Федеральное государственное образовательное бюджетное учреждение высшего образования

«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

(Финансовый университет)

Кафедра информационных технологий

Факультет информационных технологий и анализа больших данных

Документ подписан усиленной неквалифицированной электронной подписью
Организация: Финансовый университет при Правительстве РФ
Утвержено: Проректор по учебной и методической работе Е.А. Каменева
Сертификат: kgrHLCcSFZ2FWc6rsxTRfo5xSRZoWVCL
Дата: 08.10.2025 г.

Г.Л. Деденко

Основы сетевого администрирования

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки:
01.04.02 - Прикладная математика и информатика,
Образовательная программа «Инженер машинного обучения»
Направленность программы:
«Инженер машинного обучения»

Рекомендовано
Факультет информационных технологий и анализа больших данных
(протокол № 03 от 16.12.2025 г.)
Одобрено
Кафедра информационных технологий
(протокол № 12 от 03.12.2025 г.)

© Москва 2026

СОДЕРЖАНИЕ

1.	Наименование дисциплины	3
2.	Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине	3
3.	Место дисциплины в структуре образовательной программы	5
4.	Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся	5
5.	Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий	6
5.1.	Содержание дисциплины	6
5.2.	Учебно-тематический план	9
5.3.	Содержание семинаров	10
6.	Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	14
6.1.	Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы	14
6.2.	Перечень вопросов, заданий, тем для подготовки к текущему контролю	18
7.	Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	23
8.	Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	30
9.	Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	31
10.	Методические указания для обучающихся по освоению дисциплины	32
11.	Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем	38
12.	Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	39

1. Наименование дисциплины

«Основы сетевого администрирования».

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции
ПК-6	Способность настраивать и управлять инфраструктурой развертывания прикладных программных решений	Демонстрировать способность настраивать и поддерживать серверную и сетевую инфраструктуру для развертывания интеллектуальных систем	**знать:** принципы IP-адресации, классы адресов, маски подсетей и механизмы маршрутизации данных;структуру и принципы работы стека протоколов TCP/IP, назначение протоколов транспортного (TCP, UDP) и прикладного уровней (HTTP, FTP);назначение и принципы работы базовых сетевых сервисов: DNS, DHCP, SMTP;принципы конфигурации сетевого оборудования (коммутаторы, маршрутизаторы), технологии VLAN и списки контроля доступа (ACL);принципы настройки безопасного удаленного доступа (VPN) и межсетевого экранирования (firewall) в Linux; **уметь:** рассчитывать количество доступных IP-адресов в подсети и настраивать статическую/динамическую адресацию;настраивать виртуальные локальные сети (VLAN) на коммутаторах для сегментации трафика;устанавливать и настраивать Linux-сервер, управлять пользователями и правами доступа;настраивать сетевые службы (SSH, DNS, DHCP) и межсетевой экран в среде Linux;
		Использовать в работе основные принципы администрирования сложных	**знать:** основные команды командной строки Linux для управления системными

		систем, инструментальные средства управления операциями разработки ПО	настройками и автоматизации задач;методы журналирования и анализа системных событий, инструменты мониторинга сетевого трафика (SNMP, Wireshark);способы оптимизации производительности и масштабируемости сетевых сервисов;принципы администрирования систем управления базами данных (СУБД), методы резервного копирования и восстановления данных; **уметь:** использовать скрипты для автоматизации рутинных задач сетевого администрирования в Linux;анализировать журналы (логи) системы и сетевых устройств для выявления и устранения сбоев;устанавливать и настраивать СУБД (MySQL/PostgreSQL), управлять базами данных, таблицами и разрешениями пользователей;выполнять процедуры резервного копирования (бэкапа) и восстановления данных прикладных систем;

3. Место дисциплины в структуре образовательной программы

Дисциплина «Основы сетевого администрирования» относится к «Модулю направленности программы магистратуры».

4. Объем дисциплины (модуля) в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Очная форма обучения

Вид учебной работы по дисциплине	**Всего (в з/е и часах)**	**Модуль 5 (в часах)**
Общая трудоёмкость дисциплины	3/108	108
Контактная работа-Аудиторные занятия	24	24
Лекции	8	8
Семинары, практические занятия	16	16
Самостоятельная работа	84	84
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	Экзамен	Экзамен

5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объемов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Введение в компьютерные сети и сетевое администрирование

Назначение и основные понятия компьютерных сетей: узел, хост, сегмент, локальная и глобальная сеть, клиент–сервер, одноранговое взаимодействие. Цели сетевого администрирования: обеспечение доступности, целостности и конфиденциальности сетевых ресурсов, поддержка пользователей и прикладных систем. Базовые модели OSI и TCP/IP, их уровни и роли в передаче данных. Типы топологий, виды сетевого оборудования (концентратор, коммутатор, маршрутизатор, точка доступа) и их функции. Сетевой администратор в ИТ-инфраструктуре организации, его задачи и зоны ответственности. Взаимосвязи сетевого администрирования с системным администрированием и обслуживанием прикладных программных решений.

Тема 2. IP-адресация, подсети и основы маршрутизации

Принципы IP-адресации в сетях IPv4: структура адреса, маска подсети, сетевой и узловой адрес, широковещательный адрес. Понятие подсетей, разбиения сети на подсети с учётом количества хостов и резервов. Частные и публичные адресные пространства, назначение шлюза по умолчанию. Основы статической и динамической маршрутизации, представления о таблице маршрутизации, порядке выбора маршрута и типичных ошибках конфигурации. Настройка адресации на рабочих станциях и серверах, проверка связности (ping, tracert/traceroute), анализ типовых проблем на уровне IP.

Тема 3. Стек протоколов TCP/IP и прикладные сетевые сервисы

Структура и работа стека TCP/IP. Функции уровней: канального (Ethernet), сетевого (IP), транспортного (TCP, UDP) и прикладного. Отличия между TCP и UDP, понятия порта, сокета, установления и завершения соединения, управление потоком и перегрузкой. Основные протоколы, используемые прикладными системами: HTTP/HTTPS, FTP, SMTP/POP3/IMAP, а также их роль в повседневной работе пользователей и сервисов. Типичные сценарии использования протоколов, их взаимодействие и влияние параметров протоколов на производительность и надёжность работы приложений. Базовые утилиты диагностики: telnet/netcat, nslookup, например, для проверки доступности сервисов.

Тема 4. Управление сетевым оборудованием: коммутаторы, маршрутизаторы, VLAN

Принципы работы коммутаторов и маршрутизаторов как ключевых компонентов сетевой инфраструктуры. Процесс коммутации кадров, таблицы MAC-адресов, отличие «умного» коммутатора от простого концентратора. Роль маршрутизатора в разделении сетей и организации выхода в Интернет. Технологии виртуальных локальных сетей (VLAN): назначение, логическая сегментация, повышение безопасности и управляемости сети. Базовые подходы к настройке оборудования: выбор интерфейсов, назначение IP-адресов, настройка VLAN и межсетевой маршрутизации, сохранение конфигурации и чтение журналов. Примеры типичной структуры офисной сети и минимально необходимого набора настроек для её функционирования.

Тема 5. Основы сетевого администрирования в Linux

Знакомство с Linux как типичной серверной ОС для сетевых задач. Варианты дистрибутивов, их структура, основные каталоги и службы. Базовые команды работы в командной строке, управление пользователями и группами, правами доступа к файлам и каталогам. Настройка сетевых параметров: задать IP-адрес, маску, шлюз, DNS-серверы, проверить маршруты и интерфейсы. Конфигурация службы удалённого доступа (SSH), организация безопасного подключения к серверу, основы работы с конфигурационными файлами. Включение Linux-сервер в сетевую инфраструктуру и предоставление сервисов для прикладных программных решений и пользователей.

Тема 6. Сетевые службы: DNS, DHCP и сервисы доступа к ресурсам

Базовые сетевые службы, без которых невозможна устойчивая работа прикладных систем. Принципы работы DNS: доменные имена, зоны, типы записей (A, CNAME, MX и др.), процесс резолюции имени в IP-адрес. Назначение DHCP, механизмы выдачи адресов, параметры аренды, резервирование адресов. Установка и базовая настройка DNS- и DHCP-служб в лабораторной среде. Сервисы доступа к файлам и ресурсам (например, FTP, простые службы обмена файлами), их настройка и ограничение доступа. Влияние корректной работы DNS- и DHCP-служб на доступность и стабильность прикладных программных решений.

Тема 7. Сетевая безопасность: межсетевые экраны, VPN и журналы событий

Основные понятия сетевой безопасности: угрозы, уязвимости, атаки, политика безопасности. Принципы работы межсетевых экранов (firewall): фильтрация по IP-адресам, портам и протоколам, концепция «запрещено всё, что не разрешено». Основы

организации защищённого удалённого доступа с помощью VPN, логика построения туннеля и шифрования трафика. Значение журналов событий (логов) сетевых устройств и серверов: какие события фиксируются, как их анализировать, какие типичные аномалии могут свидетельствовать о проблемах или атаках. Простые наборы правил для firewall, включение и проверка VPN-доступ и использование логи для базовой диагностики и аудита безопасности.

Тема 8. Сетевые аспекты работы прикладных систем и резервное копирование

Элементы сетевой инфраструктуры с потребностями прикладных программных решений. Типовые сценарии развертывания веб-приложений и СУБД в локальной сети: размещение серверов, доступ пользователей, разграничение прав. Требования приложений к сети по пропускной способности, задержкам, надёжности и безопасности. Резервное копирование как важный элемент администрирования: виды резервных копий, выбор объектов для бэкапа (конфигурации, базы данных, пользовательские данные), периодичность и хранение копий. Минимальные средства обеспечения сохранности данных и устойчивость работы прикладных систем в реальной сетевой инфраструктуре организации.

5.2. Учебно-тематический план

№ п/п	Наименование тем(разделов) дисциплины	Трудоемкость в часах				
		Всего	Контактная работа - Аудиторная работа			Самостоятельная работа
			Общая, в т.ч.:	Лекции	Семинары, практические занятия	
1	Введение в компьютерные сети и сетевое администрирование	13	3	1	2	10
2	IP-адресация, подсети и основы маршрутизации	13	3	1	2	10
3	Стек протоколов TCP/IP и прикладные сетевые сервисы	14	3	1	2	11
4	Управление сетевым оборудованием: коммутаторы, маршрутизаторы, VLAN	14	3	1	2	11
5	Основы сетевого администрирования в Linux	14	3	1	2	11
6	Сетевые службы: DNS, DHCP и сервисы доступа к ресурсам	13	3	1	2	10
7	Сетевая безопасность: межсетевые экраны, VPN и журналы событий	13	3	1	2	10
8	Сетевые аспекты работы прикладных систем и резервное копирование	14	3	1	2	11
	Итого	108	24	8	16	84

5.3. Содержание семинаров

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарах, практических занятиях	Формы проведения занятий
Введение в компьютерные сети и сетевое администрирование	Что такое компьютерная сеть, какие задачи она решает для организации. Чем отличаются локальные, глобальные и корпоративные сети, примеры из практики. Клиент–серверная и одноранговая модели: преимущества и ограничения каждой. Модели OSI и TCP/IP: уровни и их назначение, соответствия между моделями. Роль сетевого администратора: зона ответственности, типовые ежедневные задачи, взаимодействие с пользователями и разработчиками.	Семинар-беседа с опорой на наглядные схемы.Разбор простых кейсов («как организовать сеть в маленьком офисе»).Работа в малых группах: построение схемы сети, последующая защита.Мини-опрос / блиц-тест по базовым понятиям.
IP-адресация, подсети и основы маршрутизации	Структура IPv4-адреса: сеть/узел, что такое маска подсети. Чем отличаются частные и публичные IP-адреса, где какие используются. Что такое подсеть, зачем делят сеть на подсети, примеры. Таблица маршрутизации: какие записи в неё попадают и как выбирается маршрут. Типичные ошибки при настройке IP-адресации и шлюза по умолчанию, способы их диагностики.	Решение задач на разбиение сети на подсети и вычисление адресов.Практическая работа за компьютером: настройка IP и шлюза, проверка ping/traceroute.Разбор типовых ошибок конфигурации на примерах «сломанных» схем.Коллективное составление таблицы маршрутизации для простого сценария.
Стек протоколов TCP/IP и прикладные сетевые сервисы	Какие уровни включает стек TCP/IP, за что отвечает каждый уровень. Различия TCP и UDP: когда целесообразно применять тот или иной протокол. Понятия порт, сокет, установление и завершение соединения. Назначение HTTP/HTTPS, FTP, SMTP/POP3/IMAP в работе прикладных систем. Как параметры протоколов (тайм-ауты, размеры окон и т. п.) влияют на производительность приложений.	Семинар с разбором «жизненного пути» пакета по уровням стека.Практическая работа: использование telnet/netcat, nslookup для проверки сервисов.Анализ реальных заголовков TCP/IP в сниффере (Wireshark) на демонстрации

		преподавателя.Обсуждение кейсов выбора протокола (TCP vs UDP) для разных типов приложений.
Управление сетевым оборудованием: коммутаторы, маршрутизаторы, VLAN	Чем коммутатор отличается от концентратора, что такое таблица MAC-адресов. Роль маршрутизатора в сети: разграничение сегментов, выход в Интернет. Что такое VLAN, для чего используется логическая сегментация сети. Какие риски и проблемы решаются за счёт выделения отдельных VLAN. Общие принципы настройки коммутатора и маршрутизатора: адресация, сохранение конфигурации, просмотр логов.	Практическая работа в симуляторе / виртуальной лаборатории по настройке портов и VLAN.Разбор схемы типичного офисного сегмента с несколькими VLAN и роутером.Групповая работа: предложить структуру сети для заданной организации и обосновать её.Демонстрация преподавателем примеров конфигурации и их разбор.
Основы сетевого администрирования в Linux	Особенности Linux как серверной ОС: структура, основные каталоги и службы. Зачем администратору командная строка, базовые команды работы с файлами и процессами. Управление пользователями и группами: принципы разграничения доступа. Настройка сетевых параметров в Linux: IP, маска, шлюз, DNS. Роль SSH: зачем нужен удалённый доступ, базовые настройки безопасности.	Практическая работа за терминалом: выполнение базовых команд, настройка сети.Мини-лабораторная по настройке SSH-доступа к серверу.Разбор типичных ошибок в конфигурационных файлах (адреса, маршруты, DNS).Обсуждение в формате «вопрос–ответ» по отличиям Linux и Windows при администрировании сети.
Сетевые службы: DNS, DHCP и сервисы доступа к ресурсам	Зачем нужен DNS, как происходит преобразование имени в IP-адрес. Типы основных DNS-записей (A, CNAME, MX) и где они применяются. Роль DHCP в сети: какие параметры получает клиент, преимущества автоматической выдачи адресов.	Практическая работа: установка и базовая настройка DNS- и DHCP-служб в лабораторной

	Какие проблемы могут возникать при неправильной работе DNS или DHCP и как их диагностировать. Какие сервисы обеспечивают доступ к файлам и ресурсам (например, FTP), требования к их настройке и безопасности.	среде.Разбор схемы взаимодействия клиента с DNS и DHCP (последовательность сообщений).Анализ типичных сбоев («не открывается сайт», «нет IP-адреса») по логам и утилитам.Работа в группах: разработка простой структуры доменных имён для организации.
Сетевая безопасность: межсетевые экраны, VPN и журналы событий	Основные угрозы и уязвимости в локальных сетях организации. Принципы работы сетевого firewall: по каким полям фильтруется трафик. Концепция «запрещено всё, что не разрешено»: плюсы и минусы в реальной эксплуатации. Назначение VPN, чем «обычное» подключение отличается от защищённого туннеля. Какие события фиксируются в журналах сетевых устройств и серверов и как по ним обнаруживать проблемы и атаки.	Практическая работа: составление простых правил firewall и проверка их действия.Демонстрация сценария подключения через VPN и обсуждение, какие угрозы снимаются.Разбор реальных (или учебных) фрагментов логов: поиск аномалий и ошибок.Семинар-дискуссия по выработке базовой политики безопасности для небольшой организации.
Сетевые аспекты работы прикладных систем и резервное копирование	Как типичная прикладная система (веб-приложение + СУБД) использует сеть. Какие сетевые требования важны для приложений: пропускная способность, задержка, надёжность. Варианты размещения серверов приложений и БД в локальной сети, плюсы и минусы разных схем. Зачем нужно резервное копирование в сетевой инфраструктуре, какие объекты необходимо копировать. Различия полных, инкрементальных и дифференциальных копий, требования к хранению и проверке бэкапов.	Практическая работа: разбор схемы развертывания простого веб-приложения в сети.Групповое проектирование: предложить схему размещения серверов и пользователей для заданного кейса.Мини-лабораторная: создание и

		восстановление резервной копии конфигурации/БД в учебной среде.Обсуждение типичных инцидентов («упал сервер», «повредилась БД») и планов действий администратора.

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Наименование тем (разделов) дисциплины	**Перечень вопросов, отводимых на самостоятельное освоение**	**Формы внеаудиторной самостоятельной работы**
Введение в компьютерные сети и сетевое администрирование	История развития компьютерных сетей, ключевые этапы и стандарты. Различные виды топологий (шина, кольцо, звезда, «дерево», смешанные): достоинства и недостатки. Сравнение локальных, глобальных и корпоративных сетей на конкретных примерах. Подробное сопоставление уровней моделей OSI и TCP/IP. Профессии в области администрирования и поддержки сетей, типовые карьерные траектории.	Изучение рекомендованных разделов учебника и конспектирование ключевых понятий.Подготовка краткого реферата (1–2 стр.) об эволюции компьютерных сетей в организации по выбору студента.Составление схемы сети (домашней или учебной аудитории) с пояснениями к каждому элементу.Подготовка глоссария основных терминов по теме.
IP-адресация, подсети и основы маршрутизации	Правила классификации IPv4-адресов (классы, частные диапазоны). Алгоритм расчёта диапазона адресов подсети по заданной маске. Методы нумерации подсетей и распределения адресов между ними. Примеры статических и динамических маршрутов в простой сети. Сравнение ручной и автоматической настройки IP-параметров на рабочих станциях.	Решение задач по подсетям (расчёт масок, количества хостов, адресов сети/бродкаста).Составление таблицы маршрутизации для учебной схемы сети.Выполнение домашних практикумов в виртуальной среде (настройка IP, проверка связности).Подготовка краткого отчёта с примером

		проектирования адресного плана небольшого офиса.
Стек протоколов TCP/IP и прикладные сетевые сервисы	Детальное назначение каждого уровня стека TCP/IP и примеры протоколов. Механизмы установления и завершения TCP-соединения (трёхстороннее рукопожатие и др.). Сравнение TCP и UDP для типовых приложений (веб, почта, потоковое видео, игры). Форматы адресов и портов в записях брандмауэра и журналах. Примеры заголовков TCP и UDP (поля, назначение).	Изучение описаний протоколов в рекомендованной литературе и составление кратких конспектов.Анализ захваченных пакетов (по заранее подготовленным дампам) с ответами на вопросы преподавателя.Выполнение мини-практикума: проверка доступности сетевых сервисов с помощью telnet/netcat, nslookup и оформление отчёта.Подготовка сравнительной таблицы «Протокол – уровень – типичные приложения – особенности».
Управление сетевым оборудованием: коммутаторы, маршрутизаторы, VLAN	Подробный разбор работы коммутатора: формирование и обновление таблицы MAC-адресов. Основные режимы портов коммутатора, понятия trunk/access. Типичные сценарии применения VLAN в офисных и учебных сетях. Назначение и примеры использования статической маршрутизации на маршрутизаторе. Общие принципы резервирования и отказоустойчивости на уровне сетевого оборудования (на концептуальном уровне).	Моделирование работы сети в симуляторе (Packet Tracer, GNS3 и т.п.) по готовому заданию.Самостоятельное составление схемы офисной сети с указанием VLAN и связей между ними.Подготовка текстового описания базовой конфигурации коммутатора/маршрутизатора.Анализ примерных конфигурационных файлов с ответами на контрольные вопросы.
Основы сетевого администрирования в	Основные отличия файловой структуры Linux от других ОС. Команды управления файлами,	Работа в личной виртуальной машине:

Linux	каталогами, процессами, правами доступа. Механизм учётных записей пользователей и групп в Linux, файлы /etc/passwd, /etc/group. Настройка сетевых параметров в разных дистрибутивах (конфигурационные файлы, утилиты). Основы конфигурирования службы SSH (аутентификация по паролю и по ключу).	выполнение списка базовых команд с фиксацией результатов.Подготовка инструкции «Как создать пользователя и настроить ему доступ по SSH».Настройка сетевого интерфейса в виртуальной машине и проверка связности (ping, traceroute).Составление краткого справочника по основным сетевым утилитам Linux (ip, ifconfig, ping, traceroute, ssh и т.п.).
Сетевые службы: DNS, DHCP и сервисы доступа к ресурсам	Структура доменного пространства, понятия зоны и домена. Назначение основных типов DNS-записей и примеры их использования. Подробный разбор процесса получения IP-адреса клиентом от DHCP-сервера. Настройка параметров выдачи адресов: время аренды, резервирование, исключения из пула. Особенности настройки служб доступа к файлам (например, FTP) с учётом безопасности.	Настройка простого DNS- и DHCP-сервера в виртуальной среде по методическим указаниям и оформление отчёта.Составление схемы взаимодействия клиента с DNS и DHCP с пояснениями.Анализ логов DNS/DHCP (подготовленных преподавателем) и ответ на вопросы по сбоям.Подготовка мини-инструкции по организации безопасного обмена файлами в небольшой сети.
Сетевая безопасность: межсетевые экраны, VPN и журналы событий	Классификация сетевых угроз и базовые меры защиты на уровне сети. Синтаксис и семантика типичных правил для пакетного фильтра (firewall). Основные типы VPN (site-to-site, remote access) и области их применения. Структура и типы записей в журналах сетевых устройств и ОС. Примеры инцидентов, которые можно выявить по анализу логов.	Настройка набора правил firewall в учебной среде по сценарию преподавателя и фиксация результатов.Подготовка краткого описания политики

		безопасности для учебной сети (1–2 страницы).Анализ фрагментов логов (предоставленных преподавателем) с поиском подозрительных записей.Теоретическое задание: сравнение различных схем организации VPN и их плюсов/минусов.
Сетевые аспекты работы прикладных систем и резервное копирование	Типичные схемы развертывания веб-приложения и СУБД в локальной сети. Влияние параметров сети (задержка, пропускная способность, потери) на работу приложений. Критерии выбора объектов для резервного копирования в ИТ-инфраструктуре. Сравнение видов резервных копий: полные, инкрементальные, дифференциальные. Требования к хранению резервных копий и проверке их работоспособности.	Разработка схемы размещения серверов и пользователей для заданного прикладного решения.Подготовка плана резервного копирования для небольшой организации (что, как и как часто сохранять).Практическая работа в виртуальной среде: создание и восстановление тестовой резервной копии.Краткий анализ реального или учебного кейса отказа сервера/БД с предложением плана действий администратора.

6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю

Примерные вопросы к контрольной работе

Блок: Основы сетей и модели

1. Дайте определение компьютерной сети, узла и линка. В чем отличие физической топологии от логической?

2. Сравните архитектуры «Клиент–Сервер» и «Одноранговая сеть» (Peer-to-Peer): преимущества, недостатки, области применения.

3. Перечислите 7 уровней модели OSI и кратко опишите функции каждого уровня.

4. Стек протоколов TCP/IP: назовите 4 уровня и приведите примеры протоколов для каждого из них.

5. В чем заключается процесс инкапсуляции и декапсуляции данных при передаче по сети?

6. Что такое MAC-адрес? Какова его структура и на каком уровне модели OSI он используется?

7. В чем техническое различие между концентратором (hub), коммутатором (switch) и маршрутизатором (router)?

8. Структура IPv4-адреса. Что такое октет? Диапазоны значений в октете.

Блок: IP-адресация и маршрутизация

1. Классы IP-адресов (A, B, C, D, E): диапазоны и назначения. Почему классовая адресация устарела?
2. Что такое маска подсети и какую роль она играет в определении адреса сети и адреса узла?
3. CIDR-нотация (бесклассовая адресация): как расшифровать запись вида /24, /30, /16?
4 Перечислите диапазоны частных («серых») IP-адресов согласно RFC 1918. В чем их отличие от публичных («белых»)?
5. Что такое шлюз по умолчанию (Default Gateway) и что происходит, если он не указан на хосте?
6 Понятие таблицы маршрутизации. Какие типы маршрутов в ней бывают

(connected, static, dynamic)?
7. Что такое Loopback-интерфейс и адрес 127.0.0.1? Зачем они нужны?

Блок: Транспортный и прикладной уровни

1. Протокол TCP: механизм установления соединения («трехстороннее рукопожатие»).
2. Структура заголовка TCP: для чего нужны флаги SYN, ACK, FIN, RST?
3. Протокол UDP: основные отличия от TCP, преимущества и примеры использования (DNS, streaming).
4. Понятие сетевого порта (port). Диапазоны портов (well-known, registered, dynamic).
5. Протоколы прикладного уровня: назначение HTTP, FTP, SMTP, SSH. Какие стандартные порты они используют?
6. В чем разница между протоколами POP3 и IMAP при работе с электронной почтой?

Блок: Сетевые службы и Linux

1. Служба DNS: иерархия доменных имен, отличие рекурсивного запроса от итеративного.
2. Основные типы записей DNS: A, AAAA, MX, CNAME, NS, PTR.
3. Служба DHCP: процесс DORA (Discover, Offer, Request, Acknowledge). Зачем нужно время аренды (lease time)?
4. Файловая система Linux: назначение каталогов /etc, /var, /home, /bin.
5. Права доступа в Linux: чтение, запись, выполнение. Как они отображаются в символьной нотации (rwx)?
6. Пользователи и группы в Linux. Кто такой суперпользователь (root) и каковы риски работы под ним?
7. Назначение протокола SSH. Аутентификация по паролю vs аутентификация по ключам.

Блок: Безопасность и администрирование

1. Что такое VLAN? Преимущества использования виртуальных локальных сетей в организации.
2. Понятие транка (trunk) и тегирования трафика (стандарт 802.1Q).
3. Межсетевой экран (Firewall): принципы работы (stateless vs stateful). Политики «default drop» и «default allow».
4. NAT (Network Address Translation): назначение, виды (SNAT, DNAT, Masquerading).

5. VPN (Virtual Private Network): сценарии Site-to-Site и Remote Access. Что такое туннелирование?

6. Резервное копирование: полное, дифференциальное и инкрементальное. В чем разница по времени создания и времени восстановления?

7. Утилиты диагностики: назначение команд ping, traceroute, nslookup, netstat.

8. Основные логи (журналы событий) в Linux: /var/log/syslog, /var/log/auth.log. Что в них искать?

Примерные задания контрольной работы

1. Переведите маску подсети из десятичного формата 255.255.255.192 в префиксную нотацию (CIDR).

2. Для IP-адреса 192.168.10.150 и маски /24 определите адрес сети и широковещательный (broadcast) адрес.

3. Рассчитайте, сколько полезных хостов можно разместить в подсети с маской /28.

4. Дана сеть 172.16.0.0/16. Разбейте её на подсети так, чтобы в каждой было не менее 500 хостов. Укажите новую маску.

5 **.** Проанализируйте вывод команды ls -l для файла: -rwxr-x---. Запишите эти права в числовом формате (например, 777).

6 **.** Напишите команду Linux для смены владельца файла report.txt на пользователя student и группу teachers.

7. Вам нужно создать пользователя developer и добавить его в группу sudo. Напишите необходимые команды.

8. Расшифруйте строку таблицы маршрутизации: 0.0.0.0/0 via 192.168.1.1 dev eth0. Что она означает?

9. Напишите команду ping, которая отправит ровно 5 пакетов на узел google.com и покажет результат.

10. В выводе netstat вы видите строку: tcp LISTEN 0.0.0.0:80. Какая служба, вероятнее всего, слушает этот порт?

11. Сформируйте строку конфигурации для DNS-зоны, чтобы домен www.example.com указывал на IP 10.10.10.5 (запись типа A).

12. Напишите команду (например, grep), чтобы найти все строки, содержащие слово "Error", в файле /var/log/syslog.

13. Объясните, почему при попытке подключиться к серверу команда ping проходит успешно, а веб-страница в браузере не открывается.

14. Спроектируйте правило для firewall (псевдокод или iptables), которое

запрещает входящий трафик с IP-адреса 192.168.1.100.

15. Вы находитесь на сервере без графического интерфейса. Какой командой можно просмотреть текущие IP-адреса на сетевых интерфейсах?

16. Рассчитайте, какой тип резервного копирования (полный, инкрементальный, дифференциальный) займет меньше всего места на диске при ежедневном изменении 5% данных, если бэкапы хранятся неделю.

17. Определите по дампу трафика, какой протокол транспортного уровня (TCP или UDP) используется, если в заголовке пакета есть поле "Sequence Number".

18. У вас есть коммутатор. На портах 1-10 настроен VLAN 10, на портах 11-20 — VLAN 20. Компьютер из порта 2 не видит компьютер в порту 12. Объясните причину и способ решения (без смены VLAN).

19. Напишите команду SSH для подключения к серверу с IP 10.0.0.2 под пользователем admin с использованием нестандартного порта 2222.

20. При настройке DHCP вы указали диапазон 192.168.1.10 – 192.168.1.20. Сколько устройств смогут одновременно получить IP-адрес?

21. Преобразуйте двоичный IP-адрес 11000000.10101000.00000001.00000001 в десятичный формат.

22. Какую команду нужно выполнить в Linux, чтобы перезапустить службу веб-сервера (например, Apache или Nginx)?

23. Опишите последовательность действий для безопасного копирования файла data.tar с локальной машины на удаленный сервер в папку /tmp.

24. В чем ошибка конфигурации, если маска подсети указана как 255.255.255.250?

25. Вы забыли пароль root в MySQL. Опишите алгоритм сброса пароля (концептуально: остановка службы, запуск в безопасном режиме...).

26. Напишите cron-выражение для запуска скрипта резервного копирования каждый день в 3 часа ночи.

27. Что вернет команда nslookup, если DNS-сервер недоступен? Как отличить эту ошибку от ошибки «домен не найден»?

28. Приведите пример команды для добавления статического маршрута к сети 10.20.0.0/24 через шлюз 192.168.1.254.

29. Как с помощью утилиты traceroute определить, на каком узле (хопе) обрывается соединение?

30. Сравните права доступа 755 и 644. Для каких типов файлов (исполняемые скрипты, конфиги) они обычно применяются?

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях Кафедры

информационных технологий Факультета информационных технологий и анализа больших данных.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Перечень компетенций с указанием индикаторов их достижения в процессе освоения образовательной программы содержится в разделе 2. *Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения и планируемых результатов обучения по дисциплине.*

Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний

ПК-6 Способность настраивать и управлять инфраструктурой развертывания прикладных программных решений

1) Демонстрировать способность настраивать и поддерживать серверную и сетевую инфраструктуру для развертывания интеллектуальных систем

Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции

Знать: принципы IP-адресации, классы адресов, маски подсетей и механизмы маршрутизации данных; структуру и принципы работы стека протоколов TCP/IP, назначение протоколов транспортного (TCP, UDP) и прикладного уровней (HTTP, FTP); назначение и принципы работы базовых сетевых сервисов: DNS, DHCP, SMTP; принципы конфигурации сетевого оборудования (коммутаторы, маршрутизаторы), технологии VLAN и списки контроля доступа (ACL); принципы настройки безопасного удаленного доступа (VPN) и межсетевого экранирования (firewall) в Linux;

Уметь: рассчитывать количество доступных IP-адресов в подсети и настраивать статическую/динамическую адресацию; настраивать виртуальные локальные сети (VLAN) на коммутаторах для сегментации трафика; устанавливать и настраивать Linux-сервер, управлять пользователями и правами доступа; настраивать сетевые службы (SSH, DNS, DHCP) и межсетевой экран в среде Linux;

Типовые контрольные задания

Задание 1: Рассчитать маску подсети для заданного количества хостов и определить диапазон допустимых IP-адресов.

Задание 2: Сконфигурировать на виртуальном коммутаторе VLAN для разделения трафика двух отделов и настроить ACL для ограничения доступа.

Задание 3: Настроить на Linux-сервере службу SSH для безопасного входа, запретив доступ по паролю и разрешив только по ключам.

2) Использовать в работе основные принципы администрирования сложных систем, инструментальные средства управления операциями разработки ПО

Результаты обучения (умения и знания), соотнесенные с индикаторами достижения компетенции

Знать: основные команды командной строки Linux для управления системными настройками и автоматизации задач; методы журналирования и анализа системных событий, инструменты мониторинга сетевого трафика (SNMP, Wireshark); способы оптимизации производительности и масштабируемости сетевых сервисов; принципы администрирования систем управления базами данных (СУБД), методы резервного копирования и восстановления данных;

Уметь: использовать скрипты для автоматизации рутинных задач сетевого администрирования в Linux; анализировать журналы (логи) системы и сетевых устройств для выявления и устранения сбоев; устанавливать и настраивать СУБД (MySQL/PostgreSQL), управлять базами данных, таблицами и разрешениями пользователей; выполнять процедуры резервного копирования (бэкапа) и восстановления данных прикладных систем;

Типовые контрольные задания

Задание 1: Проанализировать предоставленный лог-файл (или дамп трафика Wireshark), выявить аномальную активность и предложить меры по устранению проблемы.

Задание 2: Развернуть тестовую базу данных в MySQL/PostgreSQL, создать пользователя с ограниченными правами и выполнить SQL-запрос на выборку данных.

Задание 3: Написать сценарий (или описать алгоритм) для автоматического резервного копирования базы данных по расписанию и проверить целостность копии.

Примеры практико-ориентированных заданий

Задание 1. Инвентаризация и схема сети учебного класса / домашней сети

• Выполнить обследование доступной сети (аудитория, дом, общежитие).

• Определить типы устройств (ПК, принтеры, точки доступа, маршрутизатор, коммутатор), тип подключения, примерные роли.

• Построить логическую схему сети (в любой удобной нотации), выделив сегменты, шлюз, соединения с Интернетом.

• Кратко описать, какую роль выполняет каждый элемент и какие риски/узкие места видны с точки зрения администратора.

Задание 2. Проектирование адресного плана для небольшой организации

• Дан сценарий: офис на 40–60 рабочих мест, выделенный канал в Интернет, отдельный сегмент для серверов.

• Необходимо:

Задание 3. Диагностика сетевой связности и типовых проблем IP-уровня

• На учебном стенде или в виртуальной среде заданы несколько машин с «поломанной» конфигурацией.

• Студент с помощью ping, tracert/traceroute, ipconfig/ifconfig, таблиц маршрутизации определяет:

Задание 4. Анализ трафика стека TCP/IP

• Используя сниффер (на демонстрации преподавателя или в виртуальной машине), захватить фрагмент трафика: обращение к веб-сайту, отправка письма, загрузка файла.

• Определить: какие протоколы задействованы, какие порты используются, как выглядят TCP-соединения, где видны DNS-запросы.

• Ответить на вопросы по структуре пакетов и взаимодействию протоколов на разных уровнях.

Задание 5. Настройка простейшей офисной сети на базе коммутатора и маршрутизатора

• В симуляторе или лабораторной стойке:

• Оформить конфигурации и схему сети.

Задание 6. Базовое сетевое администрирование в Linux

• В виртуальной машине с Linux:

Задание 7. Развёртывание и настройка DNS- и DHCP-служб

• На Linux-сервере (или в подготовленном образе):

Задание 8. Настройка межсетевого экрана и базовых правил фильтрации

• На маршрутизаторе или Linux-хосте:

Задание 9. Организация защищённого удалённого доступа (VPN / туннель)

• В учебной среде настроить простейший сценарий защищённого доступа:

Задание 10. Резервное копирование конфигураций и данных прикладной системы

• В лабораторной среде развернуть простой сценарий: веб-служба + небольшая база данных или набор конфигурационных файлов.

• Разработать и выполнить процедуру:

Примерные вопросы для подготовки к экзамену

1. Понятие компьютерной сети. Основные цели и задачи сетевого администрирования в организации.

2. Классификация сетей (LAN, MAN, WAN, корпоративные, домашние). Примеры и особенности администрирования.

3. Топологии сетей, их достоинства и недостатки с точки зрения надёжности и масштабируемости.

4. Модели OSI и TCP/IP: уровни, основные функции, соответствие уровней друг другу.

5. Клиент–серверная и одноранговая архитектуры. Влияние выбранной архитектуры на организацию сети и администрирование.

6. Понятия узла, хоста, сегмента, точки доступа. Основные типы сетевого оборудования и их функции.

7. Структура IPv4-адреса. Маска подсети, адрес сети, адрес хоста, широковещательный адрес. Примеры вычисления.

8. Частные и публичные диапазоны IP-адресов. Назначение шлюза по умолчанию.

9. Понятие подсети. Алгоритм разбиения сети на подсети. Пример построения адресного плана.

10. Таблица маршрутизации: типы маршрутов, порядок выбора маршрута. Пример настройки статического маршрута.

11. Основные причины отсутствия связи на уровне IP и последовательность действий администратора по их диагностике.

12. Назначение и структура стека протоколов TCP/IP. Основные протоколы на каждом уровне.

13. Протоколы TCP и UDP: отличия, механизмы установления и завершения соединения, надёжность доставки.

14. Назначение прикладных протоколов HTTP/HTTPS, FTP, SMTP/POP3/IMAP. Типичные порты и сценарии использования.

15. Понятия порта и сокета. Как используются адрес и порт при настройке сервисов и фильтрации трафика.

16. Принцип работы коммутатора. Таблица MAC-адресов, отличие коммутатора от концентратора.

17. Роль маршрутизатора в сети. Разделение сетей, организация выхода в Интернет, основные функции.

18. Понятие VLAN. Цели логической сегментации сети, примеры использования VLAN в офисе.

19. Общие принципы настройки коммутатора и маршрутизатора для простой сети: адресация, шлюзы, сохранение конфигурации.

20. Особенности Linux как серверной операционной системы. Основные каталоги и службы, роль командной строки.

21. Модель пользователей и групп в Linux. Примеры настройки прав доступа к каталогам и файлам.

22. Настройка сетевых параметров в Linux (IP, маска, шлюз, DNS) и средства проверки маршрутов и связности.

23. Назначение службы SSH. Основные параметры настройки, требования к безопасности удалённого доступа.

24. Назначение и принцип работы DNS. Понятия домена, зоны, записи A, CNAME, MX. Схема резолюции имени.

25. Назначение и принцип работы DHCP. Последовательность получения IP-адреса клиентом, основные параметры аренды.

26. Типовой сценарий совместной работы DNS- и DHCP-служб в локальной сети организации.

27. Организация сетевого доступа к файлам и ресурсам (на примере FTP или аналогичных служб). Риски и меры защиты.

28. Основные угрозы сетевой безопасности в локальных сетях: примеры атак и уязвимостей.

29. Принципы работы межсетевого экрана (firewall). Фильтрация по IP-адресам, портам, протоколам, направлениям.

30. Политика безопасности «запрещено всё, что не разрешено»: преимущества, недостатки и область применения.

31. Основная идея VPN. Отличия защищённого туннеля от обычного нешифрованного подключения. Примеры использования.

32. Назначение журналов событий (логов) сетевых устройств и ОС. Какие события важны администратору и почему.

33. Типовой сценарий развертывания веб-приложения и СУБД в локальной сети. Размещение серверов, варианты доступа пользователей.

34. Требования прикладных систем к сети (полоса пропускания, задержка, надёжность, безопасность) и их влияние на архитектуру сети.

35. Понятие резервного копирования. Основные объекты бэкапа в инфраструктуре (конфигурации, базы данных, пользовательские данные).

36. Виды резервных копий (полная, инкрементальная, дифференциальная), их достоинства и ограничения.

37. Требования к хранению резервных копий и проверке восстановления. Пример простого регламента бэкапа для небольшой организации.

Пример экзаменационного билета

Экзаменационный билет №

1. Теоретический вопрос: Стек протоколов TCP/IP. Функции уровней (канального, сетевого, транспортного, прикладного). Основные протоколы на каждом уровне (15 баллов)

2. Теоретический вопрос: Понятие VLAN. Цели логической сегментации сети, примеры использования VLAN в офисной инфраструктуре. Отличие тегированного и нетегированного трафика (15 баллов)

3. Практическая задача: Для сети 172.16.0.0/24 необходимо выделить подсеть для отдела маркетинга, в котором планируется 30 рабочих станций. Рассчитайте оптимальную маску подсети, адрес сети, адрес шлюза (первый доступный) и широковещательный адрес (30 баллов)

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Малютин, А. Г. Базовые протоколы стека TCP/IP [Электронный ресурс] : учебно-методическое пособие для самостоятельной работы / Малютин А. Г. Омск : ОмГУПС, 2021 36 с. Утверждено методическим советом университета Книга из коллекции ОмГУПС - Инженерно-технические науки https://e.lanbook.com/book/264458. [БИК ID: RU-LAN-BOOK-264458]

2. Лысиков, А. А. Изучение принципов работы протоколов в стеке TCP/IP [Электронный ресурс] : методические рекомендации к лабораторным работам по дисциплине «сети и телекоммуникации» / Лысиков А. А. Самара : ПГУТИ, 2020 77 с. Книга из коллекции ПГУТИ - Инженерно-технические науки https://e.lanbook.com/book/255488. [БИК ID: RU-LAN-BOOK-255488]

Дополнительная литература:

1. Гайнанова, Р. Ш. Разработка приложений в Visual C# для работы с базой данных MS SQL SERVER 2012 [Электронный ресурс] : учебно-методическое пособие / Гайнанова Р. Ш. Казань : КНИТУ, 2019 84 с. Книга из коллекции КНИТУ - Информатика https://e.lanbook.com/book/196072 ISBN 978-5-7882-2663-7. [БИК ID: RU-LAN-BOOK-196072]

2. Ставров, С. Г. Практикум по работе с базами данных в Microsoft Visio и СУБД Microsoft SQL Server [Электронный ресурс] : учебное пособие / Ставров С. Г.,Кочетков А. Е. Иваново : ИГЭУ, 2018 80 с. Печатается по решению редакционно-издательского совета ФГБОУВО «Ивановский государственный энергетический университет имени В.И. Ленина». Книга из коллекции ИГЭУ - Инженерно-технические науки https://e.lanbook.com/book/154589. [БИК ID: RU-LAN-BOOK-154589]

3. Мартишин, Сергей Анатольевич Базы данных.Практическое применение СУБД SQL и NoSOL-типа для применения проектирования информационных систем : Учебное пособие : Учебное пособие / Институт системного программирования Российской академии наук ; Российский государственный социальный университет 1 Москва : Издательский Дом "ФОРУМ", 2024 368 с. (Высшее образование) ВО - Бакалавриат https://znanium.com/catalog/document?id=434322

ISBN 978-5-8199-0946-1 ISBN 978-5-16-104936-5 (электр. издание) ISBN 978-5-16-018662-7 (ISBN соиздателя) . [БИК ID: RU\infra-m\znanium\bibl\2096940]

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Электронная библиотека Финансового университета (ЭБ) http://elib.fa.ru/ (http://library.fa.ru/files/elibfa.pdf)

2. Электронно-библиотечная система BOOK.RU http://www.book.ru

3. Электронно-библиотечная система "Университетская библиотека ОНЛАЙН" http://biblioclub.ru/

4. Научная электронная библиотека eLibrary.ru http://elibrary.ru

5. Информационно-образовательный портал Финуниверситета: https://org.fa.ru

6. •Электронно-библиотечная система Znanium http://www.znanium.ru/

7. •Электронно-библиотечная система издательства «ЮРАЙТ» https://urait.ru/

8. •Электронно-библиотечная система издательства Лань https://e.lanbook.com/

10. Методические указания для обучающихся по освоению дисциплины

1. Общие рекомендации по изучению дисциплины

Дисциплина «Основы сетевого администрирования» относится к числу базовых профессиональных дисциплин и направлена на формирование у обучающихся целостного представления о построении, функционировании и администрировании компьютерных сетей, а также на развитие компетенций в области настройки и сопровождения сетевой инфраструктуры, обеспечивающей работу прикладных программных решений (в том числе компетенции ПК-6).

Освоение дисциплины требует:

- регулярного посещения лекций и практических занятий;

- активного участия в обсуждениях и выполнении практических заданий;

- систематической самостоятельной работы с конспектами, учебной и справочной литературой;

- своевременного выполнения домашних и лабораторных заданий, предусмотренных рабочей программой.

Особенностью дисциплины является её практико-ориентированный характер: теоретические сведения (модели OSI и TCP/IP, IP-адресация, протоколы, сетевые службы) должны сразу закрепляться в задачах по настройке сетевых параметров, диагностике неисправностей, конфигурации сервисов в среде Linux, настройке DNS, DHCP, межсетевого экрана, простейших VPN-сценариев и процедур резервного копирования.

2. Рекомендации по работе на лекциях

1. Вести конспект.
На лекциях даётся систематизированный материал, который не всегда полностью повторяет учебник. Рекомендуется:

- фиксировать определения (узел, хост, сегмент, VLAN, подсеть, шлюз, NAT и др.);

- записывать схемы моделей OSI и TCP/IP, типовых сетей и сценариев развертывания приложений;

- отмечать типичные примеры из практики (офисная сеть, учебная сеть, сервер Linux, веб-приложение и СУБД и т.п.).

2. Выделять связи между темами.
При конспектировании обращать внимание на то, как:

- IP-адресация и маршрутизация связаны с работой прикладных протоколов;

- настройки в Linux отражаются на сетевом взаимодействии;

- настройки DNS, DHCP, firewall непосредственно влияют на доступность приложений и безопасность.

3. Задавать вопросы.
При возникновении непонимания (например, по расчёту подсетей или различию TCP/UDP, принципам работы VLAN, SSH, VPN) рекомендуется задавать уточняющие вопросы на лекции или сразу после неё, не откладывая на конец семестра.

4. Перед лекцией просматривать план темы.
Накануне занятия полезно:

- просмотреть заголовки разделов учебника по планируемой теме;

- вспомнить вопросы, которые вызывали затруднения ранее.
Это позволит воспринимать новый материал более осознанно и «встраивать» его в уже имеющуюся систему знаний.

3. Рекомендации по работе на практических и лабораторных занятиях

Практические и лабораторные занятия являются основным средством формирования навыков сетевого администрирования. Их успешное выполнение напрямую влияет на степень освоения дисциплины и уровень сформированности компетенций.

Обучающимся рекомендуется:

1. Заранее знакомиться с содержанием предстоящей работы.
Перед занятием:

- прочитать соответствующий пункт РПД, план темы, при необходимости — фрагмент учебника;

- просмотреть методические указания к лабораторной работе (если выданы заранее): понять цель, перечень шагов и ожидаемый результат.

2. Точно следовать заданию, фиксируя каждый шаг.
При выполнении работ по настройке IP-адресации, Linux, DNS, DHCP, firewall:

- записывать исходные условия (адреса, маски, пароли, имена машин/доменов);

- кратко фиксировать основные команды и фрагменты конфигурационных файлов, которые привели к нужному результату;

- отмечать типичные ошибки и способы их устранения.

3. Активно использовать средства диагностики.
При возникновении проблем:

- применять ping, tracert/traceroute, ipconfig/ifconfig, просмотр таблиц маршрутизации;

- анализировать логи (журналы событий) служб и ОС;

- не ограничиваться «перезапуском» службы, а пытаться понять причину сбоя.

4. Соблюдать аккуратность и безопасность.
При выполнении работы:

- не изменять конфигурации, выходящие за рамки задания;

- не использовать пароли, не согласованные с преподавателем;

- не подключать к учебной сети несанкционированные устройства и не запускать программное обеспечение, не предусмотренное методическими указаниями.

5. Готовить отчёт сразу по результатам занятия.
Рекомендуется оформлять отчёт в день проведения работы, пока свежи детали:

- сформулировать цель и краткий теоретический обзор;

- привести схему сети (если применимо);

- описать последовательность действий, основные команды и конфигурации;

- зафиксировать результаты тестов (ping, вывод команд, скриншоты при необходимости);

- сделать выводы, указав, чему научились в рамках работы.

4. Рекомендации по выполнению самостоятельной работы

Самостоятельная работа является неотъемлемой частью дисциплины и включает:

- решение задач по IP-адресации и маршрутизации;

- подготовку схем сетей и адресных планов;

- работу в виртуальной среде (Linux, DNS, DHCP, firewall, VPN, резервное копирование);

- подготовку небольших рефератов и глоссариев по темам.

Рекомендуется:

1. Планировать самостоятельную работу равномерно.
Не откладывать выполнение домашних заданий на конец модуля/семестра. Оптимальный режим — 2–3 подхода в неделю небольшими блоками.

2. Использовать виртуальные среды.
При отсутствии доступа к учебным стендам дома рекомендуется:

- развернуть простую виртуальную машину с Linux;

- отрабатывать в ней базовые навыки: команды, настройка сети, запуск служб.

3. Закреплять теорию через задачи.
Для тем по IP-адресации, маршрутизации, протоколам:

- решать задачи на расчёт подсетей, разработку адресного плана;

- моделировать, как изменится сеть при добавлении новых сегментов или устройств.

4. Готовить краткие конспекты по ключевым темам.
Например:

- обзор основных протоколов прикладного уровня (HTTP, FTP, SMTP и др.) с указанием портов и назначения;

- сводная таблица команд Linux для работы с сетью и пользователями;

- схема процесса работы DNS и DHCP.

5. Систематически готовиться к контрольным мероприятиям.
При подготовке к текущему и итоговому контролю:

- использовать перечни вопросов и заданий, приведённые в рабочей программе;

- повторять теорию по конспектам и учебникам;

- самостоятельно воспроизводить типовые конфигурации и команды (по памяти).

5. Рекомендации по работе с литературой и электронными ресурсами

Для успешного освоения дисциплины обучающимся следует:

1. Опираясь на список основной литературы, отработать ключевые темы курса:

- общая теория компьютерных сетей и моделей OSI/TCP/IP;

- IP-адресация, маршрутизация, протоколы;

- сетевое оборудование и логическая сегментация (VLAN);

- Linux как серверная платформа, сетевые службы;

- основы сетевой безопасности и резервного копирования.

2. Использовать дополнительную литературу и официальную документацию по следующим направлениям:

- руководство по базовым командам и службам Linux;

- документация по настройке DNS, DHCP, SSH и других сетевых сервисов;

- материалы по настройке межсетевого экрана и VPN.

3. Критически относиться к интернет-источникам.
При использовании материалов сети Интернет отдавать предпочтение:

- официальной документации;

- учебным материалам крупных образовательных и научных организаций;

- методическим материалам, рекомендованным преподавателем.
Не полагаться полностью на случайные форумы и блоги без проверки информации.

4. Вести собственный электронный архив.
Рекомендуется создавать структурированную папку:

- конспекты в электронном виде;

- примеры конфигураций (фрагменты файлов, командные сценарии);

- ссылки на наиболее полезные ресурсы.
Это упростит подготовку к итоговым контрольным мероприятиям и последующим дисциплинам.

6. Подготовка к текущему контролю и промежуточной аттестации

Текущий контроль успеваемости по дисциплине предусматривает проверку как теоретических знаний, так и практических навыков. Для успешной сдачи контрольной работы и промежуточной аттестации обучающимся рекомендуется:

1. Систематизировать знания по всем 8 темам:

- повторить базовые определения и классификации (сети, топологии, протоколы, оборудование);

- ещё раз проработать алгоритмы IP-адресации и подсетей, примеры таблиц маршрутизации;

- освежить в памяти назначение основных протоколов TCP/IP и прикладного уровня;

- просмотреть схемы типовых сетей и сценариев развертывания приложений.

2. Отработать типовые практические навыки:

- по памяти выполнить несколько задач на разбиение сети на подсети и построение адресных планов;

- продумать, какие команды Linux используются для настройки сети и проверки связности;

- вспомнить ключевые шаги по настройке DNS, DHCP, firewall и VPN в лабораторных заданиях;

- мысленно (или на бумаге) воспроизвести последовательность действий при резервном копировании и восстановлении данных.

3. Использовать перечни вопросов и практико-ориентированных заданий, приведённые в рабочей программе, как основу для самопроверки.
Полезно составить для себя карточки с вопросами и проверять, насколько быстро и полно вы можете на них ответить.

1. Анализировать выполненные ранее работы.
Перед контрольной:

- просмотреть отчёты по лабораторным и практическим заданиям;

- обратить внимание на замечания преподавателя;

- сделать выводы о типичных ошибках и продумать, как их избежать.

7. Типичные ошибки и способы их избежать

В ходе освоения дисциплины обучающиеся чаще всего сталкиваются со следующими затруднениями:

1. Механическое запоминание команд и адресов без понимания.
Способ профилактики:

- всегда пытаться объяснить себе принцип (как формируется адрес, как выбирается маршрут, что делает команда/служба).

1. Запоздалое выполнение самостоятельных заданий.
Способ профилактики:

- распределить нагрузку по неделям, фиксировать сроки выполнения работ, не накапливать «хвосты».

2. Невнимательное отношение к схемам и таблицам.
Способ профилактики:

- аккуратно чертить схемы сети и адресные планы, сверять их с реальной конфигурацией в лаборатории.

3. Игнорирование журналов и средств диагностики.
Способ профилактики:

- при любой проблеме первым делом использовать ping, tracert/traceroute, просмотр логов, а не ограничиваться «перезапуском».

4. Формальный подход к отчётам.
Способ профилактики:

- описывать не только итог («работает / не работает»), но и путь решения, ошибки и способы их исправления.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем

Комплект лицензионного программного обеспечения:

1. Python 3.8
2. Jupyter Notebook (Windows 10)
3. Текстовый редактор
4. Docker

5. Kubernets
6. Реляционная СУБД
7. Astra Linux
8. Редактор кода VS CODE
9. Kaspersky

Современные профессиональные базы данных и информационные справочные системы:

1. Информационно-правовая система «Консультант Плюс»
2. Электронная энциклопедия: http://ru.wikipedia.org/wiki/Wiki
3. СУБД MongoDB
4. Система комплексного раскрытия информации «СКРИН» - http://www.skrin.ru/
5. Информационно-правовая система «Гарант»

Сертифицированные программные и аппаратные средства защиты информации:

1. не предусмотрены

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

1. **Учебная аудитория** для проведения учебных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная оборудованием и техническими средствами обучения: мебель аудиторная (столы, стулья, доска аудиторная), набор демонстрационного оборудования (проектор, экран)

2. **Помещение для самостоятельной работы** обучающихся оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде Университета.

3. **Компьютерный класс** для проведения учебных занятий, предусмотренных программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенный оборудованием и техническими средствами обучения: мебель аудиторная (столы, стулья, доска аудиторная), персональные компьютеры, набор демонстрационного оборудования (проектор, экран)

4. Библиотека, читальный зал