили совместимость оборудования разных производителей. Благодаря TCP/IP могут взаимодействовать домашние устройства, корпоративные сети, серверы дата-центров и глобальный Интернет.

Ответ 7

MAC-адрес и IP-адрес нужны для идентификации устройств в сети, однако они используются на разных уровнях и выполняют разные функции. MAC-адрес работает на канальном уровне, а IP-адрес — на сетевом.

MAC-адрес — это аппаратный адрес сетевого интерфейса. Он обычно записывается в шестнадцатеричном формате и состоит из шести байтов. Пример MAC-адреса:

00:1A:2B:3C:4D:5E

MAC-адрес применяется для доставки Ethernet-кадров внутри одной локальной сети. Когда компьютер хочет отправить данные другому устройству в своей подсети, он должен узнать его MAC-адрес. Для этого используется протокол ARP, который связывает известный IP-адрес с MAC-адресом.

IP-адрес — это логический адрес устройства. В IPv4 он состоит из четырёх чисел от 0 до 255, разделённых точками. Например:

192.168.1.25

IP-адрес используется для передачи пакетов между разными сетями. Маршрутизаторы анализируют IP-адрес назначения и определяют, куда переслать пакет дальше. Благодаря IP устройство из одной локальной сети может связаться с сервером, находящимся в другой стране.

При передаче данных в пределах одной сети используются и MAC-, и IP-адреса. Например, компьютер 192.168.1.10 отправляет данные принтеру 192.168.1.50. В IP-пакете указывается адрес назначения 192.168.1.50, а в Ethernet-кадре — MAC-адрес сетевого интерфейса принтера.

Если данные отправляются в Интернет, компьютер не знает MAC-адрес удалённого сервера. Поэтому он формирует кадр, адресованный MAC-адресу шлюза — маршрутизатора. Маршрутизатор затем создаёт новый кадр для следующего участка сети. На каждом участке MAC-адреса могут меняться, а IP-адреса отправителя и получателя обычно остаются прежними.

Следовательно, MAC-адрес используется для локальной доставки кадров, а IP-адрес — для маршрутизации пакетов между сетями. Эти адреса не конкурируют, а дополняют друг друга.

Ответ 8

IPv4-адрес — это 32-битный логический адрес, который используется для идентификации устройства в сети TCP/IP. Обычно он записывается в виде четырёх десятичных чисел, разделённых точками. Каждое число называется октетом и может иметь значение от 0 до 255. Пример IPv4-адреса:

192.168.15.25

Сам по себе IP-адрес не даёт полной информации о сети. Для определения границы сети используется маска подсети. Например:

IP-адрес: 192.168.15.25

Маска: 255.255.255.0

Префикс: /24

Маска 255.255.255.0 означает, что первые 24 бита относятся к сети, а последние 8 бит — к конкретному устройству. В такой конфигурации адрес сети будет:

192.168.15.0

Адрес сети обозначает не отдельное устройство, а всю подсеть. Он используется в таблицах маршрутизации и не назначается компьютеру, принтеру или серверу.

Адрес узла — это адрес конкретного устройства внутри сети. В сети 192.168.15.0/24 адресами узлов будут, например, 192.168.15.1, 192.168.15.25, 192.168.15.100. Обычно первый доступный адрес назначают маршрутизатору, но это не обязательное правило.

Широковещательный адрес, или broadcast, используется для отправки пакета всем устройствам данной подсети. В сети 192.168.15.0/24 широковещательным будет адрес:

192.168.15.255

Таким образом, диапазон обычных адресов устройств составит от 192.168.15.1 до 192.168.15.254.

Шлюз по умолчанию — это IP-адрес маршрутизатора в локальной сети. Например:

Шлюз: 192.168.15.1

Если компьютер обращается к адресу внутри своей подсети, например к 192.168.15.50, данные отправляются напрямую. Если необходимо обратиться к адресу другой сети, например к 8.8.8.8,

компьютер отправляет пакет на шлюз. Маршрутизатор затем передаёт пакет дальше по таблице маршрутизации.

Маска подсети нужна, чтобы устройство понимало, находится ли адрес назначения в локальной сети или трафик необходимо передать маршрутизатору.

Ответ 9

Частные IPv4-адреса — это адреса, предназначенные для использования внутри локальных сетей организаций, квартир, учебных заведений и предприятий. Они не маршрутизируются напрямую в глобальном Интернете. Это означает, что компьютер с адресом 192.168.1.10 может работать в локальной сети, но не может быть напрямую доступен из Интернета без дополнительной настройки.

RFC 1918 выделяет три диапазона частных IPv4-адресов: 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16.

Первый диапазон:

10.0.0.0 – 10.255.255.255

Он очень большой и часто используется крупными организациями, у которых много подразделений, VLAN и сетевых сегментов.

Второй диапазон:

172.16.0.0 – 172.31.255.255

Он используется в средних и крупных сетях. Важно помнить, что не весь диапазон 172.x.x.x является частным. Частными считаются только адреса от 172.16.0.0 до 172.31.255.255.

Третий диапазон:

192.168.0.0 – 192.168.255.255

Он чаще всего применяется в домашних сетях, небольших офисах и учебных аудиториях. Например, домашний маршрутизатор может иметь адрес 192.168.1.1, а ноутбук — 192.168.1.100.

Для выхода частных адресов в Интернет используется NAT, Network Address Translation. NAT выполняется на маршрутизаторе. Когда внутренний компьютер отправляет запрос в Интернет, маршрутизатор заменяет его частный IP-адрес на публичный IP-адрес внешнего интерфейса. При получении ответа маршрутизатор определяет, какому внутреннему устройству предназначены данные, и передаёт их обратно.

Например, компьютер с адресом 192.168.1.20 открывает веб-сайт. В локальной сети используется частный адрес, но для внешнего сервера соединение выглядит так, будто запрос пришёл от публичного адреса маршрутизатора, например 203.0.113.10.

Частные адреса позволяют экономить ограниченное пространство IPv4, повторно использовать одинаковые адресные диапазоны в разных организациях и скрывать внутреннюю структуру сети от прямого доступа из Интернета. Однако NAT не следует считать полноценной заменой межсетевого экрана: для защиты всё равно необходимы правила фильтрации трафика.

Ответ 10

Исходная сеть имеет адрес 192.168.20.0/24. Префикс /24 означает, что первые 24 бита адреса относятся к части сети, а оставшиеся 8 бит используются для адресации устройств. Такая сеть содержит 256 адресов: от 192.168.20.0 до 192.168.20.255.

Необходимо создать не менее шести подсетей. Для этого нужно занять часть битов, ранее предназначенных для адресов устройств. Расчёт выполняется по формуле:

$$2^n \setminus 6$$

где n — количество битов, которые будут заимствованы для создания подсетей. При двух дополнительных битах получится только четыре подсети:

$$2^2 = 4$$

Этого недостаточно. При трёх битах получится восемь подсетей:

$$2^3 = 8$$

Следовательно, необходимо увеличить префикс с /24 до /27.

Новая маска сети:

$$255.255.255.224$$

После выделения трёх бит под номер подсети остаётся пять бит для адресов узлов:

$$2^5 = 32$$

Каждая подсеть содержит 32 адреса. Из них один адрес является адресом сети, один — широковещательным адресом. Поэтому доступно:

$$32 - 2 = 30$$

адресов для компьютеров, серверов, камер и других устройств.

Подсеть	Адрес сети	Доступные адреса узлов	Широковещательный адрес
1	192.168.20.0/27	192.168.20.1–192.168.20.30	192.168.20.31
2	192.168.20.32/27	192.168.20.33–192.168.20.62	192.168.20.63
3	192.168.20.64/27	192.168.20.65–192.168.20.94	192.168.20.95
4	192.168.20.96/27	192.168.20.97–192.168.20.126	192.168.20.127
5	192.168.20.128/27	192.168.20.129–192.168.20.158	192.168.20.159
6	192.168.20.160/27	192.168.20.161–192.168.20.190	192.168.20.191

Оставшиеся две подсети будут 192.168.20.192/27 и 192.168.20.224/27. Такое разделение можно использовать для разных подразделений: администрации, учебных кабинетов, серверов, IP-камер, преподавателей и гостевого Wi-Fi.

Ответ 11

Статическая IP-адресация — это ручное назначение сетевых параметров на каждом устройстве. Администратор вводит IP-адрес, маску подсети, шлюз по умолчанию и DNS-сервер. Например, файловому серверу можно назначить:

IP-адрес: 192.168.10.10
Маска: 255.255.255.0
Шлюз: 192.168.10.1
DNS: 192.168.10.1

Преимущество статической адресации в том, что адрес устройства не меняется. Это важно для серверов, принтеров, камер, сетевых хранилищ, NVR, маршрутизаторов и коммутаторов. Если сетевой принтер постоянно имеет адрес 192.168.10.50, его можно настроить на рабочих компьютерах, и пользователи всегда будут обращаться к нему по одному адресу.

Недостатком статической адресации является необходимость вручную настраивать каждое устройство. В большой сети это трудоёмко и увеличивает риск ошибок. Например, если два компьютера получают один и тот же IP-адрес, возникнет конфликт адресов. Это может проявляться как нестабильная работа сети, потеря доступа к Интернету или невозможность открыть нужный сервер.

DHCP, Dynamic Host Configuration Protocol, — это протокол, позволяющий автоматически выдавать сетевые параметры. Компьютер подключается к сети, отправляет DHCP-запрос и получает свободный IP-адрес, маску, шлюз, DNS-сервер и срок аренды адреса. Например, DHCP-сервер может выдавать адреса в диапазоне от 192.168.10.100 до 192.168.10.200.

DHCP удобен для рабочих станций, ноутбуков, смартфонов, планшетов, гостевых устройств и компьютеров студентов. При подключении к сети они автоматически получают параметры, поэтому администратору не нужно вручную настраивать каждое устройство.

На практике часто используется смешанная схема. Серверы и критически важное оборудование получают статические адреса. Пользовательские устройства работают через DHCP. Для принтеров, камер и других важных устройств можно использовать DHCP-резервирование: сервер DHCP выдаёт определённому MAC-адресу всегда один и тот же IP-адрес. Такой вариант удобнее ручной настройки, но при этом сохраняет постоянство адреса.

Ответ 12

DNS, Domain Name System, — это система доменных имён. Её основное назначение состоит в преобразовании доменных имён, понятных пользователю, в IP-адреса, которые необходимы компьютерам и маршрутизаторам для передачи данных.

Например, пользователь вводит в браузере адрес:

www.example.com

Однако браузер не может отправить пакет только по имени сайта. Ему нужен IP-адрес сервера. Для этого выполняется DNS-запрос. Сначала операционная система проверяет локальный DNS-кэш: возможно, адрес уже был получен ранее и ещё не устарел. Если записи нет, компьютер отправляет запрос на настроенный DNS-сервер.

DNS-сервер может сразу выдать ответ из собственного кэша. Если ответа нет, он начинает последовательный поиск. Сначала запрашиваются корневые DNS-серверы, затем серверы доменной зоны верхнего уровня, например .ru, .com или .org, после чего происходит обращение к

авторитетному DNS-серверу конкретного домена. Авторитетный сервер хранит актуальные DNS-записи домена.

После получения IP-адреса DNS-сервер отправляет результат клиенту. Браузер использует этот IP-адрес для подключения к веб-серверу. Затем происходит установка TCP-соединения и, при использовании HTTPS, защищённого TLS-соединения.

Основные типы DNS-записей:

- **A** — связывает имя с IPv4-адресом.
- **AAAA** — связывает имя с IPv6-адресом.
- **CNAME** — создаёт псевдоним для другого доменного имени.
- **MX** — определяет почтовые серверы домена.
- **PTR** — используется для обратного разрешения: получения имени по IP-адресу.
- **TXT** — хранит текстовые данные, например записи для проверки домена или настройки почтовой защиты.

DNS применяется не только в Интернете. В организации можно создать внутреннюю DNS-зону. Например, вместо обращения к серверу по адресу `192.168.10.10` сотрудники могут использовать имя `fileserver.local`. Если IP-адрес сервера изменится, администратору достаточно изменить DNS-запись, а не перенастраивать каждый компьютер.

Ответ 13

Маршрутизатор — это сетевое устройство, которое соединяет разные IP-сети и передаёт пакеты между ними. Он работает преимущественно на сетевом уровне модели OSI и принимает решения на основе IP-адресов назначения. Маршрутизатор использует таблицу маршрутизации, чтобы определить, куда направить каждый пакет.

Например, в организации могут существовать отдельные сети:

`192.168.10.0/24` — администрация
`192.168.20.0/24` — учебные кабинеты
`192.168.30.0/24` — серверы
`192.168.40.0/24` — камеры видеонаблюдения

Чтобы устройства из этих сетей могли взаимодействовать друг с другом, необходимо устройство маршрутизации. Это может быть отдельный маршрутизатор, межсетевой экран или коммутатор третьего уровня. Он имеет интерфейсы или виртуальные интерфейсы в разных подсетях и пересылает пакеты между ними в соответствии с правилами доступа.

Шлюз по умолчанию — это IP-адрес маршрутизатора в локальной сети. Он используется, когда компьютер хочет передать данные в другую сеть. Например, компьютер имеет:

IP-адрес: `192.168.10.25`
Маска: `255.255.255.0`
Шлюз: `192.168.10.1`

Если компьютер обращается к адресу `192.168.10.50`, он определяет, что этот адрес находится в той же локальной сети, и отправляет данные напрямую. Если адрес назначения — `8.8.8.8`, он не относится к локальной сети. Поэтому компьютер передаёт пакет на шлюз `192.168.10.1`.

Если шлюз указан неверно, отключён или недоступен, компьютер сможет работать только с устройствами своей локальной сети. Например, он сможет обратиться к принтеру или соседнему компьютеру, но не сможет выйти в Интернет, открыть удалённый сайт или подключиться к серверу в другой подсети.

Маршрутизатор также может выполнять функции NAT, VPN, DHCP, фильтрации трафика, контроля доступа и подключения к провайдеру. В домашних сетях один маршрутизатор часто объединяет функции точки доступа Wi-Fi, коммутатора, DHCP-сервера, NAT и межсетевого экрана.

Ответ 14

Таблица маршрутизации — это набор правил, по которым устройство определяет, куда отправить IP-пакет. Такие таблицы есть не только на маршрутизаторах, но и на обычных компьютерах, серверах и смартфонах. Каждая запись обычно содержит сеть назначения, префикс или маску, интерфейс выхода и при необходимости адрес следующего маршрутизатора.

Рассмотрим таблицу:

192.168.1.0/24	— напрямую через интерфейс LAN
10.10.0.0/16	— через шлюз 192.168.1.2
0.0.0.0/0	— через шлюз 192.168.1.1

Первая запись означает, что сеть 192.168.1.0/24 является локальной. Для отправки данных устройствам этой сети не нужно обращаться к другому маршрутизатору. Компьютер определяет MAC-адрес получателя через ARP и передаёт Ethernet-кадр напрямую.

Вторая запись говорит, что сеть 10.10.0.0/16 доступна через маршрутизатор 192.168.1.2. Если адрес назначения начинается с 10.10, пакет должен быть передан именно этому шлюзу.

Третья запись 0.0.0.0/0 является маршрутом по умолчанию. Она используется, если для адреса назначения не найден более конкретный маршрут. Обычно это путь в Интернет через основной маршрутизатор.

Адрес назначения	Выбранный маршрут	Результат
192.168.1.50	192.168.1.0/24	Передача напрямую в LAN
10.10.5.20	10.10.0.0/16	Передача на 192.168.1.2
8.8.8.8	0.0.0.0/0	Передача на 192.168.1.1

Адрес 192.168.1.50 входит в сеть 192.168.1.0/24, поэтому пакет будет отправлен напрямую. Адрес 10.10.5.20 соответствует маршруту 10.10.0.0/16, поэтому следующим узлом станет 192.168.1.2. Адрес 8.8.8.8 не входит в первые две сети, поэтому будет применён маршрут по умолчанию через 192.168.1.1.

При выборе маршрута действует правило наиболее длинного совпадения префикса. Если адресам соответствуют несколько маршрутов, выбирается наиболее конкретный. Например, маршрут /24 будет иметь приоритет перед /16, а /16 — перед маршрутом /0.

Ответ 15

Концентратор, или hub, и коммутатор, или switch, применяются для соединения нескольких устройств в локальной сети. Однако принцип их работы существенно различается. Концентратор

является устаревшим устройством физического уровня, а коммутатор работает преимущественно на канальном уровне модели OSI.

Концентратор принимает сигнал на одном порту и повторяет его на все остальные порты. Он не анализирует MAC-адрес назначения и не знает, какому устройству предназначен передаваемый кадр. Поэтому если один компьютер отправляет данные другому, этот трафик фактически получают все устройства, подключённые к концентратору.

Все порты концентратора входят в один домен коллизий. Если два устройства начинают передачу одновременно, возникает коллизия. В старых полудуплексных Ethernet-сетях это приводило к повторной передаче кадров и снижению производительности. Чем больше устройств подключено к концентратору, тем выше вероятность коллизий и ниже эффективность сети.

Коммутатор работает иначе. Он изучает MAC-адреса устройств, подключённых к его портам, и создаёт таблицу коммутации. Когда коммутатор получает Ethernet-кадр, он смотрит на MAC-адрес назначения. Если адрес известен, кадр передаётся только на нужный порт. Остальные устройства не получают этот трафик.

Коммутатор создаёт отдельный домен коллизий на каждом порту. Современные соединения работают в полнодуплексном режиме: устройство может одновременно передавать и получать данные. Это обеспечивает высокую скорость и стабильную работу сети.

Современные коммутаторы также поддерживают VLAN, QoS, зеркалирование портов, агрегацию каналов, контроль доступа и PoE. Концентраторы не имеют таких возможностей. Именно поэтому они практически не используются в современных сетях: они создают лишний трафик, снижают производительность, ухудшают безопасность и не поддерживают современные функции управления.

Ответ 16

VLAN, Virtual Local Area Network, — это виртуальная локальная сеть. VLAN позволяет логически разделить одну физическую сеть на несколько независимых сегментов. Устройства могут быть подключены к одному коммутатору, но при этом находиться в разных VLAN и не обмениваться данными напрямую.

Например, в колледже можно создать следующие VLAN:

VLAN 10 — администрация
VLAN 20 — преподаватели
VLAN 30 — студенты
VLAN 40 — серверы
VLAN 50 — IP-камеры
VLAN 60 — гостевой Wi-Fi

Компьютер администрации, подключённый к порту VLAN 10, будет находиться в отдельном широковещательном домене. Студенческий компьютер на порту VLAN 30 не увидит широковещательный трафик VLAN 10 и не сможет напрямую подключиться к компьютеру администрации.

Обычные порты коммутатора называются access-портами. Каждый такой порт обычно принадлежит одной VLAN. Например, порт 1 можно назначить в VLAN 10 для рабочего места администрации, а порт 15 — в VLAN 30 для студенческого компьютера.

Для передачи нескольких VLAN между коммутаторами используется trunk-порт. По одному физическому кабелю могут передаваться кадры разных VLAN. Для их различия применяется маркировка IEEE 802.1Q, то есть специальные теги в Ethernet-кадрах.

VLAN даёт несколько преимуществ. Во-первых, она уменьшает широковещательный трафик. Во-вторых, повышает безопасность: гостевой Wi-Fi, камеры и рабочие станции администрации можно изолировать. В-третьих, упрощает управление: устройства объединяются по функциональному назначению, а не только по месту подключения.

Однако VLAN не заменяет межсетевой экран. Если между VLAN включить маршрутизацию без ограничений, устройства смогут обмениваться данными. Поэтому необходимо применять правила firewall или ACL. Например, студентам можно разрешить доступ к образовательному серверу, но запретить доступ к компьютерам бухгалтерии и камерам.

Сегментация снижает последствия инцидентов. Если вредоносное ПО попадает в студенческий сегмент, оно не должно автоматически получить доступ к серверной инфраструктуре или устройствам администрации. NIST отмечает, что сегментация уменьшает риск распространения угроз благодаря разделению сети на изолированные области.[\[nist\]](#)

Ответ 17

Wi-Fi — это технология беспроводной локальной сети, которая позволяет устройствам обмениваться данными по радиоканалу. Вместо кабеля между ноутбуком и коммутатором используется точка доступа. Она создаёт беспроводную сеть с определённым именем, которое называется SSID.

Пользователь видит SSID в списке доступных сетей, выбирает нужную сеть и проходит аутентификацию. Если пароль или другие данные доступа введены верно, устройство подключается к точке доступа. Затем обычно через DHCP получает IP-адрес, маску, шлюз и DNS-сервер. После этого ноутбук или смартфон может работать с локальными ресурсами и Интернетом.

Wi-Fi может использовать диапазоны 2,4 ГГц, 5 ГГц и 6 ГГц. Диапазон 2,4 ГГц обычно имеет большую дальность, но сильнее подвержен помехам. В нём работают многие бытовые устройства: Bluetooth-устройства, некоторые беспроводные камеры, микроволновые печи и другие источники радиопомех. Диапазон 5 ГГц предоставляет больше каналов и часто обеспечивает более высокую скорость, но хуже проходит через стены.

Основные угрозы Wi-Fi включают подбор слабого пароля, подключение посторонних пользователей, перехват незашифрованного трафика в открытых сетях, создание поддельной точки доступа и использование устаревших алгоритмов защиты. Например, злоумышленник может создать сеть с названием, похожим на название сети организации, чтобы пользователи подключились к ней по ошибке.

Для защиты следует использовать WPA3-Personal, а при отсутствии такой возможности — WPA2-Personal с надёжным длинным паролем. Не рекомендуется применять WEP и старые режимы WPA, поскольку они считаются небезопасными. Также необходимо менять заводской пароль администратора точки доступа, обновлять прошивку, отключать ненужные сервисы управления и ограничивать доступ к настройкам оборудования.

В организации желательно создавать несколько отдельных Wi-Fi-сетей: для сотрудников, студентов и гостей. Каждая сеть должна быть привязана к отдельной VLAN. Гостевой Wi-Fi должен иметь доступ только к Интернету и не должен видеть серверы, рабочие станции администрации, камеры и сетевые хранилища.

Ответ 18

TCP и UDP — это транспортные протоколы, которые обеспечивают передачу данных между приложениями в сетях TCP/IP. Оба протокола используют номера портов, но имеют разные принципы работы и применяются в разных ситуациях.

TCP, Transmission Control Protocol, является протоколом с установлением соединения. Перед передачей данных клиент и сервер выполняют процедуру согласования, которую часто называют трёхсторонним рукопожатием. TCP обеспечивает надёжную передачу: сегменты нумеруются, подтверждаются получателем, а потерянные данные передаются повторно. TCP также гарантирует, что данные будут собраны в правильном порядке.

TCP используется там, где важна точность и полнота передачи. Например, при скачивании файла нельзя допустить потерю части данных. При открытии веб-страницы браузер должен получить корректный HTML-код, таблицы стилей и скрипты. Поэтому HTTP, HTTPS, FTP, SMTP, SSH и многие другие протоколы работают поверх TCP.

UDP, User Datagram Protocol, не устанавливает соединение и не гарантирует доставку пакетов. Он не проверяет, дошёл ли пакет до получателя, не обеспечивает повторную отправку и не восстанавливает порядок данных. За счёт этого UDP имеет меньшие накладные расходы и часто обеспечивает более низкую задержку.

UDP используется в ситуациях, где важна скорость и актуальность информации. Например, в голосовой связи потеря одного небольшого пакета менее критична, чем задержка в несколько секунд. Поэтому VoIP, видеоконференции, потоковое видео, онлайн-игры и некоторые DNS-запросы могут использовать UDP.

Характеристика	TCP	UDP
Установка соединения	Есть	Нет
Гарантия доставки	Есть	Нет
Порядок данных	Сохраняется	Не гарантируется
Повторная передача	Есть	Нет
Накладные расходы	Выше	Ниже
Применение	Веб, файлы, почта, SSH	Игры, DNS, VoIP, видео

Нельзя сказать, что один протокол лучше другого. TCP нужен для надёжности, а UDP — для скорости и минимальной задержки. Выбор зависит от требований конкретного приложения.

Ответ 19

Сетевой порт — это логический номер, который позволяет операционной системе определить, какой программе предназначены полученные данные. Один компьютер может одновременно использовать браузер, мессенджер, почтовый клиент, VPN, удалённый рабочий стол и другие программы. Все они могут работать через один IP-адрес, но используют разные порты.

IP-адрес идентифицирует устройство в сети. Например:

192.168.1.25

Порт идентифицирует службу или программу на конкретном устройстве. Например, веб-сервер обычно принимает HTTP-запросы на порту 80, а HTTPS-запросы — на порту 443.

Комбинация IP-адреса и порта называется сокетом. Пример:

192.168.1.25:443

Это означает, что на устройстве с адресом 192.168.1.25 работает служба, ожидающая подключения на порту 443.

При соединении важны адреса и порты обеих сторон. Например, браузер пользователя может установить соединение:

Клиент: 192.168.1.50:53124
Сервер: 93.184.216.34:443

Порт 53124 является временным клиентским портом, который операционная система выбрала автоматически. Порт 443 — стандартный порт HTTPS-сервера.

Распространённые порты:

Порт	Служба	Назначение
21	FTP	Передача файлов
22	SSH	Защищённое удалённое управление
23	Telnet	Устаревшее удалённое управление
25	SMTP	Отправка электронной почты
53	DNS	Разрешение доменных имён
67 и 68	DHCP	Автоматическая настройка сети
80	HTTP	Обычный веб-трафик
110	POP3	Получение почты
123	NTP	Синхронизация времени
143	IMAP	Доступ к почте на сервере
443	HTTPS	Защищённый веб-трафик
3389	RDP	Удалённый рабочий стол Windows

Порты важны при настройке межсетевого экрана. Например, можно разрешить пользователям выход в Интернет по HTTPS на порт 443, но запретить входящие подключения из Интернета к порту 3389, если удалённый рабочий стол не используется через VPN.

Ответ 20

HTTP, HyperText Transfer Protocol, — это протокол прикладного уровня, который используется для обмена данными между браузером и веб-сервером. По HTTP передаются веб-страницы, изображения, стили, скрипты, документы и другие файлы. Обычный HTTP чаще всего использует TCP-порт 80.

Главный недостаток HTTP заключается в отсутствии шифрования. Если пользователь вводит логин, пароль, персональные данные или другую конфиденциальную информацию, она может передаваться в открытом виде. В небезопасной сети злоумышленник может попытаться перехватить такой трафик.

HTTPS, HyperText Transfer Protocol Secure, — это защищённый вариант HTTP. Он работает поверх TLS, Transport Layer Security, и обычно использует TCP-порт 443. HTTPS обеспечивает шифрование данных, проверку целостности и аутентификацию сервера.

TLS решает три основные задачи. Во-первых, он шифрует передаваемую информацию, чтобы её нельзя было прочитать при перехвате. Во-вторых, TLS контролирует целостность данных: если кто-то попытается изменить пакет в пути, соединение обнаружит это. В-третьих, TLS помогает убедиться, что браузер подключается к настоящему серверу, а не к поддельному.

При открытии сайта по HTTPS сервер передаёт браузеру цифровой сертификат. В сертификате содержится информация о домене и ключах шифрования. Браузер проверяет, соответствует ли сертификат доменному имени, не истёк ли срок его действия и выдан ли он доверенным центром сертификации.

HTTPS необходимо использовать для сайтов с авторизацией, интернет-магазинов, электронных журналов, личных кабинетов, банковских сервисов и любых систем, которые передают конфиденциальные данные. Однако наличие HTTPS не означает, что сайт обязательно честный или безопасный. Мошеннический сайт тоже может иметь сертификат. Поэтому пользователь должен обращать внимание на доменное имя, содержание страницы и не вводить пароли на подозрительных ресурсах.

Ответ 21

Витая пара — это распространённый тип кабеля, применяемый для построения Ethernet-сетей. Она состоит из восьми медных проводников, сгруппированных в четыре пары. Каждая пара скручена, что уменьшает электромагнитные помехи и взаимное влияние проводников.

Для подключения витой пары к компьютеру, коммутатору, маршрутизатору или патч-панели чаще всего применяется модульный коннектор 8P8C, который в быту обычно называют RJ-45. При обжиме кабеля важно правильно расположить жилы в разъёме. Наиболее распространены стандарты T568A и T568B.

Порядок жил по стандарту T568A:

- 1 — бело-зелёный
- 2 — зелёный
- 3 — бело-оранжевый
- 4 — синий
- 5 — бело-синий
- 6 — оранжевый
- 7 — бело-коричневый
- 8 — коричневый

Порядок жил по стандарту T568B:

- 1 — бело-оранжевый
- 2 — оранжевый
- 3 — бело-зелёный
- 4 — синий
- 5 — бело-синий
- 6 — зелёный
- 7 — бело-коричневый
- 8 — коричневый

Прямой кабель имеет одинаковую схему на обоих концах. Например, T568B–T568B. Он традиционно используется для подключения устройств разного типа: компьютер — коммутатор, коммутатор — маршрутизатор, точка доступа — коммутатор.

Кроссовый кабель имеет разные схемы обжима: T568A на одном конце и T568B на другом. Раньше он применялся для соединения двух однотипных устройств: двух компьютеров, двух коммутаторов или компьютера с маршрутизатором без промежуточного коммутатора.

Современное оборудование часто поддерживает Auto MDI-X. Эта функция автоматически определяет расположение передающих и принимающих пар и позволяет использовать прямой кабель даже там, где раньше требовался кроссовый. Однако умение различать T568A, T568B, прямой и кроссовый кабель важно при работе со старым оборудованием и при диагностике физических проблем сети.

После обжима кабель необходимо проверить тестером. Он помогает выявить обрыв проводника, перепутанные жилы, короткое замыкание и плохой контакт.

Ответ 22

В Windows для диагностики сети используются встроенные утилиты командной строки. Наиболее полезными являются `ipconfig`, `ping`, `tracert` и `nslookup`. Они позволяют проверить сетевые настройки, доступность устройств, маршрут прохождения пакетов и работу DNS.

Команда:

```
ipconfig
```

показывает основные настройки сетевых адаптеров: IP-адрес, маску подсети и шлюз по умолчанию. Более подробный вариант:

```
ipconfig /all
```

дополнительно показывает MAC-адрес, используемые DNS-серверы, DHCP-настройки, срок аренды IP-адреса и состояние адаптера. Если компьютер получил адрес вида 169.254.x.x, это обычно означает, что он не смог получить параметры от DHCP-сервера.

Команда:

```
ping адрес
```

проверяет доступность узла по сети. Например:

```
ping 192.168.1.1
```

позволяет проверить связь со шлюзом. Команда:

```
ping 8.8.8.8
```

проверяет, проходит ли трафик к внешнему IP-адресу. Если внешний IP отвечает, но сайты по именам не открываются, возможна проблема с DNS.

Команда:

```
tracert адрес
```

показывает путь, который проходит пакет до удалённого узла. Например:

```
tracert 8.8.8.8
```

отобразит промежуточные маршрутизаторы. Это помогает определить, на каком участке сети возникают задержки или потеря связи.

Команда:

```
nslookup имя_сайта
```

используется для проверки DNS. Например:

```
nslookup example.com
```

покажет, какой DNS-сервер обработал запрос и какой IP-адрес был найден для доменного имени.

Если сайт не открывается, можно использовать следующую последовательность:

1. Выполнить `ipconfig /all` и проверить IP-адрес, маску, шлюз и DNS.
2. Выполнить `ping 127.0.0.1` для проверки локального стека TCP/IP.
3. Выполнить `ping` собственного IP-адреса.
4. Проверить шлюз командой `ping 192.168.1.1`.
5. Проверить внешний адрес: `ping 8.8.8.8`.
6. Проверить DNS: `nslookup example.com`.
7. При необходимости выполнить `tracert 8.8.8.8`.

Такой алгоритм позволяет определить, где находится проблема: в физическом подключении, настройках IP, маршрутизаторе, интернет-канале или DNS.

Ответ 23

Межсетевой экран, или `firewall`, — это программное или аппаратное средство, которое контролирует сетевой трафик по заданным правилам. Он анализирует входящие и исходящие соединения и принимает решение: разрешить, запретить или дополнительно проверить трафик.

Простейший `firewall` работает на основе IP-адресов, портов и протоколов. Например, он может разрешить пользователям доступ к веб-сайтам по TCP-порту 443, запретить входящие подключения к удалённому рабочему столу на порт 3389 и блокировать подозрительные попытки доступа извне.

Современные межсетевые экраны могут быть более функциональными. Они способны отслеживать состояние соединений, проверять приложения, фильтровать веб-трафик, создавать VPN-туннели, обнаруживать атаки, блокировать вредоносные сайты и сегментировать сеть между VLAN.

Основные правила безопасной настройки сети:

- Разрешать только нужный трафик и блокировать всё остальное.
- Не открывать административные сервисы напрямую в Интернет.
- Использовать VPN для удалённого доступа к внутренним ресурсам.
- Разделять сеть на VLAN: администрация, серверы, студенты, гости, камеры.
- Не давать гостевому Wi-Fi доступ к внутренним ресурсам.
- Регулярно обновлять прошивки маршрутизаторов, точек доступа и `firewall`.
- Менять заводские логины и пароли.
- Использовать сложные уникальные пароли и многофакторную аутентификацию.

- Вести журнал событий и контролировать попытки несанкционированного доступа.
- Делать резервные копии конфигурации сетевого оборудования.

Особое значение имеет принцип минимальных привилегий. Если сотруднику нужен доступ только к файловому серверу и принтеру, не следует предоставлять ему доступ ко всем внутренним сегментам. Аналогично камеры должны передавать поток на сервер записи, но не должны иметь доступ к компьютерам администрации.

Сегментация и контроль доступа позволяют снизить последствия инцидента. NIST рассматривает изоляцию сегментов и современные модели безопасного сетевого доступа как важную часть защищённой архитектуры.

Ответ 24

VPN, Virtual Private Network, — это виртуальная частная сеть. Она создаёт защищённый канал связи через общедоступную сеть, чаще всего через Интернет. Данные внутри VPN-туннеля шифруются, поэтому их содержимое не должно быть доступно посторонним пользователям сети.

Первый распространённый сценарий применения VPN — удалённый доступ сотрудников. Например, преподаватель или администратор находится дома, но ему необходимо подключиться к внутреннему файловому серверу, системе электронного документооборота, серверу баз данных или панели управления оборудованием. Пользователь запускает VPN-клиент, проходит аутентификацию и получает разрешённый доступ к ресурсам организации.

Второй сценарий — соединение нескольких офисов или филиалов. Например, главный корпус колледжа и удалённое подразделение могут быть соединены site-to-site VPN. В этом случае маршрутизаторы на обеих площадках создают постоянный защищённый туннель. Пользователи в разных зданиях могут работать с общими ресурсами так, словно находятся в одной сети.

VPN обеспечивает несколько преимуществ. Во-первых, шифрует данные при передаче через Интернет. Во-вторых, позволяет организовать удалённую работу. В-третьих, уменьшает необходимость открывать опасные административные порты прямо в Интернет. Например, вместо публикации RDP-сервера наружу администратор может сначала подключиться к VPN, а затем использовать удалённый рабочий стол внутри защищённой сети.

Однако VPN не является абсолютной защитой. Если компьютер пользователя заражён вредоносным ПО, оно может использовать уже установленное VPN-соединение. Если применяются слабые пароли или устаревшие протоколы, безопасность снижается. Поэтому рекомендуется использовать современные VPN-протоколы, многофакторную аутентификацию, строгие правила доступа, обновления и журналирование.

Корпоративный VPN не следует путать с публичными VPN-сервисами. Корпоративный VPN предназначен для безопасного доступа к конкретной внутренней сети. Публичный VPN обычно направляет интернет-трафик через сервер стороннего провайдера, но не делает пользователя полностью анонимным и требует доверия к оператору сервиса.

Ответ 25

Для офиса на 25 сотрудников рекомендуется создать управляемую сеть с сегментацией по VLAN. В офисе имеются рабочие компьютеры, Wi-Fi, сетевой принтер, файловый сервер и IP-камеры. Все эти устройства имеют разное назначение и уровень доверия, поэтому их не следует помещать в одну общую подсеть.

На границе с Интернетом должен быть установлен маршрутизатор или межсетевой экран. Он обеспечивает подключение к провайдеру, NAT, DHCP, VPN, фильтрацию трафика и маршрутизацию между VLAN. Далее устанавливается управляемый гигабитный коммутатор. Желательно использовать коммутатор с запасом портов: на 48 портов либо два 24-портовых коммутатора. Это позволит подключить не только 25 компьютеров, но и сервер, принтер, точки доступа, камеры, NVR и резервные линии.

Для питания IP-камер и точек доступа удобно использовать PoE-коммутатор. PoE позволяет передавать питание и данные по одному Ethernet-кабелю, что упрощает установку оборудования.

Пример адресации:

VLAN	Назначение	Подсеть	Шлюз
10	Рабочие компьютеры	192.168.10.0/24	192.168.10.1
20	Серверы и принтеры	192.168.20.0/24	192.168.20.1
30	IP-камеры и NVR	192.168.30.0/24	192.168.30.1
40	Гостевой Wi-Fi	192.168.40.0/24	192.168.40.1
99	Управление оборудованием	192.168.99.0/24	192.168.99.1

Компьютеры сотрудников могут получать адреса автоматически по DHCP. Серверу, принтеру, камерам и NVR лучше выдать постоянные адреса или настроить DHCP-резервирование.

Правила безопасности должны ограничивать связь между сегментами. Рабочие станции могут обращаться к файловому серверу и принтеру. Камеры должны иметь доступ только к NVR, серверу времени и при необходимости к ограниченному набору внешних сервисов. Гостевой Wi-Fi должен иметь доступ только в Интернет и не должен видеть рабочие станции, серверы, принтеры или камеры.

Такая схема обеспечивает стабильную работу, упрощает поиск неисправностей, позволяет расширять сеть и снижает риск распространения угроз между разными категориями устройств.

Ответ 26

Если компьютер показывает подключение к сети, но не открывает сайты, необходимо последовательно проверить все уровни: физическое подключение, IP-настройки, доступность шлюза, выход в Интернет и работу DNS. Нельзя сразу менять настройки без диагностики, потому что это может усложнить поиск причины.

Сначала нужно проверить физическое соединение. При проводном подключении следует убедиться, что кабель плотно вставлен в сетевую карту и коммутатор, а на портах горят индикаторы. Можно попробовать другой патч-корд или другой порт коммутатора. При Wi-Fi необходимо проверить, к правильной ли сети подключён компьютер, достаточен ли сигнал и не включён ли режим полёта.

Затем необходимо открыть командную строку и выполнить:

```
ipconfig /all
```

Нужно проверить, есть ли корректный IP-адрес, маска подсети, шлюз по умолчанию и DNS-серверы. Если адрес начинается с 169.254, это означает, что DHCP не выдал параметры. В этом случае можно попытаться обновить аренду:

```
ipconfig /release  
ipconfig /renew
```

Далее следует проверить локальный сетевой стек:

```
ping 127.0.0.1
```

Если ответа нет, возможно повреждены компоненты TCP/IP, отключён адаптер или есть проблема с драйвером. После этого полезно проверить свой IP-адрес и адрес шлюза:

```
ping свой_IP  
ping адрес_шлюза
```

Если шлюз не отвечает, проблема находится в пределах локальной сети: кабель, Wi-Fi, VLAN, коммутатор, IP-конфликт, неверная маска или неисправный маршрутизатор.

Если шлюз доступен, необходимо проверить внешний IP-адрес:

```
ping 8.8.8.8
```

Если внешний IP отвечает, но сайты не открываются по именам, следует проверить DNS:

```
nslookup example.com
```

Если DNS не работает, необходимо проверить адреса DNS-серверов, настройки маршрутизатора, локальный firewall или прокси-сервер.

Дополнительно нужно проверить, не включён ли VPN, не настроен ли ошибочный прокси-сервер, не блокирует ли доступ антивирус или межсетевой экран. Если проблема наблюдается только в браузере, стоит проверить расширения, настройки прокси и попробовать другой браузер.

После устранения неисправности нужно повторно проверить доступность шлюза, внешний IP, DNS и открытие сайтов. Такой алгоритм помогает точно определить источник проблемы, а не выполнять случайные действия.

Ответ 27

IPv6, Internet Protocol version 6, был создан из-за ограниченности адресного пространства IPv4. В IPv4 используется 32-битная адресация, что даёт примерно 4,3 миллиарда адресов. При огромном количестве компьютеров, смартфонов, серверов, камер, датчиков, автомобилей и устройств Интернета вещей этого количества стало недостаточно.

IPv6 использует 128-битные адреса. Это обеспечивает чрезвычайно большое количество возможных адресов. Пример IPv6-адреса:

```
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

IPv6-адрес записывается в шестнадцатеричном виде группами по четыре символа. Ведущие нули можно опускать, а одну последовательность нулевых блоков можно заменить двойным двоеточием. Поэтому этот адрес можно сократить:

```
2001:db8:85a3::8a2e:370:7334
```

Характеристика	IPv4	IPv6
Размер адреса	32 бита	128 бит
Пример адреса	192.168.1.10	2001:db8::10
NAT	Часто используется	Обычно не нужен для экономии адресов
Broadcast	Используется	Не применяется
Автонастройка	DHCP или ручная настройка	SLAAC, DHCPv6, ручная настройка
Заголовок пакета	Более сложный	Упрощённый и расширяемый

IPv6 не использует широковещательные сообщения в привычном IPv4-виде. Вместо этого применяются multicast и anycast. Это позволяет эффективнее передавать данные группам устройств.

Одним из преимуществ IPv6 является SLAAC — Stateless Address Autoconfiguration. Устройство может автоматически сформировать адрес на основе префикса, который получает от маршрутизатора. Это упрощает настройку сетей.

Переход на IPv6 происходит постепенно. Многие сети используют dual stack, то есть одновременно поддерживают IPv4 и IPv6. Это необходимо, потому что значительная часть оборудования и интернет-сервисов продолжает использовать IPv4.

IPv6 не делает сеть автоматически безопасной. Необходимы правильные настройки firewall, контроль доступа, мониторинг и обучение администраторов. Если IPv6 включён, но не контролируется, он может стать обходным путём для правил безопасности, настроенных только для IPv4.

Ответ 28

QoS, Quality of Service, — это набор технологий управления качеством сетевого обслуживания. QoS позволяет распределять сетевые ресурсы и задавать приоритет для определённых видов трафика. Это особенно важно, когда канал связи перегружен и одновременно работают разные сервисы: веб-сайты, облачные хранилища, видеоконференции, телефония, резервное копирование и обновления программ.

Разные приложения по-разному реагируют на задержки и потери пакетов. Например, загрузка большого файла может идти медленнее, но пользователь всё равно получит файл. Для голосового звонка или видеоконференции задержка критична. Если звуковые пакеты поступают слишком поздно, речь начинает прерываться, появляется эхо, задержки и искажения.

Основными характеристиками качества сети являются пропускная способность, задержка, джиттер и потери пакетов. Пропускная способность показывает, какой объём данных может передать канал. Задержка — время прохождения пакета. Джиттер — неравномерность задержек. Потери пакетов — количество данных, которые не дошли до получателя.

QoS может классифицировать трафик по протоколу, IP-адресу, номеру порта, VLAN, DSCP-метке или типу приложения. Затем коммутатор, маршрутизатор или firewall помещает пакеты в разные очереди. Голосовой трафик может получить высокий приоритет, видеоконференции — средний или высокий, обычный веб-трафик — стандартный, а загрузки и обновления — низкий.

Пример распределения приоритетов:

Трафик	Приоритет
IP-телефония	Высокий
Видеоконференции и онлайн-занятия	Высокий
Электронный журнал и учебные платформы	Средний
Обычный веб-трафик	Стандартный
Загрузки и резервные копии	Низкий

QoS не увеличивает физическую скорость Интернета. Если канал имеет скорость 100 Мбит/с, QoS не превратит его в 1 Гбит/с. Однако QoS позволяет использовать имеющуюся полосу разумнее и сохранять работу критичных сервисов при высокой нагрузке.

Ответ 29

Мониторинг сети — это постоянное наблюдение за состоянием сетевых устройств, серверов, каналов связи и сервисов. Основная цель мониторинга заключается в своевременном выявлении неисправностей, перегрузок, ошибок и потенциальных угроз. Без мониторинга администратор обычно узнаёт о проблемах только после жалоб пользователей.

Например, если интернет-канал перегружен, пользователи могут жаловаться на медленную работу сайтов и видеоконференций. Система мониторинга позволяет заранее увидеть, что загрузка канала достигает 95–100 процентов в определённое время. Администратор сможет настроить QoS, перенести резервное копирование на ночное время или увеличить пропускную способность канала.

Основные показатели, которые необходимо контролировать:

- Доступность маршрутизаторов, коммутаторов, серверов, NVR и точек доступа.
- Загрузку процессора и оперативной памяти устройств.
- Использование интернет-канала и портов коммутаторов.
- Потери пакетов, задержку и джиттер.
- Ошибки портов: CRC, обрывы, дуплексные несоответствия.
- Температуру оборудования.
- Свободное место на дисках серверов и систем видеозаписи.
- Состояние DHCP, DNS, VPN, файлового сервера, почты и других сервисов.
- События безопасности, попытки входа и блокировки firewall.
- Наличие резервных копий и срок действия сертификатов.

Для мониторинга часто используется протокол SNMP. Он позволяет получать с сетевых устройств информацию о состоянии интерфейсов, количестве ошибок, температуре, загрузке процессора и других параметрах. Для сбора журналов применяется syslog. Для анализа сетевых потоков могут использоваться NetFlow, sFlow и аналогичные технологии.

Примерами систем мониторинга являются Zabbix, PRTG, LibreNMS, Nagios и Grafana в сочетании с системами сбора метрик. Даже в небольшой организации полезно настроить контроль доступности маршрутизатора, интернет-канала, сервера, NVR и свободного места на дисках.

Мониторинг нужен не только для устранения аварий, но и для планирования развития сети. Накопленные данные позволяют понять, какие участки сети требуют модернизации, где появляются ошибки и когда нужно заменить оборудование.

Ответ 30

Защищённая сеть учебного заведения должна обеспечивать работу администрации, преподавателей, студентов, серверов, Wi-Fi, камер и гостей, но при этом разделять эти категории устройств по уровню доверия. Главный принцип проектирования — не помещать все устройства в одну общую сеть. Административные компьютеры, серверы, камеры, учебные классы и гостевой Wi-Fi должны быть изолированы с помощью VLAN и правил межсетевого экрана.

Пример логической структуры:

VLAN	Назначение	Подсеть
10	Администрация	10.10.10.0/24
20	Преподаватели	10.10.20.0/24
30	Компьютерные классы	10.10.30.0/23
40	Серверы	10.10.40.0/24
50	Камеры и NVR	10.10.50.0/24
60	Корпоративный Wi-Fi	10.10.60.0/24
70	Гостевой Wi-Fi	10.10.70.0/24
99	Управление оборудованием	10.10.99.0/24

На границе с Интернетом устанавливается маршрутизатор или межсетевой экран. Он выполняет NAT, VPN, фильтрацию трафика, маршрутизацию между VLAN, журналирование и контроль внешних подключений. Внутри сети применяются управляемые коммутаторы с поддержкой VLAN. Для IP-камер и точек доступа удобно использовать коммутаторы PoE.

Правила доступа должны быть строгими. Администрация и преподаватели могут обращаться к нужным серверным ресурсам. Компьютерные классы могут получать доступ к образовательным платформам и отдельным файловым ресурсам, но не должны видеть компьютеры администрации. Камеры должны передавать видеопотоки только на NVR. Гостевой Wi-Fi должен иметь доступ исключительно к Интернету.

Для Wi-Fi можно создать отдельные SSID:

College-Staff
College-Student
College-Guest

Каждый SSID должен быть связан со своей VLAN. Для сотрудников желательно применять индивидуальную аутентификацию. Для гостевой сети необходимо запретить доступ к внутренним подсетям.

Важной частью проекта является администрирование. Необходимо вести схему сети, таблицу IP-адресов, журнал оборудования, маркировку кабелей и портов. Следует регулярно обновлять прошивки, делать резервные копии конфигураций маршрутизаторов и коммутаторов, контролировать журналы событий и проверять резервное копирование серверов.

Удалённое администрирование должно выполняться через VPN, а не через открытые в Интернет интерфейсы управления. Для важных учётных записей рекомендуется многофакторная аутентификация. Также нужен план реагирования на инциденты: заражение компьютера, отказ маршрутизатора, потерю Интернета, утечку данных или несанкционированный доступ.

Сегментация является важнейшей мерой защиты, поскольку она ограничивает распространение угрозы. NIST отмечает, что разделение сети на защищённые сегменты помогает снизить последствия инцидентов, изолируя потенциально опасный трафик и устройства.[\[nist\]](#)

6. Примеры оценочных средств для проведения промежуточной аттестации

6.1 Варианты тестов для проведения

Вариант 1

1. Доступом к сети называют:

- а. взаимодействие станции (узла сети) со средой передачи данных для обмена информацией с другими станциями;
- б. взаимодействие станции со средой передачи данных для обмена информацией с другой;
- в. это установление последовательности, в которой станции получают доступ к среде передачи данных;
- г. это установление последовательности, в которой серверы получают доступ к среде передачи данных.

2. Конфликтом называется:

- а. ситуация, при которой две или более станции "одновременно" бездействуют;
- б. ситуация, при которой две или более станции "одновременно" пытаются захватить линию;
- в. ситуация, при которой два или более сервера "одновременно" пытаются захватить линию;
- г. ситуация, при которой сервер и рабочая станция "одновременно" пытаются захватить линию.

3. Дискретная модуляция это...

- а. процесс представления цифровой информации в дискретной форме;
- б. процесс представления синусоидального несущего сигнала;
- в. процесс представления на основе последовательности прямоугольных импульсов;
- г. процесс представления аналоговой информации в дискретной форме.

4. Коммуникационный протокол описывающий формат пакета данных называется:

- а. TCP/IP
- б. TCP
- в. UDP
- г. IP

5. Метод потенциального кодирования NRZ это...

- д. метод биполярного кодирования с альтернативной инверсией;
- е. метод без возвращения к нулю;
- ж. метод с потенциальным кодом с инверсией при единице;
- з. биполярный импульсный код.

6. Маршрутизация это...

- а. это правило назначения выходной линии связи данного узла связи ТКС для передачи пакета, базирующегося на информации, содержащейся в заголовке пакета (адреса отправителя и получателя), и информации о загрузке этого узла (длина очередей пакетов) и, возможно, ТКС в целом;
- б. это процесс передачи данных с одного ПК на другой ПК, когда эти ПК находятся в разных сетях;
- в. это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения;
- г. специализированный сетевой компьютер, имеющий как минимум один сетевой интерфейс и

пересылающий пакеты данных между различными сегментами сети, связывающий разнородные сети различных архитектур, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.

7. Какие способы маршрутизации существуют:

- а. централизованная, распределенная, смешанная;
- б. адаптивная, децентрализованная, смешанная;
- в. прямая, косвенная, смешанная;
- г. прямая, децентрализованная, центральная.

8. Компьютерная сеть это ...

- а. группа компьютеров связанных между собой с помощью витой пары;
- б. группа компьютеров связанных между собой;
- в. система связи компьютеров или вычислительного оборудования (серверы, маршрутизаторы и другое оборудование);
- г. группа компьютеров обменивающихся информацией.

9. Узел сети, с помощью которого соединяются две сети построенные по одинаковой технологии:

- а. мультиплексор;
- б. хаб;
- в. шлюз;
- г. мост.

10. Сервер-это?

- а. сетевая программа, которая ведёт диалог одного пользователя с другим;
- б. мощный компьютер, к которому подключаются остальные компьютеры;
- в. компьютер отдельного пользователя, подключённый в общую сеть;
- г. стандарт, определяющий форму представления и способ пересылки сообщения.

11. В компьютерной сети Интернет транспортный протокол TCP обеспечивает:

- а. передачу информации по заданному адресу
- б. способ передачи информации по заданному адресу
- в. получение почтовых сообщений
- г. передачу почтовых сообщений

12. Компьютер, подключённый к Интернету, обязательно должен иметь:

- а. Web – сайт;
- б. установленный Web – сервер;
- в. IP – адрес;
- г. брандмауэр.

13. Как по-другому называют корпоративную сеть:

- а. глобальная
- б. региональная
- в. локальная
- г. отраслевая

14. Домен-это...

- а. часть адреса, определяющая адрес компьютера пользователя в сети
- б. название программы, для осуществления связи между компьютерами
- в. название устройства, осуществляющего связь между компьютерами
- г. единица скорости информационного обмена

15. Провайдер – это:

- а. владелец узла сети, с которым заключается договор на подключение к его узлу;
- б. специальная программа для подключения к узлу сети;
- в. владелец компьютера с которым заключается договор на подключение его компьютера к узлу сети;
- г. аппаратное устройство для подключения к узлу сети.

16. Сетевой шлюз это:

- а. встроенный межсетевой экран;
- б. устройство подключения компьютера к телефонной сети
- в. устройство внешней памяти
- г. аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы.

17. Коммутация – это:

- а. это процесс передачи данных с одного ПК на другой ПК, когда эти ПК находятся в разных сетях;
- б. процесс соединения абонентов коммуникационной сети через транзитные узлы.
- в. это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения;
- г. специализированный сетевой компьютер, имеющий как минимум один сетевой интерфейс и пересылающий пакеты данных между различными сегментами сети, связывающий разнородные сети различных архитектур, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.

18. В зависимости от направления возможной передачи данных способы передачи данных по линии связи делятся на следующие типы:

- а. полусимплексный, полудуплексный, симплексный;
- б. полусимплексный, полудуплексный, дуплексный;
- в. дуплексный, полудуплексный, симплексный;
- г. симплексный, дуплексный.

19. При частотном методе уплотнении происходит:

- а. передача информации в цифровом виде;
- б. процесс распространения оптического излучения в многомодовом оптическом волокне;
- в. увеличения пропускной способности систем передачи информации;
- г. передача информационного потока по физическому каналу на соответствующей частоте – поднесущей.

20. В функции канального уровня входит:

- а. формирование кадра, контроль ошибок и повышение достоверности, обеспечение кодонезависимой передачи, восстановление исходной последовательности блоков на приемной стороне, управление потоком данных на уровне звена, устранение последствий потерь или дублирования кадров;
- б. формирование кадра, контроль ошибок и повышение достоверности, обеспечение кодозависимой передачи, восстановление исходной последовательности блоков на приемной стороне, управление потоком данных на уровне звена, устранение последствий потерь или дублирования кадров;
- в. контроль ошибок и повышение достоверности, обеспечение кодозависимой передачи, восстановление исходной последовательности блоков на передающей стороне, управление потоком данных на уровне звена, устранение последствий потерь или дублирования кадров;
- г. контроль ошибок и повышение достоверности, обеспечение кодозависимости передачи, восстановление исходной последовательности блоков на передающей стороне, управление

потоком данных на уровне звена.

Вариант-II

1. Управлением доступа к среде называют:

- а. взаимодействие станции (узла сети) со средой передачи данных для обмена информацией с другими станциями;
- б. взаимодействие станции со средой передачи данных для обмена информацией с другой;
- в. это установление последовательности, в которой станции получают доступ к среде передачи данных;
- г. это установление последовательности, в которой серверы получают доступ к среде передачи данных.

2. Типичная среда передачи данных в ЛВС это...

- а. отрезок (сегмент) коаксиального кабеля;
- б. сетевой адаптер подключенный к витой паре;
- в. маршрутизатор связанный с контроллером;
- г. среда распространения Wi-Fi.

3. Аналоговая модуляция это...

- а. процесс представления цифровой информации в дискретной форме;
- б. передача дискретных данных по каналам связи на основе последовательности прямоугольных импульсов;
- в. передача дискретных данных по каналам связи на основе синусоидального несущего сигнала;
- г. процесс представления аналоговой информации в дискретной форме.

4. Программа, взаимодействующая с сетевым адаптером называется:

- а. сетевой драйвер
- б. передающая среда
- в. мультиплексор
- г. сетевой адаптер

5. Метод потенциального кодирования АМІ это...

- а. метод биполярного кодирования с альтернативной инверсией;
- б. метод без возвращения к нулю;
- в. метод с потенциальным кодом с инверсией при единице;
- г. биполярный импульсный код.

6. Алгоритм маршрутизации это...

- а. это правило назначения выходной линии связи данного узла связи ТКС для передачи пакета, базирующегося на информации, содержащейся в заголовке пакета (адреса отправителя и получателя), и информации о загрузке этого узла (длина очередей пакетов) и, возможно, ТКС в целом;
- б. это процесс передачи данных с одного ПК на другой ПК, когда эти ПК находятся в разных сетях;
- в. это последовательность маршрутизаторов, которые должен пройти пакет от отправителя до пункта назначения;
- г. специализированный сетевой компьютер, имеющий как минимум один сетевой интерфейс и пересылающий пакеты данных между различными сегментами сети, связывающий разнородные сети различных архитектур, принимающий решения о пересылке на основании информации о топологии сети и определённых правил, заданных администратором.

7. Какие методы маршрутизации существуют:

- а. прямая, децентрализованная, адаптивная;
- б. адаптивная, децентрализованная, смешанная;
- в. прямая, фиксированная, смешанная;
- г. простая, фиксированная, адаптивная.

8. Сервер, служащий для хранения файлов, которые используются всеми рабочими станциями называется:

- а. сервер телекоммуникаций;
- б. дисковый сервер;
- в. файловый сервер;
- г. почтовый сервер.

9. Информация в компьютерных сетях передается по каналам связи в виде отдельных:

- а. сообщений;
- б. данных;
- в. посланий;
- г. пакетов.

10. Основными требованиями, предъявляемыми к алгоритму маршрутизации являются:

- а. оптимальность выбора маршрута, простота реализации, устойчивость, быстрая сходимости, гибкость реализации;
- б. прямой маршрут, помехоустойчивость;
- в. передача пакета в узел связи, передача пакета в направлении, не приводящем к минимальному времени его доставки;
- г. время доставки пакетов адресату, нагрузка на сеть, затраты ресурса в узлах связи.

11. Для соединения компьютеров в сетях используются кабели различных типов. По какому из них передаётся информация, закодированная в пучке света.

- а. витая пара;
- б. телефонный;
- в. коаксиальный;
- г. оптико – волоконный.

12. Задан адрес электронной почты в сети Интернет: user_name@mtu-net.ru. Каково имя домена верхнего уровня?

- а. ru ;
- б. mtu-net.ru;
- в. mtu-net;
- г. user-name.

13. Как называется узловой компьютер в сети:

- а. терминал
- б. модем
- в. хост-компьютер
- г. браузер.

14. Модем это...

- а. устройство передачи информации от одного компьютера к другому посредством использования телефонных линий;
- б. устройство передачи информации от сервера к рабочей станции;
- в. устройство передачи информации только внутри локальной сети;
- г. устройство передачи аналоговых сигналов от рабочей станции к серверу.

15. Брандмауэр – это:

- д. встроенный межсетевой экран;
- е. устройство подключения компьютера к телефонной сети;
- ж. устройство внешней памяти;
- з. компьютер-сервер.

16. Сетевой шлюз это:

- а. встроенный межсетевой экран;
- б. устройство подключения компьютера к телефонной сети;
- в. устройство внешней памяти;
- г. аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы.

17. Какие схемы коммутации абонентов в сетях существуют:

- а. коммутация каналов, сообщений, серверов;
- б. коммутация каналов, ячеек, сообщений, пакетов;
- в. коммутация каналов, ячеек, рабочих станций, пакетов;
- г. коммутация каналов, ячеек, рабочих станций, серверов, пакетов.

18. Коммутация пакетов это:

- а. образование непрерывного составного физического канала из последовательно соединенных отдельных канальных участков для прямой передачи данных между узлами;
- б. передача единого блока данных между транзитными компьютерами сети с временной буферизацией этого блока на диске каждого компьютера;
- в. техника коммутации абонентов, которая была специально разработана для эффективной передачи компьютерного трафика;
- г. сетевая программа, которая ведёт диалог одного пользователя с другим.

19. При уплотнении по поляризации происходит:

- а. передача информации в цифровом виде;
- б. процесс распространения оптического излучения в многомодовом оптическом волокне;
- в. увеличения пропускной способности систем передачи информации;
- г. уплотнение потоков информации с помощью оптических несущих, имеющих линейную поляризацию.

20. Байт-ориентированные протоколы обеспечивают:

- а. передачу пакетов данных, поступающих от протоколов верхних уровней, узлу назначения, адрес которого также указывает протокол верхнего уровня;
- б. возможность представления информации 8-битным расширенным двоичным кодом EBCDIC;
- в. управление передачей данных, представляемых байтами;
- г. уплотнение потоков информации с помощью оптических несущих, имеющих линейную поляризацию.

6.2 Ключи ответа тестов промежуточной аттестации

Вариант-I

Вопрос	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Ответ	<i>a</i>	<i>б</i>	<i>г</i>	<i>г</i>	<i>б</i>	<i>б</i>	<i>a</i>	<i>в</i>	<i>г</i>	<i>б</i>	<i>б</i>	<i>в</i>	<i>г</i>	<i>a</i>	<i>a</i>	<i>г</i>	<i>б</i>	<i>в</i>	<i>г</i>	<i>a</i>

Вариант-II

Вопрос	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Ответ	<i>в</i>	<i>a</i>	<i>б</i>	<i>a</i>	<i>a</i>	<i>a</i>	<i>г</i>	<i>в</i>	<i>г</i>	<i>a</i>	<i>г</i>	<i>a</i>	<i>в</i>	<i>a</i>	<i>a</i>	<i>г</i>	<i>б</i>	<i>в</i>	<i>г</i>	<i>в</i>