МИНИСТЕРСТВО ОБРАЗОВАНИЯ СВЕРДЛОВСКОЙ ОБЛАСТИ
ГАПОУ СО
«НИЖНЕТАГИЛЬСКИЙ ТОРГОВО-ЭКОНОМИЧЕСКИЙ КОЛЛЕДЖ»

Утверждаю:
Зам. директора по УР
_____ М.Г. Дмитриева
«30» июня 2026 г.

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ

«Основы компьютерных сетей»

(ОП.09)

по специальности
09.02.12 Техническая эксплуатация и сопровождение информационных систем

Нижний Тагил 2026

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Комплект оценочных средств составлен в соответствии с требованиями федерального государственного образовательного стандарта среднего профессионального образования и примерной основной образовательной программы по специальности 09.02.12 Техническая эксплуатация и сопровождение информационных систем.

Организация-разработчик:

ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Разработчики:

Репьев Егор Денисович, преподаватель первой квалификационной категории ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Ильина Виктория Денисовна, преподаватель без квалификационной категории ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

СОДЕРЖАНИЕ

5.1 ПАСПОРТ КОМПЛЕКТА КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ.....4
5.1.1 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....4
5.1.2 ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ.....5
5.1.3 ОПИСАНИЕ ПРОЦЕДУРЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ.....5
5.1.4 КРИТЕРИИ ОЦЕНКИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ.....8
5.2 КОМПЛЕКТ «ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ».....9
5.2.1 Вопросы к экзамену.....9
5.2.2 Типовые практические задания..... 13
5.2.3 Задания для экзамена..... 14
5.3 КОМПЛЕКТ «ТЕКУЩИЙ КОНТРОЛЬ» 29
5.3.1 Задания для срезов знаний..... 29
5.3.2 Тестовые задания 30
5.3.3 Задания для проверочных, самостоятельных и контрольных работ... 38
5.3.4 Лабораторные и практические работы 44
5.3.5 Компьютерные программы для контроля знаний студентов 46

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

5.1 ПАСПОРТ КОМПЛЕКТА КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

5.1.1 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Предметом оценки освоения учебной дисциплины (УД) являются умения и знания. Контроль и оценка этих дидактических единиц осуществляются с использованием следующих форм и методов:

Таблица 1 – Формы и методы контроля и оценки дидактических единиц

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения	Наименование оценочного средства
Уметь:		
– настраивать сетевые интерфейсы, статическую и динамическую адресацию, имя узла и DNS-клиент в Debian/Ubuntu	Оценка выполнения практических работ. Контрольная работа. Экзамен.	ПР №4, 5; КР №1; билеты
– рассчитывать адреса сетей, маски и подсети (VLSM), составлять план адресации и проверять расчёты сценарием	Оценка выполнения практических работ. Тестирование. Контрольная работа. Экзамен.	ПР №2, 3; тесты 6–14; КР №1; билеты
– развёртывать и администрировать службы DHCP и DNS	Оценка выполнения практических работ. Тестирование. Экзамен.	ПР №6, 7; тесты 20–24; билеты
– настраивать VLAN и мосты Linux, статическую и динамическую маршрутизацию	Оценка выполнения практических работ. Контрольная работа. Экзамен.	ПР №8–10; КР №2; билеты
– настраивать NAT и межсетевой экран nftables/ufw	Оценка выполнения практической работы. Контрольная работа. Экзамен.	ПР №11; КР №2; билеты
– настраивать SSH по ключам, обратный прокси nginx с TLS, VPN WireGuard и SSH-туннели	Оценка выполнения практических работ. Контрольная работа. Экзамен.	ПР №12, 13; КР №2; билеты
– настраивать сети Docker и Docker Compose	Оценка выполнения практической работы. Контрольная работа. Экзамен.	ПР №14; КР №2; билеты
– диагностировать сетевые неисправности по уровням, организовывать мониторинг и резервное копирование конфигураций; выявлять сетевые инциденты (ПК 1.6, ПК 1.7)	Оценка выполнения практических работ. Контрольная работа. Экзамен.	ПР №1, 5, 15; КР №1; билеты
– безопасно использовать российские ИИ-ассистенты для диагностики сетей и разбора конфигураций с проверкой результата	Оценка выполнения практической работы. Тестирование. Экзамен.	ПР №16; тесты 45–48; билеты №21–24

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения	Наименование оценочного средства
Знать:		
– понятия сети, топологии, методы доступа, сетевые модели OSI и TCP/IP, пакетная передача	Тестирование. Контрольная работа №1. Экзамен.	Тесты 1–4; КР №1; билеты
– аппаратные компоненты сетей, технологии Ethernet и Wi-Fi	Тестирование. Экзамен.	Тесты 1, 4, 5; билеты
– адресация: MAC, IPv4, IPv6, маски и CIDR, подсети и VLSM, порты и имена	Тестирование. Контрольная работа №1. Экзамен.	Тесты 6–14; КР №1; билеты
– коммутация, VLAN, статическая и динамическая маршрутизация, трансляция адресов	Тестирование. Контрольная работа №2. Экзамен.	Тесты 25–30; КР №2; билеты
– протоколы ARP, IP, ICMP, TCP, UDP, DHCP, DNS, SSH, HTTP и TLS	Тестирование. Контрольные работы №1, 2. Экзамен.	Тесты 15–24, 33–38; КР №1, 2; билеты
– межсетевые экраны, VPN, сетевые угрозы, требования 152-ФЗ	Тестирование. Контрольная работа №2. Экзамен.	Тесты 31, 32, 36, 40; КР №2; билеты
– сети контейнеров Docker и Docker Compose, публикация портов	Тестирование. Контрольная работа №2. Экзамен.	Тесты 41–43; КР №2; билеты
– основы мониторинга сетей, документирование и резервное копирование конфигураций	Тестирование. Экзамен.	Тест 44; билеты
– возможности, ограничения и риски применения ИИ-ассистентов; требования 152-ФЗ	Тестирование. Экзамен.	Тесты 45–48; билеты №21–24

Оценка освоения УД предусматривает использование пятибалльной системы оценки.

5.1.2 ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Таблица 2 – Запланированные формы промежуточной аттестации

№ семестра	Формы промежуточной аттестации	Форма проведения
5	Экзамен	Устный ответ по билету и выполнение практического задания

5.1.3 ОПИСАНИЕ ПРОЦЕДУРЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Экзамен по дисциплине проводится в 5 семестре и устанавливает уровень сформированности умений и усвоения знаний по всему курсу. К экзамену

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

допускаются обучающиеся, выполнившие и защитившие все практические работы и получившие положительные оценки за контрольные работы. Билет содержит два теоретических вопроса (по темам разных разделов курса) и практическое задание (расчёт подсетей, анализ фрагмента конфигурации, журнала или вывода утилит). Всего в банке 24 билета. Использование ИИ-ассистентов и посторонних материалов на экзамене не допускается.

В результате освоения дисциплины студент должен уметь:

– настраивать сетевые интерфейсы, статическую и динамическую адресацию, имя узла и DNS-клиент в Debian/Ubuntu (ip, ifupdown, netplan, systemd-networkd);

– рассчитывать адреса сетей, маски, широковещательные адреса и диапазоны узлов, разбивать сети на подсети (в том числе по методу VLSM), составлять план адресации и проверять расчёты сценарием Bash или утилитой ipcalc;

– развёртывать и администрировать службы DHCP и DNS (dnsmasq, Kea, BIND9, unbound), проверять их работу утилитами dig и tcpdump;

– настраивать VLAN и мосты Linux, статическую и динамическую маршрутизацию (FRRouting, OSPF), превращать узел Linux в маршрутизатор;

– настраивать трансляцию адресов (NAT) и межсетевой экран nftables/ufw по принципу «запрещено всё, кроме разрешённого», проверять и сохранять правила;

– настраивать защищённый удалённый доступ и прикладные службы: SSH по ключам, SSH-туннели, VPN WireGuard, обратный прокси nginx с TLS;

– настраивать сети Docker и Docker Compose, публиковать порты контейнеров, не нарушая политику межсетевого экрана;

– диагностировать сетевые неисправности по уровням модели (ip, ping, mtr, ss, tcpdump, dig, curl), анализировать журналы; организовывать мониторинг доступности (Prometheus, blackbox_exporter, Grafana) и резервное копирование конфигураций в Git;

– использовать российские ИИ-ассистенты (GigaChat, Алиса AI) для диагностики сетей и разбора сетевых конфигураций с обязательной проверкой результата и соблюдением требований безопасности (обезличивание данных, ссылка на использование ИИ в отчёте).

В результате освоения дисциплины студент должен знать:

– понятия компьютерной сети, топологии, методы доступа к среде, сетевые модели OSI и TCP/IP, принципы пакетной передачи данных;

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

– аппаратные компоненты сетей: кабельные системы, сетевые адаптеры, коммутаторы, маршрутизаторы, точки доступа; технологии Ethernet и Wi-Fi;

– адресацию в сетях: MAC-адреса, IPv4 и IPv6, маски и CIDR, подсети и VLSM, частные и специальные адреса, порты и доменные имена;

– принципы коммутации, VLAN (IEEE 802.1Q), статической и динамической маршрутизации (OSPF), трансляции адресов;

– протоколы ARP, IP, ICMP, TCP, UDP, DHCP, DNS, SSH, HTTP и TLS и принципы их взаимодействия;

– принципы работы межсетевых экранов и VPN, типовые сетевые угрозы (прослушивание, ARP-спуфинг, подмена DNS, отказ в обслуживании), требования Федерального закона №152-ФЗ к защите сетевых соединений;

– особенности сетей контейнеров Docker и Docker Compose, публикации портов и их взаимодействия с правилами межсетевого экрана;

– основы мониторинга сетей (метрики доступности и задержки, оповещения), порядок документирования сети и резервного копирования конфигураций;

– возможности, ограничения и риски применения ИИ-ассистентов при диагностике и настройке сетей; правила безопасной работы с ними.

Количество заданий для студента: 3 (два теоретических вопроса и одно практическое задание)

Время выполнения каждого задания и максимальное время на проведение аттестации:

Вопрос 1 – 10 мин.

Вопрос 2 – 10 мин.

Практическое задание – 20 мин.

Всего на экзамен (с подготовкой) – 45 мин. на одного обучающегося.

Условия выполнения заданий

Помещение: лаборатория «Компьютерных сетей»

Требования охраны труда: инструктаж по технике безопасности при работе с вычислительной техникой и электрооборудованием.

Оборудование:

– компьютеры по числу экзаменуемых (при необходимости – с виртуальными машинами Debian/Ubuntu);

– проектор;

– билеты на бумажном и электронном носителях.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Перечень справочной и нормативной литературы, разрешённой для использования:

1. Непрограммируемый калькулятор;
2. Памятка по сетевым командам Linux и таблица степеней двойки, выданные преподавателем;
3. Справочные страницы man (в офлайн-режиме) – только для практического задания.

5.1.4 КРИТЕРИИ ОЦЕНКИ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Таблица 3 – Критерии оценки

Оценка	Показатели оценки
Отлично (90–100 баллов)	Студент умеет увязывать теорию с практикой (решает задачи, формулирует выводы, поясняет полученные результаты), владеет понятийным аппаратом, полно и глубоко овладел материалом, обосновывает свои суждения и даёт правильные ответы на вопросы преподавателя.
Хорошо (75–89 баллов)	Студент умеет увязывать теорию с практикой, владеет понятийным аппаратом, полно овладел материалом, но ответы содержат некоторые неточности и требуют уточнения и комментария со стороны преподавателя.
Удовлетворительно (60–74 балла)	Студент знает и понимает материал, но изложение неполное, непоследовательное, допускаются неточности в определении понятий, студент не может обосновать свои ответы на уточняющие вопросы.
Неудовлетворительно (менее 60 баллов)	Студент допускает ошибки в определении понятий, искажающие их смысл, беспорядочно и неуверенно излагает материал, делает ошибки в ответах на уточняющие вопросы.

Распределение баллов на экзамене

Задание	Максимум баллов
Теоретический вопрос 1	30
Теоретический вопрос 2	30
Практическое задание	40
Итого	100

Оценка выставляется по сумме баллов: 90–100 – «отлично», 75–89 – «хорошо», 60–74 – «удовлетворительно», менее 60 – «неудовлетворительно». В практическом задании 10 баллов начисляется за проверку результата (повторный расчёт, команды диагностики) и обоснование мер безопасности; при предложении действий, нарушающих правила безопасной работы (передача реальных адресов, паролей и ключей внешним сервисам, отключение межсетевого экрана «для проверки»), баллы за задание снижаются.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

5.2 КОМПЛЕКТ «ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ»

5.2.1 Вопросы к экзамену

1. Понятие компьютерной сети, ресурсы и службы сети. Топологии (шина, звезда, кольцо, ячеистая, смешанная) и методы доступа к среде (CSMA/CD, CSMA/CA).
2. Модель OSI: уровни, функции, блоки данных. Инкапсуляция и деинкапсуляция при передаче данных. Примеры протоколов и устройств по уровням.
3. Модель TCP/IP: уровни, соответствие модели OSI, примеры протоколов. Причины распространения модели TCP/IP.
4. Принципы пакетной передачи данных. Задержка, пропускная способность, полезная загрузка канала. Расчёт времени передачи файла по каналу.
5. Коммуникационное оборудование: концентратор, коммутатор, маршрутизатор, точка доступа. Уровень работы устройства, коллизионный и широковещательный домены.
6. Технология Ethernet: кадр, MAC-адрес, таблица коммутации. Кабельные системы: витая пара (категории, длина сегмента), оптоволокно.
7. Беспроводные сети IEEE 802.11: стандарты и диапазоны, SSID, каналы, защита WPA2/WPA3, причины нестабильной связи.
8. Протокол ARP: назначение, ARP-запрос и ответ, таблица соседей (ip neigh). Угроза ARP-спуфинга и меры защиты.
9. Адресация IPv4: маска и длина префикса, адрес сети, широковещательный адрес, диапазон узлов. Порядок расчёта по адресу и маске, число узлов в подсети.
10. Частные и специальные адреса IPv4 (RFC 1918, 127.0.0.0/8, 169.254.0.0/16, адреса для документации). Признаки, по которым узел определяет, находится ли адресат в его подсети.
11. Разбиение сети на подсети. Метод VLSM: алгоритм, выбор префикса по числу узлов, сети «точка-точка» (/30, /31). Проверка плана адресации.
12. Суммирование маршрутов (агрегирование): условия объединения сетей, пример объединения четырёх сетей /24, случай, когда объединение невозможно.
13. Адресация IPv6: формат и сокращение записи, типы адресов (global unicast, link-local, ULA, multicast), автоконфигурация SLAAC, двойной стек.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

14. Составление плана адресации организации: сегменты, резерв адресов, документирование, правила именования и хранения плана.
15. Сетевая подсистема Linux: пакет iproute2 (ip addr, ip link, ip route, ip neigh). Устаревшие команды ifconfig и route и их аналоги.
16. Настройка адресации в Debian: файл /etc/network/interfaces (ifupdown), статическая и динамическая конфигурация, имя узла и /etc/hosts, применение и откат изменений.
17. Настройка адресации в Ubuntu: netplan, systemd-networkd и NetworkManager. Структура файла netplan, команды netplan generate, try и apply, типичные ошибки.
18. Методика диагностики сети по уровням модели: порядок проверок и применяемые утилиты. Типичные неисправности и их признаки.
19. Протокол ICMP. Принцип работы ping и traceroute/mtr, роль поля TTL. Интерпретация потерь пакетов на промежуточных узлах.
20. Утилиты ss и tcpdump: назначение, основные ключи и фильтры. Чтение вывода; что нельзя делать с перехваченным трафиком (152-ФЗ).
21. Протокол DHCP: процесс получения адреса (DISCOVER, OFFER, REQUEST, ACK), аренда, порты, широковещательные сообщения. Адреса 169.254.0.0/16.
22. DHCP-сервер в Linux (dnsmasq, Kea): пул, резервирование по MAC-адресу, параметры шлюза и DNS, DHCP relay. Угрозы: чужой DHCP-сервер, истощение пула.
23. Система DNS: иерархия, рекурсивный и авторитетный серверы, зоны, делегирование, кэш и TTL.
24. Типы записей DNS (A, AAAA, CNAME, MX, TXT, NS, SOA, PTR). Прямая и обратная зоны, разбор ответа утилиты dig.
25. Установка и проверка DNS-сервера BIND9 (named-checkconf, named-checkzone), кэширующий резолвер unbound. Порядок разрешения имени в Linux: /etc/hosts, nsswitch.conf, resolv.conf, systemd-resolved.
26. Безопасность DNS: открытые рекурсивные серверы, подмена ответов, DNSSEC (общие сведения), контроль доступа к рекурсии.
27. Коммутация кадров: обучение таблицы MAC-адресов, широковещательный шторм, петли и протокол STP (общие сведения).
28. VLAN: назначение, стандарт IEEE 802.1Q, тег, access- и trunk-порты, native VLAN. Межсетевое взаимодействие VLAN.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

29. Мосты Linux и VLAN-aware bridge: команды ip link и bridge vlan. Меры безопасности коммутации (отключение неиспользуемых портов, VLAN управления).
30. Таблица маршрутизации, шлюз по умолчанию, метрика. Правило наиболее длинного префикса. Утилита ip route get.
31. Маршрутизатор на базе Linux: параметр net.ipv4.ip_forward, постоянное сохранение (sysctl.d), статические маршруты. Типичные причины отсутствия связи между подсетями.
32. Статическая и динамическая маршрутизация. Сравнение RIP и OSPF, понятие автономной системы и BGP (общие сведения).
33. Протокол OSPF в FRRouting: области, роутер-идентификатор, соседи, анонсирование сетей. Причины, по которым соседство не устанавливается.
34. Трансляция сетевых адресов: SNAT, DNAT, PAT (masquerade), проброс портов. Почему NAT не является средством защиты.
35. Межсетевой экран: фильтрация без отслеживания и с отслеживанием состояния (conntrack), политика «запрещено всё, кроме разрешённого», порядок правил.
36. nftables: таблицы, цепочки input, forward, output и правила; проверка синтаксиса и сохранение; надстройка ufw. Риск потери доступа при удалённой настройке.
37. Признаки сетевых инцидентов (подбор паролей SSH, сканирование портов, всплеск трафика) и источники данных для их обнаружения. Действия при обнаружении инцидента (ПК 1.7).
38. Правило наиболее длинного префикса и суммарные маршруты: приведите пример таблицы из четырёх записей и определите маршрут для трёх адресов.
39. Транспортный уровень: порты и сокеты. Сравнение протоколов TCP и UDP, примеры приложений. Состояния сокета в выводе ss.
40. Протокол TCP: трёхстороннее рукопожатие и завершение соединения, состояния LISTEN, ESTABLISHED, TIME_WAIT.
41. Протокол TCP: порядковые номера и подтверждения, скользящее окно, управление потоком и перегрузкой, повторная передача.
42. SSH: аутентификация по ключам, файл known_hosts, укрепление конфигурации sshd (запрет входа root и по паролю), защита от подбора паролей (fail2ban).
43. Протокол HTTP: структура запроса и ответа, методы, коды состояния, заголовки. Утилита curl. Принципы HTTP/2.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

44. HTTP: cookies и их атрибуты, кэширование (Cache-Control, ETag, ответ 304). Что передавать в заголовках, а что – нельзя.
45. Протокол TLS и HTTPS: назначение, рукопожатие, сертификат X.509, цепочка доверия, SNI. Самоподписанные сертификаты и Let's Encrypt (принцип).
46. Обратный прокси nginx: проксирование на приложение, перенаправление с HTTP на HTTPS, заголовки безопасности, проверка конфигурации (nginx -t).
47. Электронная почта: SMTP, IMAP, запись MX, понятие SPF. Порты и безопасность соединения.
48. Виртуальные частные сети: назначение, типы (site-to-site, remote access), сравнение WireGuard, OpenVPN и IPsec на уровне принципов.
49. WireGuard: пары ключей, разделы [Interface] и [Peer], AllowedIPs, Endpoint. SSH-туннели. Хранение закрытых ключей. Требования 152-ФЗ к защите каналов.
50. Сети Docker: драйверы bridge, host, none, overlay. Мост docker0, пользовательские сети, встроенный DNS и разрешение имён контейнеров.
51. Публикация портов контейнеров и правила nftables/iptables, создаваемые Docker. Риск обхода правил ufw. Привязка публикации к 127.0.0.1.
52. Docker Compose: сети frontend и backend, параметр internal, изоляция базы данных. Недопустимость хранения секретов в репозитории.
53. Мониторинг сети: метрики доступности и задержки, пороги, оповещения. Prometheus, blackbox_exporter, Grafana; SNMP (общие сведения).
54. Документирование сети и резервное копирование конфигураций: схемы, таблица адресации, Git (GitVerse). Регламент реагирования на сетевой инцидент и запись в журнал.
55. Российские ИИ-ассистенты (GigaChat, GigaCode, Алиса AI, YandexGPT): назначение и возможности. Что можно поручить ИИ в сетевом администрировании и как сформулировать запрос.
56. Риски применения ИИ-ассистентов при работе с сетями: ошибки в расчётах, несуществующие параметры, устаревшие команды, небезопасные рекомендации, утечка данных.
57. Проверка результата ИИ: синтаксический контроль (nft -c, nginx -t, netplan generate, named-checkconf, docker compose config), расчёт сценарием, сверка с документацией, испытание на стенде с откатом.
58. Правила безопасной работы с ИИ-ассистентами: обезличивание конфигураций и журналов, запрет передачи паролей, ключей и

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

персональных данных (152-ФЗ), указание использования ИИ в отчёте, запрет на экзамене. Приведите пример небезопасной рекомендации ИИ и её разбор.

5.2.2 Типовые практические задания

1. Выполните в draw.io логическую схему сети небольшой организации: головной офис (рабочие места, серверы, точка доступа Wi-Fi), два филиала, выход в Интернет через маршрутизатор. Обозначьте устройства, интерфейсы, подсети и адреса шлюзов, приложите таблицу адресации.
2. Для узла 172.19.200.17/20 определите маску, адрес сети, широковещательный адрес, диапазон узлов и число узлов. Проверьте результат сценарием Bash и утилитой ipcalc, сопоставьте результаты. Эталон: маска 255.255.240.0; сеть 172.19.192.0/20; broadcast 172.19.207.255; узлы 172.19.192.1 – 172.19.207.254; число узлов 4094.
3. Выполните распределение сети 192.168.80.0/24 по методу VLSM для подразделений: «Бухгалтерия» – 90 узлов, «Отдел продаж» – 45, «Серверы» – 20, «Принтеры» – 6, канал «точка-точка» – 2. Заполните таблицу и проверьте отсутствие пересечений. Эталон: Бухгалтерия – 192.168.80.0/25, узлы 192.168.80.1 – 192.168.80.126, broadcast 192.168.80.127; Отдел продаж – 192.168.80.128/26, узлы 192.168.80.129 – 192.168.80.190, broadcast 192.168.80.191; Серверы – 192.168.80.192/27, узлы 192.168.80.193 – 192.168.80.222, broadcast 192.168.80.223; Принтеры – 192.168.80.224/29, узлы 192.168.80.225 – 192.168.80.230, broadcast 192.168.80.231; Канал – 192.168.80.232/30, узлы 192.168.80.233 – 192.168.80.234, broadcast 192.168.80.235.
4. Настройте в Ubuntu статический адрес 192.168.10.20/24 со шлюзом 192.168.10.1 и DNS-сервером 192.168.10.2 с помощью netplan, примените настройку безопасным способом (netplan try) и проверьте результат командами ip addr, ip route, resolvectl status.
5. Настройте в Debian интерфейс eth1 со статическим адресом 172.16.5.10/24, шлюзом 172.16.5.1 и DNS 172.16.5.2 в файле /etc/network/interfaces; задайте имя узла srv-net01 и запись в /etc/hosts; примените настройку и проверьте её.
6. Разверните DHCP-сервер dnsmasq для сети 192.168.30.0/24: пул 192.168.30.100 – 192.168.30.200, шлюз 192.168.30.1, DNS 192.168.30.2, резервирование адреса 192.168.30.250 по MAC-адресу. Получите адрес на клиенте и зафиксируйте обмен DISCOVER, OFFER, REQUEST, ACK в tcpdump.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

7. Создайте в BIND9 прямую зону lab.test с записями NS, A, CNAME и MX и обратную зону для сети 192.0.2.0/24. Проверьте файлы командами named-checkconf и named-checkzone, выполните запросы dig для каждого типа записи и сравните с ответом кэширующего резолвера unbound.
8. Создайте VLAN-aware bridge br0 на Linux: порты eth1 и eth2 – access VLAN 10, порт eth3 – access VLAN 20, порт eth4 – trunk для VLAN 10 и 20. Подтвердите изоляцию VLAN перехватом трафика и опишите, как организовать связь между VLAN.
9. Превратите Linux-узел в маршрутизатор между сетями 192.168.1.0/24 и 192.168.2.0/24: включите пересылку (с сохранением после перезагрузки), настройте шлюзы на клиентах и статический маршрут к третьей сети 10.9.0.0/24 через 192.168.2.254; проверьте ip route get и mtr.
10. Настройте OSPF в FRRouting на трёх виртуальных маршрутизаторах, соединённых в цепочку; проверьте таблицу соседей и маршрутов, отключите один канал и опишите изменение маршрутов.
11. Настройте на шлюзе nftables: политика drop для цепочки forward, пересылка из сети eth1 в eth0 разрешена, masquerade для исходящих через eth0, проброс порта 8080 на узел 192.168.5.10:80; проверьте синтаксис (nft -c -f), сохраните правила и проверьте их после перезагрузки.
12. Настройте вход по SSH-ключам и обратный прокси nginx с самоподписанным сертификатом для приложения на 127.0.0.1:8000, перенаправление с HTTP на HTTPS; проверьте конфигурацию (nginx -t, sshd -t) и сертификат (openssl s_client).
13. Создайте VPN WireGuard между двумя узлами стенда: сеть туннеля 10.8.0.0/24, на клиенте в туннель направляется только трафик к сети 192.168.5.0/24; проверьте рукопожатие (wg show) и маршрут (ip route get).
14. Составьте для GigaChat или Алиса AI обезличенный запрос на разбор вывода ip route и nft list ruleset, проверьте полученные рекомендации синтаксическим контролем и сверкой с документацией, оформите отчёт об использовании ИИ (запрос, ответ, проверка, решение).

5.2.3 Задания для экзамена

Экзаменационный билет №1

Вопрос 1

Понятие компьютерной сети, ресурсы и службы сети. Топологии (шина, звезда, кольцо, ячеистая, смешанная) и методы доступа к среде (CSMA/CD, CSMA/CA).

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Вопрос 2

Коммутация кадров: обучение таблицы MAC-адресов, широковещательный шторм, петли и протокол STP (общие сведения).

Практическое задание

Для узла 10.44.77.200/21 определите маску, адрес сети, широковещательный адрес, диапазон узлов и число узлов. Напишите фрагмент сценария Bash, вычисляющий адрес сети.

Эталон практического задания (для преподавателя). маска 255.255.248.0; сеть 10.44.72.0/21; broadcast 10.44.79.255; узлы 10.44.72.1 – 10.44.79.254; число узлов 2046. Bash: IFS=. read -r a b c d <<< "10.44.77.200"; m=$(((0xFFFFFFFF << (32-21)) & 0xFFFFFFFF)); ip=$(((a<<24)|(b<<16)|(c<<8)|d)); net=$((ip & m)); echo "$((net>>24&255)).$((net>>16&255)).$((net>>8&255)).$((net&255))". Результат: 10.44.72.0.

Экзаменационный билет №2

Вопрос 1

Модель OSI: уровни, функции, блоки данных. Инкапсуляция и деинкапсуляция при передаче данных. Примеры протоколов и устройств по уровням.

Вопрос 2

VLAN: назначение, стандарт IEEE 802.1Q, тег, access- и trunk-порты, native VLAN. Межсетевое взаимодействие VLAN.

Практическое задание

Головной офис и три филиала получают сеть 10.50.0.0/22. Требуется: рабочие места головного офиса – 200 узлов, серверы – 60, филиал А – 50, филиал Б – 25, филиал В – 12, три канала «точка-точка» по 2 узла. Выполните распределение по методу VLSM, заполните таблицу и объясните порядок.

Эталон практического задания (для преподавателя). Подсети распределяются от большей к меньшей, каждая начинается на границе, кратной её размеру; остаток сети остаётся резервом.

Подсеть	Требуется узлов	Сеть	Маска	Диапазон узлов	Broadcast	Доступно узлов
Головной офис: рабочие места	200	10.50.0.0/24	255.255.255.0	10.50.0.1 – 10.50.0.254	10.50.0.255	254
Головной офис: серверы	60	10.50.1.0/26	255.255.255.192	10.50.1.1 – 10.50.1.62	10.50.1.63	62
Филиал А	50	10.50.1.64/26	255.255.255.192	10.50.1.65 – 10.50.1.126	10.50.1.127	62
Филиал Б	25	10.50.1.128/27	255.255.255.224	10.50.1.129 – 10.50.1.158	10.50.1.159	30
Филиал В	12	10.50.1.160/28	255.255.255.240	10.50.1.161 – 10.50.1.174	10.50.1.175	14
Канал ГО–А	2	10.50.1.176/30	255.255.255.252	10.50.1.177 – 10.50.1.178	10.50.1.179	2
Канал ГО–Б	2	10.50.1.180/30	255.255.255.252	10.50.1.181 – 10.50.1.182	10.50.1.183	2
Канал ГО–В	2	10.50.1.184/30	255.255.255.252	10.50.1.185 – 10.50.1.186	10.50.1.187	2

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Экзаменационный билет №3

Вопрос 1

Модель TCP/IP: уровни, соответствие модели OSI, примеры протоколов. Причины распространения модели TCP/IP.

Вопрос 2

Мосты Linux и VLAN-aware bridge: команды ip link и bridge vlan. Меры безопасности коммутации (отключение неиспользуемых портов, VLAN управления).

Практическое задание

Узлы 192.168.14.130/26, 192.168.14.190/26 и 192.168.14.194/26 подключены к одному коммутатору. Определите, какие из них могут обмениваться данными без маршрутизатора, и объясните причину.

Эталон практического задания (для преподавателя). Первые два узла принадлежат сети 192.168.14.128/26 (узлы 192.168.14.129 – 192.168.14.190) и обмениваются данными напрямую. Третий узел принадлежит сети 192.168.14.192/26; для обмена с ним нужен маршрутизатор (шлюз), так как узел определяет принадлежность адресата своей подсети по маске.

Экзаменационный билет №4

Вопрос 1

Принципы пакетной передачи данных. Задержка, пропускная способность, полезная загрузка канала. Расчёт времени передачи файла по каналу.

Вопрос 2

Таблица маршрутизации, шлюз по умолчанию, метрика. Правило наиболее длинного префикса. Утилита ip route get.

Практическое задание

Маршрутизатор должен объявлять соседу одну суммарную запись вместо четырёх: 10.60.4.0/24 – 10.60.7.0/24. Найдите суммарный маршрут и обоснуйте. Можно ли так же объединить сети 10.60.2.0/24 – 10.60.5.0/24?

Эталон практического задания (для преподавателя). 10.60.4.0/22: третий октет 4–7 (двоичные 000001xx) совпадает по 6 битам, префикс 24 − 2 = 22. Сети 10.60.2.0/24 – 10.60.5.0/24 одной записью объединить нельзя: блок из четырёх сетей начинается на границе, кратной 4, а 2 не кратно 4; получатся две записи: 10.60.2.0/23, 10.60.4.0/23.

Экзаменационный билет №5

Вопрос 1

Коммуникационное оборудование: концентратор, коммутатор, маршрутизатор, точка доступа. Уровень работы устройства, коллизионный и широковещательный домены.

Вопрос 2

Маршрутизатор на базе Linux: параметр net.ipv4.ip_forward, постоянное сохранение (sysctl.d), статические маршруты. Типичные причины отсутствия связи между подсетями.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Практическое задание

Таблица маршрутов: 0.0.0.0/0 – шлюз 10.9.0.1; 10.9.0.0/16 – шлюз 10.9.0.2; 10.9.64.0/18 – шлюз 10.9.0.3; 10.9.70.0/24 – шлюз 10.9.0.4. Определите маршрут для адресов 10.9.70.15, 10.9.80.2, 10.9.9.9, 203.0.113.8 и объясните правило выбора.

Эталон практического задания (для преподавателя). Выбирается запись с наибольшей длиной префикса, в которую входит адрес: 10.9.70.15 – 10.9.70.0/24 (шлюз 10.9.0.4); 10.9.80.2 – 10.9.64.0/18 (шлюз 10.9.0.3); 10.9.9.9 – 10.9.0.0/16 (шлюз 10.9.0.2); 203.0.113.8 – 0.0.0.0/0 (шлюз 10.9.0.1).

Экзаменационный билет №6

Вопрос 1

Технология Ethernet: кадр, MAC-адрес, таблица коммутации. Кабельные системы: витая пара (категории, длина сегмента), оптоволокно.

Вопрос 2

Статическая и динамическая маршрутизация. Сравнение RIP и OSPF, понятие автономной системы и BGP (общие сведения).

Практическое задание

Администратор настроил netplan на узле 192.168.10.20/24 (фрагмент ниже). Узел не имеет доступа к другим сетям. Найдите ошибки, исправьте и опишите, как безопасно применить настройки при удалённом доступе.

```
network:
  version: 2
  ethernets:
    eth0:
      addresses: [192.168.10.20/24]
      gateway4: 192.168.11.1
      nameservers:
        addresses: [192.168.10.2]
```

Эталон практического задания (для преподавателя). Шлюз 192.168.11.1 не принадлежит сети 192.168.10.0/24 (проверка: не принадлежит); параметр gateway4 устарел. Исправление:

```
network:
  version: 2
  ethernets:
    eth0:
      addresses: [192.168.10.20/24]
      routes:
        - to: default
          via: 192.168.10.1
      nameservers:
        addresses: [192.168.10.2]
```

Применение: netplan generate (проверка), netplan try (автоматический откат через 120 с без подтверждения), затем netplan apply; проверка ip route, resolvectl status.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Экзаменационный билет №7

Вопрос 1

Беспроводные сети IEEE 802.11: стандарты и диапазоны, SSID, каналы, защита WPA2/WPA3, причины нестабильной связи.

Вопрос 2

Протокол OSPF в FRRouting: области, роутер-идентификатор, соседи, анонсирование сетей. Причины, по которым соседство не устанавливается.

Практическое задание

На рабочей станции 192.168.10.50/24 команда ping 192.168.10.1 успешна, ping 77.88.8.8 успешна, а ping ya.ru завершается сообщением «Temporary failure in name resolution». Определите уровень неисправности, порядок дальнейших проверок и способ устранения.

Эталон практического задания (для преподавателя). Сеть до внешнего адреса работает (уровни 1–4 в порядке), неисправно разрешение имён (прикладной уровень, DNS). Проверки: cat /etc/resolv.conf и resolvectl status (адрес DNS-сервера), dig @192.168.10.2 ya.ru (отвечает ли сервер), dig @77.88.8.8 ya.ru (работает ли внешний резолвер), порт 53 UDP/TCP в межсетевом экране. Устранение: исправить DNS в netplan или DHCP-параметрах, перезапустить systemd-resolved; зафиксировать результат в протоколе диагностики.

Экзаменационный билет №8

Вопрос 1

Протокол ARP: назначение, ARP-запрос и ответ, таблица соседей (ip neigh). Угроза ARP-спуфинга и меры защиты.

Вопрос 2

Трансляция сетевых адресов: SNAT, DNAT, PAT (masquerade), проброс портов. Почему NAT не является средством защиты.

Практическое задание

Фрагмент конфигурации dnsmasq (сервер имеет адрес 192.168.30.2/24 на интерфейсе eth1). Клиенты получают адрес, но не могут выйти за пределы подсети. Найдите ошибку, укажите размер пула и объясните резервирование.

```
interface=eth1
dhcp-range=192.168.30.100,192.168.30.200,255.255.255.0,12h
dhcp-option=option:router,192.168.31.1
dhcp-option=option:dns-server,192.168.30.2
dhcp-host=aa:bb:cc:dd:ee:01,192.168.30.250
```

Эталон практического задания (для преподавателя). Шлюз 192.168.31.1 не принадлежит сети 192.168.30.0/24; верный параметр: dhcp-option=option:router,192.168.30.1. Пул 192.168.30.100 – 192.168.30.200: 101 адрес. Строка dhcp-host закрепляет адрес 192.168.30.250 за MAC-адресом aa:bb:cc:dd:ee:01 (адрес вне динамического пула, что допустимо). Проверка: dnsmasq --test, journalctl -u dnsmasq, tcpdump -i eth1 port 67 or port 68.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Экзаменационный билет №9

Вопрос 1

Адресация IPv4: маска и длина префикса, адрес сети, широковещательный адрес, диапазон узлов. Порядок расчёта по адресу и маске, число узлов в подсети.

Вопрос 2

Межсетевой экран: фильтрация без отслеживания и с отслеживанием состояния (conntrack), политика «запрещено всё, кроме разрешённого», порядок правил.

Практическое задание

В файле зоны example.test (фрагмент ниже) обнаружена ошибка, из-за которой named-checkzone завершается с ошибкой. Найдите её, исправьте и запишите PTR-запись для узла 192.0.2.80.

```
$TTL 3600
@    IN SOA ns1.example.test. admin.example.test. ( 2026090101 3600 900
604800 300 )
@    IN NS  ns1.example.test.
ns1  IN A   192.0.2.53
web  IN A   192.0.2.80
www  IN CNAME web
ftp  IN CNAME 192.0.2.80
@    IN MX  10 mail.example.test.
mail IN A   192.0.2.25
```

Эталон практического задания (для преподавателя). ftp IN CNAME web.example.test. (или ftp IN A 192.0.2.80); CNAME должен указывать на доменное имя, а не на IP-адрес. PTR: 80 IN PTR web.example.test. в зоне 2.0.192.in-addr.arpa (полное имя 80.2.0.192.in-addr.arpa); после правки увеличить серийный номер и проверить named-checkzone.

Экзаменационный билет №10

Вопрос 1

Частные и специальные адреса IPv4 (RFC 1918, 127.0.0.0/8, 169.254.0.0/16, адреса для документации). Признаки, по которым узел определяет, находится ли адресат в его подсети.

Вопрос 2

nftables: таблицы, цепочки input, forward, output и правила; проверка синтаксиса и сохранение; надстройка ufw. Риск потери доступа при удалённой настройке.

Практическое задание

Коммутатор Linux (VLAN-aware bridge br0) должен обеспечить: порты eth1, eth2 – access VLAN 10; порт eth3 – access VLAN 20; порт eth4 – trunk для VLAN 10 и 20. Запишите команды и способ проверки.

Эталон практического задания (для преподавателя). ip link add name br0 type bridge vlan_filtering 1; ip link set eth1 master br0; ip link set eth2 master br0; ip link set eth3 master br0; ip link set eth4 master br0; bridge vlan add dev eth1 vid 10 pvid untagged; bridge vlan add dev eth2 vid 10 pvid untagged; bridge vlan add dev eth3 vid 20 pvid untagged; bridge vlan add dev eth4 vid 10; bridge vlan add dev eth4 vid 20; ip link set br0 up. Проверка: bridge vlan show, ip -d link show br0; узлы в разных VLAN не должны

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

видеть друг друга на канальном уровне; связь между VLAN возможна только через маршрутизатор.

Экзаменационный билет №11

Вопрос 1

Разбиение сети на подсети. Метод VLSM: алгоритм, выбор префикса по числу узлов, сети «точка-точка» (/30, /31). Проверка плана адресации.

Вопрос 2

Признаки сетевых инцидентов (подбор паролей SSH, сканирование портов, всплеск трафика) и источники данных для их обнаружения. Действия при обнаружении инцидента (ПК 1.7).

Практическое задание

Клиент 192.168.1.10/24 (шлюз 192.168.1.1) не может обратиться к узлу 192.168.2.10/24. На шлюзе, имеющем интерфейсы eth1 (192.168.1.1/24) и eth2 (192.168.2.1/24), команда sysctl net.ipv4.ip_forward выводит «net.ipv4.ip_forward = 0». Объясните причину, исправление и проверку.

Эталон практического задания (для преподавателя). Узел-шлюз не пересылает пакеты между интерфейсами. Включение: sysctl -w net.ipv4.ip_forward=1; для сохранения – строка net.ipv4.ip_forward=1 в файле /etc/sysctl.d/99-forward.conf и sysctl --system. Дополнительно: на узле 192.168.2.10 шлюзом должен быть 192.168.2.1; в цепочке forward межсетевого экрана должна быть разрешена пересылка. Проверка: ip route get 192.168.2.10 на клиенте, mtr 192.168.2.10, tcpdump на eth2.

Экзаменационный билет №12

Вопрос 1

Суммирование маршрутов (агрегирование): условия объединения сетей, пример объединения четырёх сетей /24, случай, когда объединение невозможно.

Вопрос 2

Правило наиболее длинного префикса и суммарные маршруты: приведите пример таблицы из четырёх записей и определите маршрут для трёх адресов.

Практическое задание

Два маршрутизатора FRRouting соединены сетью 10.0.12.0/30. Соседство OSPF не устанавливается (show ip ospf neighbor пуст). Конфигурации R1 и R2 ниже. Найдите причину и исправьте.

R1:

```
router ospf
 ospf router-id 1.1.1.1
 network 10.0.12.0/30 area 0
 network 192.168.1.0/24 area 0
```

R2:

```
router ospf
 ospf router-id 2.2.2.2
 network 10.0.12.0/30 area 1
 network 192.168.2.0/24 area 1
```


ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Эталон практического задания (для преподавателя). Интерфейсы канала между маршрутизаторами находятся в разных областях (R1 – area 0, R2 – area 1): соседство в таком случае не устанавливается, так как область указывается в пакетах Hello. Исправление: на R2 указать network 10.0.12.0/30 area 0 (и network 192.168.2.0/24 area 0 для единой области). Проверка: show ip ospf neighbor (состояние Full), show ip route ospf.

Экзаменационный билет №13

Вопрос 1

Сетевая подсистема Linux: пакет iproute2 (ip addr, ip link, ip route, ip neigh). Устаревшие команды ifconfig и route и их аналоги.

Вопрос 2

Транспортный уровень: порты и сокеты. Сравнение протоколов TCP и UDP, примеры приложений. Состояния сокета в выводе ss.

Практическое задание

Напишите правила nftables для сервера: входящий трафик по умолчанию запрещён; разрешены петлевой интерфейс, ответные пакеты, SSH только из сети 192.168.10.0/24, HTTP и HTTPS из любых сетей, ping с ограничением частоты. Укажите, как проверить синтаксис и сохранить правила.

Эталон практического задания (для преподавателя). Пример:

```
table inet filter {
  chain input {
    type filter hook input priority 0; policy drop;
    iifname "lo" accept
    ct state established,related accept
    ip saddr 192.168.10.0/24 tcp dport 22 accept
    tcp dport { 80, 443 } accept
    icmp type echo-request limit rate 5/second accept
  }
}
```

Проверка синтаксиса: nft -c -f /etc/nftables.conf; применение: systemctl restart nftables; сохранение – файл /etc/nftables.conf и systemctl enable nftables. При удалённой настройке сначала открыть вторую сессию SSH.

Экзаменационный билет №14

Вопрос 1

Настройка адресации в Debian: файл /etc/network/interfaces (ifupdown), статическая и динамическая конфигурация, имя узла и /etc/hosts, применение и откат изменений.

Вопрос 2

Протокол TCP: трёхстороннее рукопожатие и завершение соединения, состояния LISTEN, ESTABLISHED, TIME_WAIT.

Практическое задание

Проанализируйте набор правил nftables и укажите не менее трёх уязвимостей. Предложите исправленный набор (доступ к MariaDB нужен только узлу 192.168.20.5).

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

```
table inet filter {
  chain input {
    type filter hook input priority 0; policy accept;
    tcp dport 22 accept
    tcp dport 3306 accept
  }
}
```

Эталон практического задания (для преподавателя). Политика accept для входящего трафика (разрешено всё, что не запрещено); SSH доступен из любой сети; порт 3306 (MariaDB) открыт всем; нет правил для lo и ответных пакетов, поэтому при смене политики на drop нарушится работа. Исправленный вариант:

```
table inet filter {
  chain input {
    type filter hook input priority 0; policy drop;
    iifname "lo" accept
    ct state established,related accept
    ip saddr 192.168.10.0/24 tcp dport 22 accept
    ip saddr 192.168.20.5 tcp dport 3306 accept
  }
}
```

Экзаменационный билет №15

Вопрос 1

Настройка адресации в Ubuntu: netplan, systemd-networkd и NetworkManager. Структура файла netplan, команды netplan generate, try и apply, типичные ошибки.

Вопрос 2

Протокол TCP: порядковые номера и подтверждения, скользящее окно, управление потоком и перегрузкой, повторная передача.

Практическое задание

Порт 8080 внешнего интерфейса eth0 шлюза необходимо перенаправить на веб-сервер 192.168.5.10 порт 80. Запишите правила nftables (DNAT и разрешение пересылки) и необходимые параметры ядра.

Эталон практического задания (для преподавателя). Пример:

```
table ip nat {
  chain prerouting { type nat hook prerouting priority -100; iifname "eth0"
tcp dport 8080 dnat to 192.168.5.10:80; }
}
table inet filter {
  chain forward { type filter hook forward priority 0; policy drop;
    ct state established,related accept
    iifname "eth0" ip daddr 192.168.5.10 tcp dport 80 accept
  }
}
```

Необходим net.ipv4.ip_forward=1; для ответов внутренний узел должен использовать шлюз как маршрут по умолчанию (иначе потребуется masquerade). Проверка: nft list ruleset, curl http://<внешний адрес>:8080 из внешней сети.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Экзаменационный билет №16

Вопрос 1

Методика диагностики сети по уровням модели: порядок проверок и применяемые утилиты. Типичные неисправности и их признаки.

Вопрос 2

SSH: аутентификация по ключам, файл known_hosts, укрепление конфигурации sshd (запрет входа root и по паролю), защита от подбора паролей (fail2ban).

Практическое задание

Дан фрагмент tcpdump. Опишите происходящее, укажите, какое значение подтверждения отправит сервер в ответ на последний сегмент, и что произойдёт, если сегмент потеряется.

```
10:00:00.000 IP 10.1.1.5.50100 > 10.1.1.9.443: Flags [S], seq 1000, win
64240, length 0
10:00:00.001 IP 10.1.1.9.443 > 10.1.1.5.50100: Flags [S.], seq 5000, ack
1001, win 65160, length 0
10:00:00.001 IP 10.1.1.5.50100 > 10.1.1.9.443: Flags [.], ack 5001, win
64240, length 0
10:00:00.002 IP 10.1.1.5.50100 > 10.1.1.9.443: Flags [P.], seq 1001:1101,
ack 5001, length 100
```

Эталон практического задания (для преподавателя). Установлено TCP-соединение клиента 10.1.1.5 с портом 443 сервера 10.1.1.9: SYN (seq 1000), SYN-ACK (seq 5000, ack 1001), ACK (ack 5001); затем клиент передал 100 байт (порядковые номера 1001–1100). Сервер подтвердит ack 1101 (номер следующего ожидаемого байта). При потере сегмента подтверждение не придёт, клиент по таймеру повторит передачу.

Экзаменационный билет №17

Вопрос 1

Протокол ICMP. Принцип работы ping и traceroute/mtr, роль поля TTL. Интерпретация потерь пакетов на промежуточных узлах.

Вопрос 2

Протокол HTTP: структура запроса и ответа, методы, коды состояния, заголовки. Утилита curl. Принципы HTTP/2.

Практическое задание

Фрагмент sshd_config сервера, доступного из Интернета, приведён ниже. Укажите риски и порядок безопасного перехода на вход по ключам.

```
PermitRootLogin yes
PasswordAuthentication yes
Port 22
```

Эталон практического задания (для преподавателя). Риски: вход root и вход по паролю допускают подбор пароля. Порядок: на рабочем месте ssh-keygen -t ed25519; ssh-copy-id пользователь@сервер; проверить вход по ключу во второй сессии; затем PermitRootLogin no, PasswordAuthentication no, проверка sshd -t, systemctl reload ssh;

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

дополнительно – ограничение по адресам в межсетевом экране и fail2ban. Закрытый ключ не копируется на другие узлы и не передаётся ИИ-сервисам.

Экзаменационный билет №18

Вопрос 1

Утилиты ss и tcpdump: назначение, основные ключи и фильтры. Чтение вывода; что нельзя делать с перехваченным трафиком (152-ФЗ).

Вопрос 2

HTTP: cookies и их атрибуты, кэширование (Cache-Control, ETag, ответ 304). Что передавать в заголовках, а что – нельзя.

Практическое задание

Веб-приложение слушает 127.0.0.1:8000. Настройте nginx для app.example.org так, чтобы HTTP перенаправлялся на HTTPS, а приложение работало за обратным прокси. Исходная конфигурация приведена ниже; укажите команду проверки.

```
server {
    listen 80;
    server_name app.example.org;
    location / {
        proxy_pass http://127.0.0.1:8000;
    }
}
```

Эталон практического задания (для преподавателя). Пример:

```
server {
    listen 80;
    server_name app.example.org;
    return 301 https://$host$request_uri;
}
server {
    listen 443 ssl;
    server_name app.example.org;
    ssl_certificate     /etc/ssl/app/fullchain.pem;
    ssl_certificate_key /etc/ssl/app/privkey.pem;
    location / {
        proxy_pass http://127.0.0.1:8000;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-Proto $scheme;
    }
}
```

Проверка: nginx -t, systemctl reload nginx, curl -I http://app.example.org (ожидается 301), openssl s_client -connect app.example.org:443 -servername app.example.org. Для самоподписанного сертификата браузер выдаст предупреждение; в эксплуатации применяется сертификат удостоверяющего центра.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Экзаменационный билет №19

Вопрос 1

Протокол DHCP: процесс получения адреса (DISCOVER, OFFER, REQUEST, ACK), аренда, порты, широковещательные сообщения. Адреса 169.254.0.0/16.

Вопрос 2

Публикация портов контейнеров и правила nftables/iptables, создаваемые Docker. Риск обхода правил ufw. Привязка публикации к 127.0.0.1.

Практическое задание

Клиентский файл WireGuard приведён ниже. Через туннель должен идти только трафик к сети VPN 10.8.0.0/24 и к сети 192.168.5.0/24. Найдите ошибку и исправьте; укажите, какие данные нельзя публиковать и передавать ИИ-сервису.

```
[Interface]
PrivateKey = <закрытый ключ клиента>
Address = 10.8.0.2/32

[Peer]
PublicKey = <открытый ключ сервера>
Endpoint = vpn.example.org:51820
AllowedIPs = 0.0.0.0/0
```

Эталон практического задания (для преподавателя). AllowedIPs = 0.0.0.0/0 направляет в туннель весь трафик клиента. Исправление:

```
[Interface]
PrivateKey = <закрытый ключ клиента>
Address = 10.8.0.2/32

[Peer]
PublicKey = <открытый ключ сервера>
Endpoint = vpn.example.org:51820
AllowedIPs = 10.8.0.0/24, 192.168.5.0/24
PersistentKeepalive = 25
```

Нельзя публиковать и передавать ИИ-сервисам закрытый ключ (PrivateKey), а также реальный адрес конечной точки и топологию; открытый ключ передаётся только администратору сервера.

Экзаменационный билет №20

Вопрос 1

DHCP-сервер в Linux (dnsmasq, Kea): пул, резервирование по MAC-адресу, параметры шлюза и DNS, DHCP relay. Угрозы: чужой DHCP-сервер, истощение пула.

Вопрос 2

Протокол TLS и HTTPS: назначение, рукопожатие, сертификат X.509, цепочка доверия, SNI. Самоподписанные сертификаты и Let's Encrypt (принцип).

Практическое задание

В docker-compose.yml (фрагмент ниже) база данных опубликована на все интерфейсы хоста, а пароль задан в открытом виде. Исправьте файл: БД доступна только

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

приложению, приложение опубликовано только на локальном интерфейсе (за обратным прокси).

```
services:
  app:
    image: registry.example.org/shop-app:1.4
    ports:
      - "8080:80"
  db:
    image: mariadb:11
    environment:
      MARIADB_ROOT_PASSWORD: root
    ports:
      - "3306:3306"
```

Эталон практического задания (для преподавателя). Пример:

```
services:
  app:
    image: registry.example.org/shop-app:1.4
    ports:
      - "127.0.0.1:8080:80"
    networks: [frontend, backend]
  db:
    image: mariadb:11
    environment:
      MARIADB_ROOT_PASSWORD_FILE: /run/secrets/db_root
    networks: [backend]
networks:
  frontend:
  backend:
    internal: true
```

Порт базы данных не публикуется; сеть backend с параметром internal изолирована от внешних сетей; пароль передаётся через секрет (файл вне репозитория). Проверка: docker compose config; docker compose exec app getent hosts db; попытка подключения к порту 3306 с другого узла должна завершиться отказом.

Экзаменационный билет №21

Вопрос 1

Сети Docker: драйверы bridge, host, none, overlay. Мост docker0, пользовательские сети, встроенный DNS и разрешение имён контейнеров.

Вопрос 2

Правила безопасной работы с ИИ-ассистентами: обезличивание конфигураций и журналов, запрет передачи паролей, ключей и персональных данных (152-ФЗ), указание использования ИИ в отчёте, запрет на экзамене. Приведите пример небезопасной рекомендации ИИ и её разбор.

Практическое задание

Напишите правило оповещения Prometheus, срабатывающее, когда узел не отвечает на ICMP-проверку blackbox_exporter более двух минут, и перечислите, какие метрики показывают доступность и задержку проверки.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Эталон практического задания (для преподавателя). Пример:

```
groups:
  - name: availability
    rules:
      - alert: HostUnreachable
        expr: probe_success{job="blackbox-icmp"} == 0
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "Узел {{ $labels.instance }} недоступен более 2 минут"
```

Доступность: probe_success (1 – успех, 0 – сбой); задержка: probe_duration_seconds; для HTTP-проверок дополнительно probe_http_status_code. Правило проверяется командой promtool check rules.

Экзаменационный билет №22

Вопрос 1

Система DNS: иерархия, рекурсивный и авторитетный серверы, зоны, делегирование, кэш и TTL.

Вопрос 2

Российские ИИ-ассистенты (GigaChat, GigaCode, Алиса AI, YandexGPT): назначение и возможности. Что можно поручить ИИ в сетевом администрировании и как сформулировать запрос.

Практическое задание

ИИ-ассистент в ответ на жалобу «служба недоступна по сети» предложил выполнить: sudo ufw disable, затем sudo iptables -F и chmod -R 777 /etc. Оцените предложение, укажите, как правильно искать причину, и что нужно указать в отчёте об использовании ИИ.

Эталон практического задания (для преподавателя). Предложение небезопасно: отключение межсетевого экрана и очистка правил оставляют узел без защиты и без диагностики причины, права 777 на /etc нарушают безопасность системы. Правильно: проверить, слушает ли служба порт (ss -tlnp), правила (nft list ruleset или ufw status verbose), журналы службы (journalctl -u), доступность с клиента (nc -vz, curl -v); при необходимости добавить конкретное разрешающее правило. В отчёте указываются ассистент, обезличенный запрос, полученный ответ, способ проверки и принятое решение.

Экзаменационный билет №23

Вопрос 1

Обратный прокси nginx: проксирование на приложение, перенаправление с HTTP на HTTPS, заголовки безопасности, проверка конфигурации (nginx -t).

Вопрос 2

Риски применения ИИ-ассистентов при работе с сетями: ошибки в расчётах, несуществующие параметры, устаревшие команды, небезопасные рекомендации, утечка данных.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Практическое задание

Нужно разбить сеть 10.30.0.0/22 на пять подсетей, в каждой до 100 узлов. ИИ-ассистент ответил: «используйте /26, это даст 5 подсетей по 100 узлов». Проверьте ответ расчётом и дайте верное решение.

Эталон практического задания (для преподавателя). Для 100 узлов необходим блок не менее 102 адресов, то есть /25 (126 узлов); /26 даёт только 62 узла, поэтому ответ ИИ неверен. Пять подсетей /25: 10.30.0.0/25, 10.30.0.128/25, 10.30.1.0/25, 10.30.1.128/25, 10.30.2.0/25; они помещаются в /22 (1024 адреса, занято 640). Проверка: сценарий на Python с модулем ipaddress.

Экзаменационный билет №24

Вопрос 1

Адресация IPv6: формат и сокращение записи, типы адресов (global unicast, link-local, ULA, multicast), автоконфигурация SLAAC, двойной стек.

Вопрос 2

Проверка результата ИИ: синтаксический контроль (nft -c, nginx -t, netplan generate, named-checkconf, docker compose config), расчёт сценарием, сверка с документацией, испытание на стенде с откатом.

Практическое задание

Для запроса к ИИ-ассистенту нужно приложить фрагмент журнала (ниже). Подготовьте безопасную версию запроса, перечислите, что необходимо обезличить, и опишите, как проверять ответ.

```
Oct  1 10:15:02 gw sshd[812]: Failed password for invalid user ivanov.petr
from 203.0.113.45 port 52114 ssh2
Oct  1 10:15:09 gw sshd[812]: Failed password for invalid user ivanov.petr
from 203.0.113.45 port 52118 ssh2
Oct  1 10:16:40 gw sshd[815]: Accepted publickey for admin from
192.168.10.7 port 40022 ssh2
```

Эталон практического задания (для преподавателя). Обезличить: имя пользователя (возможны персональные данные), внешний и внутренний адреса, имя узла (заменить на условные: user1, 198.51.100.10, 192.0.2.7, host1); пароли, ключи и токены в запрос не включать. Запрос: «Объясните записи журнала sshd и предложите меры защиты от подбора пароля». Проверка ответа: сверка с документацией sshd_config и fail2ban, испытание на стенде, запрет вывода рекомендаций с отключением защиты; использование ИИ указывается в отчёте. Событие в журнале – признак подбора пароля (ПК 1.7): внести запись в журнал инцидентов.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

5.3 КОМПЛЕКТ «ТЕКУЩИЙ КОНТРОЛЬ»

5.3.1 Задания для срезов знаний

1. Назовите уровни модели TCP/IP и укажите, какие уровни OSI соответствуют прикладному уровню TCP/IP. (Эталон: прикладной, транспортный, сетевой (межсетевой), канальный (доступ к сети); прикладному соответствуют прикладной, представительский и сеансовый.)
2. Определите число узлов в подсети 172.16.8.0/22 и широковещательный адрес. (Эталон: 1022 узлов; 172.16.11.255.)
3. Принадлежит ли адрес 10.12.47.250 сети 10.12.32.0/20? (Эталон: да; сеть охватывает 10.12.32.1 – 10.12.47.254.)
4. Какой командой пакета iproute2 можно узнать, через какой шлюз и интерфейс будет отправлен пакет на заданный адрес? (Эталон: ip route get <адрес>.)
5. Какое сообщение DHCP отправляет сервер в ответ на DHCPDISCOVER и какое – клиент затем? (Эталон: DHCPOFFER; клиент отвечает DHCPREQUEST, сервер завершает обмен DHCPACK.)
6. Какая запись DNS нужна для почтового обмена домена и какая – для обратного преобразования адреса в имя? (Эталон: MX и PTR.)
7. Чем отличается access-порт от trunk-порта и что такое native VLAN? (Эталон: access передаёт кадры одной VLAN без тега; trunk – нескольких VLAN с тегами IEEE 802.1Q; native VLAN передаётся без тега.)
8. Почему политика drop для цепочки input должна сопровождаться правилом для ответных пакетов (ct state established,related)? (Эталон: без него будут блокироваться ответы на исходящие соединения самого узла, включая DNS и обновления.)
9. Назовите два риска использования ИИ-ассистента при настройке сети и меру снижения для каждого. (Эталон: утечка адресов, ключей и данных – обезличивание и запрет передачи секретов; ошибочная или небезопасная конфигурация – синтаксический контроль, расчёт, сверка с документацией и испытание на стенде.)
10. Какой параметр Docker Compose запрещает контейнерам сети доступ во внешние сети и для чего он используется в схеме с базой данных? (Эталон: internal: true; изоляция сети backend, в которой работает база данных.)

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

5.3.2 Тестовые задания

Текущий контроль знаний по темам проводится в системе дистанционного обучения Moodle. Для каждой темы создан банк тестовых вопросов (типы: один правильный ответ, верно/неверно, краткий ответ); на занятии каждому обучающемуся выдаётся тест из случайно выбранных вопросов банка. Попыток – 2, время – 15 минут, оценка – по доле правильных ответов (90–100 % – «5», 75–89 % – «4», 60–74 % – «3»). Использование ИИ-ассистентов при тестировании не допускается.

Ниже приведён демонстрационный банк из 54 заданий с ключами. Вопросы 1–14 относятся к разделу 1, 15–24 – к разделу 2, 25–32 – к разделу 3, 33–40 – к разделу 4, 41–44 – к разделу 5; вопросы 45–48 – по теме «Российские ИИ-ассистенты в диагностике сетей». Варианты ответов приведены отдельными строками.

1. Какое устройство работает на канальном уровне и пересылает кадры на основании MAC-адресов?

а) концентратор

б) маршрутизатор

в) коммутатор

г) повторитель

Правильный ответ: в

2. Как называется блок данных протокола TCP?

а) сегмент

б) пакет

в) кадр

г) датаграмма

Правильный ответ: а

3. Какой уровень модели OSI отвечает за маршрутизацию пакетов между сетями?

а) канальный

б) сеансовый

в) транспортный

г) сетевой

Правильный ответ: г

4. Какой метод доступа к среде используют сети Wi-Fi?

а) CSMA/CD

б) CSMA/CA

в) маркерный доступ

г) опрос портов

Правильный ответ: б

5. Какой протокол определяет MAC-адрес узла по его IP-адресу в локальной сети?

а) DNS

б) ICMP

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

в) DHCP

г) ARP

Правильный ответ: г

6. Сколько узлов можно адресовать в подсети с маской 255.255.255.224?

а) 30

б) 32

в) 62

г) 14

Правильный ответ: а

7. Каков адрес сети для узла 172.16.77.130/26?

а) 172.16.77.0

б) 172.16.77.128

в) 172.16.77.192

г) 172.16.77.130

Правильный ответ: б

8. Каков широковещательный адрес для узла 10.20.30.77/27?

а) 10.20.30.63

б) 10.20.30.95

в) 10.20.30.127

г) 10.20.30.79

Правильный ответ: б

9. Какой из адресов относится к частным (RFC 1918)?

а) 172.32.0.1

б) 172.20.5.4

в) 192.169.1.1

г) 11.0.0.1

Правильный ответ: б

10. Что означает получение клиентом адреса из диапазона 169.254.0.0/16?

а) клиент не получил адрес по DHCP и назначил себе адрес автоматически

б) адрес выдан DHCP-сервером

в) адрес выдан провайдером

г) узел находится в сети VPN

Правильный ответ: а

11. Сеть 10.0.0.0/24 разделили на подсети с маской /26. Сколько подсетей получилось?

а) 2

б) 4

в) 8

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

г) 16

Правильный ответ: б

12. Каким будет суммарный маршрут для сетей 192.168.16.0/24 – 192.168.23.0/24?

а) 192.168.16.0/22

б) 192.168.16.0/21

в) 192.168.16.0/20

г) 192.168.20.0/21

Правильный ответ: б

13. Адреса IPv6, начинающиеся с fe80::, являются:

а) адресами link-local

б) глобальными

в) адресами multicast

г) адресами ULA

Правильный ответ: а

14. Какая сеть выделяется по методу VLSM первой?

а) самая маленькая

б) сеть для канала «точка-точка»

в) случайная

г) самая большая по числу узлов

Правильный ответ: г

15. Какая команда iproute2 показывает адреса интерфейсов в кратком виде?

а) ip route

б) ip -br addr

в) ip neigh

г) ip rule

Правильный ответ: б

16. Какой файл используется для настройки сети в Debian с пакетом ifupdown?

а) /etc/netplan/01-net.yaml

б) /etc/resolv.conf

в) /etc/network/interfaces

г) /etc/hosts

Правильный ответ: в

17. Какая команда netplan применяет настройки с автоматическим откатом при отсутствии подтверждения?

а) netplan try

б) netplan generate

в) netplan apply

г) netplan get

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Правильный ответ: а

18. Какой протокол использует утилита ping?

а) TCP

б) UDP

в) ARP

г) ICMP

Правильный ответ: г

19. Какое поле IP-пакета уменьшается на каждом маршрутизаторе и используется утилитой traceroute?

а) Flags

б) TTL

в) Identification

г) Checksum

Правильный ответ: б

20. Каков порядок сообщений DHCP при получении адреса?

а) DISCOVER, OFFER, REQUEST, ACK

б) REQUEST, DISCOVER, ACK, OFFER

в) OFFER, DISCOVER, ACK, REQUEST

г) DISCOVER, REQUEST, OFFER, ACK

Правильный ответ: а

21. Какие UDP-порты использует DHCP?

а) 53 и 67

б) 67 и 68

в) 80 и 443

г) 20 и 21

Правильный ответ: б

22. Какая запись DNS содержит адрес IPv6?

а) A

б) PTR

в) MX

г) AAAA

Правильный ответ: г

23. Какая команда проверяет файл зоны BIND9?

а) dig

б) named-checkzone

в) nslookup

г) rndc reload

Правильный ответ: б

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

24. Что произойдёт, если в записи DNS указать CNAME на IP-адрес?

а) запись некорректна: CNAME указывает на доменное имя

б) запись будет работать как A

в) сервер выдаст адрес IPv6

г) запись будет использована как PTR

Правильный ответ: а

25. Какой стандарт определяет тегирование кадров VLAN?

а) IEEE 802.1X

б) IEEE 802.11

в) IEEE 802.3

г) IEEE 802.1Q

Правильный ответ: г

26. Как называется порт коммутатора, передающий кадры нескольких VLAN с тегами?

а) access

б) mirror

в) trunk

г) console

Правильный ответ: в

27. Какой маршрут будет выбран для адреса 10.9.70.15 при наличии маршрутов 0.0.0.0/0, 10.9.0.0/16, 10.9.64.0/18 и 10.9.70.0/24?

а) 0.0.0.0/0

б) 10.9.0.0/16

в) 10.9.64.0/18

г) 10.9.70.0/24

Правильный ответ: г

28. Какой параметр ядра включает пересылку IPv4-пакетов между интерфейсами?

а) net.ipv4.ip_forward

б) net.ipv4.tcp_syncookies

в) kernel.randomize_va_space

г) vm.swappiness

Правильный ответ: а

29. Какой протокол динамической маршрутизации относится к протоколам состояния каналов?

а) RIP

б) ARP

в) OSPF

г) DHCP

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Правильный ответ: в

30. Какая трансляция заменяет адрес источника пакетов внутренних узлов на внешний адрес шлюза?

а) DNAT

б) обратный прокси

в) проброс порта

г) SNAT (masquerade)

Правильный ответ: г

31. Какая политика по умолчанию рекомендуется для входящего трафика межсетевого экрана?

а) drop

б) accept

в) accept только для ICMP

г) forward

Правильный ответ: а

32. Какой командой проверяется синтаксис файла правил nftables без применения?

а) nft flush ruleset

б) nft -c -f файл

в) nft list ruleset

г) systemctl restart nftables

Правильный ответ: б

33. Какой порт по умолчанию использует протокол HTTPS?

а) 80

б) 22

в) 443

г) 8080

Правильный ответ: в

34. Сколько шагов содержит установление TCP-соединения?

а) 2

б) 3

в) 4

г) 5

Правильный ответ: б

35. Какой из протоколов транспортного уровня не гарантирует доставку и порядок сегментов?

а) TCP

б) UDP

в) SSH

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

г) TLS

Правильный ответ: б

36. Какое действие повышает безопасность SSH-сервера, доступного из Интернета?

а) отключить вход по паролю после настройки ключей

б) разрешить вход root по паролю

в) перенести закрытый ключ на сервер

г) отключить межсетевой экран

Правильный ответ: а

37. Что означает ответ HTTP 301?

а) ресурс создан

б) ресурс не найден

в) постоянное перенаправление

г) ошибка сервера

Правильный ответ: в

38. Для чего служит расширение SNI протокола TLS?

а) шифрование журналов

б) аутентификация пользователя по паролю

в) сжатие данных

г) указание имени узла для выбора сертификата на одном IP-адресе

Правильный ответ: г

39. Какая директива nginx передаёт запрос приложению на другом адресе?

а) proxy_pass

б) root

в) listen

г) server_name

Правильный ответ: а

40. Что задаёт параметр AllowedIPs в конфигурации WireGuard?

а) порт прослушивания

б) список разрешённых адресов узла и маршрутов, направляемых в туннель

в) пароль пользователя

г) срок действия сертификата

Правильный ответ: б

41. Какой драйвер сети Docker используется по умолчанию для контейнеров на одном узле?

а) host

б) none

в) bridge

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

г) overlay

Правильный ответ: в

42. Что делает параметр internal: true для сети в Docker Compose?

а) запрещает выход контейнеров сети во внешние сети

б) открывает сеть в Интернет

в) включает шифрование

г) отключает DNS

Правильный ответ: а

43. Как лучше опубликовать порт приложения, которое работает за обратным прокси на том же узле?

а) "8080:80"

б) не имеет значения

в) "0.0.0.0:80:8080"

г) "127.0.0.1:8080:80"

Правильный ответ: г

44. Какая метрика blackbox_exporter показывает успех проверки (1) или сбой (0)?

а) up

б) probe_success

в) node_load1

г) process_cpu_seconds_total

Правильный ответ: б

45. Что нельзя передавать ИИ-ассистенту при разборе сетевой конфигурации?

а) обезличенные фрагменты вывода команд

б) фрагмент документации

в) вопрос о назначении параметра

г) пароли, закрытые ключи, реальные адреса и персональные данные

Правильный ответ: г

46. Что необходимо сделать с правилами nftables, предложенными ИИ-ассистентом, прежде чем применить их на рабочем сервере?

а) проверить nft -c, сверить с документацией и испытать на стенде

б) применить сразу

в) отправить в открытый репозиторий

г) отключить межсетевой экран

Правильный ответ: а

47. ИИ-ассистент утверждает, что в подсети /27 доступно 32 узла. Как правильно?

а) 32 узла

б) 30 узлов (2^5 − 2)

в) 62 узла

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

г) 14 узлов

Правильный ответ: б

48. Какая практика допустима при подготовке запроса к ИИ-ассистенту о сетевой проблеме?

а) передать журнал с реальными адресами клиентов

б) заменить реальные адреса и имена условными

в) указать пароль для проверки

г) приложить закрытый ключ WireGuard

Правильный ответ: б

49. Верно ли, что трансляция адресов (NAT) обеспечивает шифрование передаваемых данных?

Правильный ответ: неверно

50. Верно ли, что 192.168.1.255 в сети 192.168.1.0/24 является широковещательным адресом?

Правильный ответ: верно

51. Верно ли, что конфигурацию, полученную от ИИ-ассистента, можно применять на рабочем сервере без проверки?

Правильный ответ: неверно

52. Какая команда пакета iproute2 выводит таблицу маршрутизации?

Правильный ответ: ip route

53. Какая команда проверяет синтаксис конфигурации nginx?

Правильный ответ: nginx -t

54. Какой номер порта используется службой SSH по умолчанию?

Правильный ответ: 22

5.3.3 Задания для проверочных, самостоятельных и контрольных работ

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Контрольная работа №1. Модели OSI и TCP/IP, адресация IPv4 и IPv6, подсети и VLSM, DHCP, DNS и диагностика

Контрольная работа проверяет умения по разделам 1 и 2 (модели OSI и TCP/IP, оборудование, адресация IPv4 и IPv6, подсети и VLSM, DHCP, DNS и диагностика).

Вариант 1

1. Для каждого объекта укажите уровень модели OSI и название блока данных или устройства: Ethernet-кадр; IP-пакет; TCP-сегмент; коммутатор; маршрутизатор; протокол ARP.
2. Для узла 192.168.133.77/25 определите маску, адрес сети, широковещательный адрес, диапазон узлов и число узлов.
3. Выполните распределение сети 10.70.0.0/23 по методу VLSM: «Студенты» – 250 узлов, «Преподаватели» – 100, «Wi-Fi» – 60, «Серверы» – 30, канал «точка-точка» – 2. Укажите подсеть, маску, диапазон узлов, широковещательный адрес.
4. Определите, находятся ли узлы 10.0.5.200/25 и 10.0.5.20/25 в одной подсети. Что произойдёт при попытке обмена и как это исправить?
5. Запишите адрес IPv6 2001:0db8:0000:0000:0000:ff00:0042:8329 в сокращённой форме. К какому типу относится адрес fe80::/10?
6. Клиент получил адрес 169.254.37.12 вместо адреса из пула 192.168.1.100 – 192.168.1.200. Назовите возможные причины, порядок проверок на клиенте и на сервере DHCP и команды диагностики.

Вариант 2

1. Для каждого объекта укажите уровень модели OSI: концентратор; коммутатор; маршрутизатор; протокол IP; протокол DNS; протокол ICMP. Сколько широковещательных доменов образует маршрутизатор с тремя подключёнными сетями?
2. Для узла 10.130.140.5/19 определите маску, адрес сети, широковещательный адрес, диапазон узлов и число узлов.
3. Выполните распределение сети 172.20.0.0/23 по методу VLSM: «Сотрудники» – 200 узлов, «Серверы» – 60, «Гости» – 28, «Управление» – 12, два канала «точка-точка» по 2 узла.
4. Найдите суммарный маршрут для сетей 10.60.4.0/24, 10.60.5.0/24, 10.60.6.0/24, 10.60.7.0/24 и обоснуйте. Можно ли так же объединить 10.60.2.0/24 – 10.60.5.0/24?
5. Запишите адрес IPv6 2001:0db8:0000:0000:0001:0000:0000:0001 в сокращённой форме. Как называется механизм автоматической настройки адреса IPv6 без DHCP?
6. На рабочей станции ping 77.88.8.8 успешен, а ping ya.ru выдаёт «Temporary failure in name resolution». Определите уровень неисправности и последовательность проверок (файлы, команды dig и resolvectl).

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Ключи

Вариант 1: 1) Ethernet-кадр – канальный уровень (кадр); IP-пакет – сетевой (пакет); TCP-сегмент – транспортный (сегмент); коммутатор – канальный уровень; маршрутизатор – сетевой уровень; ARP – между канальным и сетевым (по модели TCP/IP – канальный уровень); 2) маска 255.255.255.128; сеть 192.168.133.0/25; broadcast 192.168.133.127; узлы 192.168.133.1 – 192.168.133.126; число узлов 126; 3) Студенты – 10.70.0.0/24, узлы 10.70.0.1 – 10.70.0.254, broadcast 10.70.0.255; Преподаватели – 10.70.1.0/25, узлы 10.70.1.1 – 10.70.1.126, broadcast 10.70.1.127; Wi-Fi – 10.70.1.128/26, узлы 10.70.1.129 – 10.70.1.190, broadcast 10.70.1.191; Серверы – 10.70.1.192/27, узлы 10.70.1.193 – 10.70.1.222, broadcast 10.70.1.223; Канал – 10.70.1.224/30, узлы 10.70.1.225 – 10.70.1.226, broadcast 10.70.1.227; 4) узлы принадлежат разным подсетям (10.0.5.128/25 и 10.0.5.0/25): прямой обмен невозможен, пакеты уходят на шлюз; исправление – изменить адрес узла или маску так, чтобы они оказались в одной подсети, либо настроить маршрутизацию между подсетями; 5) 2001:db8::ff00:42:8329; fe80::/10 – адреса link-local (действуют в пределах канала); 6) адрес 169.254.0.0/16 назначен автоматически (APIPA/link-local) из-за отсутствия ответа DHCP: проверить кабель и состояние интерфейса (ip link), наличие широковещательной связи с сервером (tcpdump port 67 or 68), работу службы DHCP (systemctl status, journalctl), пул адресов (не исчерпан ли) и VLAN порта.

Вариант 2: 1) концентратор – физический; коммутатор – канальный; маршрутизатор – сетевой; IP – сетевой; DNS – прикладной; ICMP – сетевой (по модели TCP/IP – межсетевой); маршрутизатор с тремя сетями образует три широковещательных домена; 2) маска 255.255.224.0; сеть 10.130.128.0/19; broadcast 10.130.159.255; узлы 10.130.128.1 – 10.130.159.254; число узлов 8190; 3) Сотрудники – 172.20.0.0/24, узлы 172.20.0.1 – 172.20.0.254, broadcast 172.20.0.255; Серверы – 172.20.1.0/26, узлы 172.20.1.1 – 172.20.1.62, broadcast 172.20.1.63; Гости – 172.20.1.64/27, узлы 172.20.1.65 – 172.20.1.94, broadcast 172.20.1.95; Управление – 172.20.1.96/28, узлы 172.20.1.97 – 172.20.1.110, broadcast 172.20.1.111; Канал 1 – 172.20.1.112/30, узлы 172.20.1.113 – 172.20.1.114, broadcast 172.20.1.115; Канал 2 – 172.20.1.116/30, узлы 172.20.1.117 – 172.20.1.118, broadcast 172.20.1.119; 4) 10.60.4.0/22: третий октет 4–7 совпадает по 6 битам; сети 10.60.2.0/24 – 10.60.5.0/24 одной записью объединить нельзя (получатся 10.60.2.0/23 и 10.60.4.0/23); 5) 2001:db8::1:0:0:1; SLAAC (автоконфигурация без состояния); 6) до внешнего адреса сеть работает, неисправно разрешение имён (прикладной уровень): проверить /etc/resolv.conf и resolvectl status, dig ya.ru и dig @77.88.8.8 ya.ru, доступность DNS-сервера и порта 53 в межсетевом экране; исправить параметры DNS в netplan или DHCP.

Критерии оценивания

Каждое задание оценивается в 5 баллов: 5 – верное решение с обоснованием; 3–4 – верная идея, вычислительная ошибка или неполное обоснование; 1–2 – частичное решение; 0 – решение отсутствует или неверно. Максимум – 30 баллов.

Оценка	Баллы
«5»	27–30
«4»	22–26
«3»	17–21
«2»	менее 17

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Время выполнения – 45 минут. Разрешены непрограммируемый калькулятор и памятка; ИИ-ассистенты и сеть Интернет не используются.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Контрольная работа №2. VLAN, маршрутизация, NAT и межсетевой экран, TCP, SSH, обратный прокси, VPN и сети Docker

Контрольная работа проверяет умения по разделам 3–5 (VLAN, маршрутизация, NAT и межсетевой экран, TCP, SSH, обратный прокси, VPN, сети Docker).

Вариант 1

1. Запишите команды Linux (VLAN-aware bridge br0): порт eth1 – access в VLAN 10, порт eth2 – access в VLAN 20, порт eth3 – trunk для VLAN 10 и 20.
2. Таблица маршрутов: 0.0.0.0/0 – шлюз 10.9.0.1; 10.9.0.0/16 – шлюз 10.9.0.2; 10.9.64.0/18 – шлюз 10.9.0.3; 10.9.70.0/24 – шлюз 10.9.0.4. Определите маршрут для адресов 10.9.70.15, 10.9.80.2, 10.9.9.9, 203.0.113.8.
3. Напишите правила nftables: пересылка из интерфейса eth1 в eth0 разрешена, остальная пересылка запрещена, для исходящего через eth0 трафика выполняется masquerade.
4. В sshd_config заданы PermitRootLogin yes и PasswordAuthentication yes. Опишите безопасный порядок перехода на вход по ключам и запишите итоговые параметры.
5. Фрагмент tcpdump: Flags [S], seq 2000; Flags [S.], seq 7000, ack 2001; Flags [.], ack 7001; затем клиент передал 50 байт. Опишите событие и укажите значение подтверждения сервера после передачи 50 байт.
6. В docker-compose.yml служба db опубликована как «3306:3306». Исправьте так, чтобы база данных была доступна только службе app, и объясните роль параметра internal.

Вариант 2

1. Запишите команды Linux (VLAN-aware bridge br0): порты eth1, eth2 – access в VLAN 30, порт eth3 – access в VLAN 40, порт eth4 – trunk для VLAN 30 и 40.
2. Таблица маршрутов: 0.0.0.0/0 – шлюз 172.31.0.1; 172.31.0.0/16 – шлюз 172.31.0.2; 172.31.16.0/20 – шлюз 172.31.0.3; 172.31.16.128/25 – шлюз 172.31.0.4. Определите маршрут для адресов 172.31.16.200, 172.31.20.1, 172.31.99.1, 198.51.100.5.
3. Напишите правило nftables для проброса порта 8443 внешнего интерфейса eth0 на узел 192.168.5.10 порт 443 и укажите необходимый параметр ядра.
4. Настройте перенаправление HTTP на HTTPS в nginx для portal.example.org и укажите команду проверки конфигурации.
5. Фрагмент tcpdump: Flags [S], seq 300; Flags [S.], seq 900, ack 301; Flags [.], ack 901; затем клиент передал 80 байт. Что произойдёт, если клиент не получит SYN-ACK? Укажите подтверждение сервера после передачи 80 байт.
6. Клиентский файл WireGuard содержит AllowedIPs = 0.0.0.0/0, а требуется направлять в туннель только сеть 192.168.5.0/24 и адреса VPN 10.8.0.0/24. Исправьте и укажите, какие данные нельзя передавать ИИ-сервису.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Ключи

Вариант 1: 1) ip link set br0 type bridge vlan_filtering 1; bridge vlan add dev eth1 vid 10 pvid untagged; bridge vlan add dev eth2 vid 20 pvid untagged; bridge vlan add dev eth3 vid 10; bridge vlan add dev eth3 vid 20; 2) 10.9.70.15 – 10.9.70.0/24 (шлюз 10.9.0.4); 10.9.80.2 – 10.9.64.0/18 (шлюз 10.9.0.3); 10.9.9.9 – 10.9.0.0/16 (шлюз 10.9.0.2); 203.0.113.8 – 0.0.0.0/0 (шлюз 10.9.0.1); 3) пример:

```
table inet filter {
  chain forward { type filter hook forward priority 0; policy drop;
    ct state established,related accept
    iifname "eth1" oifname "eth0" accept
  }
}
table ip nat {
  chain postrouting { type nat hook postrouting priority 100; oifname
"eth0" masquerade; }
}
```

4. сначала создать пару ключей (ssh-keygen -t ed25519) и скопировать открытый ключ (ssh-copy-id), проверить вход по ключу во второй сессии, затем PermitRootLogin no и PasswordAuthentication no, проверить sshd -t и перечитать конфигурацию (systemctl reload ssh); 5) трёхстороннее рукопожатие TCP: SYN (seq 2000), SYN-ACK (seq 7000, ack 2001), ACK 7001; подтверждение равно номеру следующего ожидаемого байта (SYN занимает один номер); после 50 байт сервер подтвердит ack 2051; 6) убрать раздел ports у db, подключить db только к сети backend с параметром internal: true (сеть без выхода во внешние сети), а приложение подключить к сетям frontend и backend; проверка docker compose config и попытка подключения к 3306 с другого узла.

Вариант 2: 1) ip link set br0 type bridge vlan_filtering 1; bridge vlan add dev eth1 vid 30 pvid untagged; bridge vlan add dev eth2 vid 30 pvid untagged; bridge vlan add dev eth3 vid 40 pvid untagged; bridge vlan add dev eth4 vid 30; bridge vlan add dev eth4 vid 40; 2) 172.31.16.200 – 172.31.16.128/25 (шлюз 172.31.0.4); 172.31.20.1 – 172.31.16.0/20 (шлюз 172.31.0.3); 172.31.99.1 – 172.31.0.0/16 (шлюз 172.31.0.2); 198.51.100.5 – 0.0.0.0/0 (шлюз 172.31.0.1); 3) пример:

```
table ip nat {
  chain prerouting { type nat hook prerouting priority -100; iifname "eth0"
tcp dport 8443 dnat to 192.168.5.10:443; }
}
```

необходим net.ipv4.ip_forward=1 и правило разрешения пересылки в цепочке forward; 4) пример:

```
server {
    listen 80;
    server_name portal.example.org;
    return 301 https://$host$request_uri;
}
```


ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

проверка: nginx -t, затем systemctl reload nginx; 5) клиент выдержит таймаут и повторно отправит SYN (с увеличивающимися интервалами), затем сообщит об ошибке соединения; причины – потеря пакетов, фильтрация межсетевым экраном, недоступность узла; после 80 байт подтверждение сервера ack 381; 6) AllowedIPs = 10.8.0.0/24, 192.168.5.0/24; нельзя передавать закрытый ключ, реальный адрес конечной точки и топологию сети.

Критерии оценивания

Каждое задание оценивается в 5 баллов: 5 – верное решение с обоснованием; 3–4 – верная идея, вычислительная ошибка или неполное обоснование; 1–2 – частичное решение; 0 – решение отсутствует или неверно. Максимум – 30 баллов.

Оценка	Баллы
«5»	27–30
«4»	22–26
«3»	17–21
«2»	менее 17

Время выполнения – 45 минут. Разрешены непрограммируемый калькулятор и памятка; ИИ-ассистенты и сеть Интернет не используются.

5.3.4 Лабораторные и практические работы

Практические работы выполняются в лаборатории компьютерных сетей на виртуальных машинах с Debian/Ubuntu в изолированной учебной сети. Сканирование, перехват трафика и изменение правил межсетевого экрана допускаются только на узлах учебного стенда. Методические указания к работам размещены в курсе Moodle. По итогам каждой работы обучающийся оформляет отчёт (схема, команды и их вывод, расчёты, выводы); использование ИИ-ассистента отражается в отчёте (запрос в обезличенном виде, ответ, способ проверки).

Перечень практических работ (32 часа, 16 работ по 2 часа)

№	Лабораторная работа	Цель работы	Источник
1	Документирование сети стенда: логическая схема в draw.io, инвентаризация интерфейсов, анализ кадров Ethernet и ARP в tcpdump	Составить логическую схему сети стенда в draw.io, выполнить инвентаризацию интерфейсов и адресов (ip -br addr, ip route, ip neigh), перехватить и разобрать кадры Ethernet и ARP-обмен в tcpdump, сопоставить поля кадра и уровни модели OSI.	новая работа (тема 1.1)
2	Расчёт адресов и масок: сценарий Bash для определения сети и широковещательного адреса, проверка утилитой ipcalc и модулем ipaddress	Определять адрес сети, широковещательный адрес и диапазон узлов по адресу и маске; написать сценарий Bash с использованием побитовых операций, сравнить результат с ipcalc и модулем ipaddress языка Python; обосновать расхождения, если они возникли.	новая работа (тема 1.2)
3	План адресации филиалов по методу VLSM, частные адреса и адреса IPv6 ULA	Построить план адресации головного офиса и трёх филиалов по методу VLSM, выделить сети для каналов «точка-точка», использовать частные адреса RFC 1918, выбрать префикс ULA для IPv6; оформить таблицу адресации и проверить отсутствие пересечений сценарием.	новая работа (тема 1.2)
4	Настройка адресации в Debian (ifupdown) и Ubuntu (netplan):	Назначить статический адрес, шлюз и DNS-серверы в Debian (/etc/network/interfaces) и Ubuntu	новая работа

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

№	Лабораторная работа	Цель работы	Источник
	статический адрес, шлюз, DNS, имя узла	(netplan), проверить применение (ip addr, ip route, resolvectl status), сохранить имя узла, объяснить последствия ошибок в маске и шлюзе.	(тема 2.1)
5	Диагностика сети по уровням: ip, ping, mtr, ss, tcpdump, журнал systemd	Применить методику диагностики по уровням: состояние интерфейса, ARP, шлюз, внешний адрес, DNS, порт службы; использовать ping, mtr, ss, tcpdump и journalctl; оформить протокол диагностики для заранее подготовленной неисправности стенда.	новая работа (тема 2.1)
6	DHCP-сервер: пул, резервирование, параметры шлюза и DNS; анализ процесса DORA	Развернуть DHCP-сервер (dnsmasq или Kea) с пулом адресов, резервированием по MAC-адресу и параметрами шлюза и DNS; проверить получение адреса клиентом, разобрать обмен DISCOVER, OFFER, REQUEST, ACK в перехвате, изучить файл аренд.	новая работа (тема 2.2)
7	DNS: зона в BIND9, кэширующий резолвер unbound, запросы dig	Создать прямую и обратную зоны в BIND9, проверить синтаксис (named-checkconf, named-checkzone), настроить кэширующий резолвер unbound, выполнить запросы dig для записей A, AAAA, CNAME, MX, PTR и объяснить поля ответа.	новая работа (тема 2.3)
8	VLAN и trunk: сегментация учебной сети средствами VLAN-aware bridge Linux	Создать VLAN-aware bridge, назначить access-порты и trunk, проверить изоляцию VLAN и прохождение тегированных кадров; объяснить роль стандарта IEEE 802.1Q и риск использования VLAN по умолчанию.	новая работа (тема 3.1)
9	Маршрутизатор на Linux: ip_forward, статические маршруты, шлюз по умолчанию, устранение ошибок маршрутизации	Превратить Linux-узел в маршрутизатор между двумя подсетями (net.ipv4.ip_forward, ip route), настроить шлюз по умолчанию на клиентах, проверить маршрут утилитами ip route get и mtr, найти и исправить заранее внесённую ошибку маршрутизации.	новая работа (тема 3.2)
10	Динамическая маршрутизация OSPF средствами FRRouting между тремя узлами	Настроить протокол OSPF в FRRouting на трёх виртуальных маршрутизаторах, проверить таблицу соседей и маршрутов (show ip ospf neighbor, show ip route), смоделировать отказ канала и наблюдать перестроение маршрутов.	новая работа (тема 3.2)
11	NAT и межсетевой экран nftables: masquerade, проброс порта, политика drop, журналирование и сохранение правил	Настроить трансляцию адресов (masquerade), проброс порта (DNAT) и фильтрацию nftables с политикой drop для цепочки forward; проверить правила (nft -c -f), журналирование и сохранение правил после перезагрузки; сопоставить с ufw.	новая работа (тема 3.3)
12	Транспортный и прикладной уровни: TCP-сеанс в tcpdump, вход по SSH-ключам, обратный прокси nginx с TLS	Перехватить установление и завершение TCP-соединения, определить флаги и номера; настроить вход по SSH-ключам с отключением входа по паролю; настроить nginx как обратный прокси с самоподписанным сертификатом и перенаправлением с HTTP на HTTPS; проверить конфигурацию (nginx -t) и цепочку (openssl s_client).	новая работа (тема 4.1)
13	VPN WireGuard и SSH-туннели между узлами учебного стенда	Создать VPN-соединение WireGuard между двумя узлами (пары ключей, AllowedIPs, Endpoint), проверить маршрутизацию через туннель, создать SSH-туннель к закрытой службе; объяснить роль ключей и ограничение допустимых адресов; обосновать хранение закрытых ключей.	новая работа (тема 4.2)

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

№	Лабораторная работа	Цель работы	Источник
14	Сети Docker и Docker Compose: пользовательские и внутренние сети, публикация портов, взаимодействие с nftables	Исследовать сети Docker: bridge по умолчанию, пользовательские сети и встроенный DNS, публикацию портов; описать в docker-compose.yml сети frontend и backend (internal), убедиться в недоступности базы данных извне; изучить правила, создаваемые Docker в nftables.	новая работа (тема 5.1)
15	Мониторинг сети: Prometheus, blackbox_exporter и Grafana в Docker Compose; оповещение о недоступности; резервная копия конфигураций в Git	Развернуть в Docker Compose стек Prometheus, blackbox_exporter и Grafana, настроить проверки ICMP и HTTP для узлов стенда и правило оповещения о недоступности; сохранить конфигурации узлов в репозитории Git (в том числе в GitVerse) без секретов.	новая работа (тема 5.2)
16	Российские ИИ-ассистенты (GigaChat, Алиса AI) в диагностике сетей: разбор конфигураций и вывода утилит с проверкой результата	Составлять корректные запросы к GigaChat и Алиса AI для объяснения вывода сетевых утилит и проверки конфигураций (netplan, nftables, nginx, WireGuard, Compose) после обезличивания; проверять ответ синтаксическим контролем, расчётом и сверкой с документацией; фиксировать использование ИИ в отчёте.	новая работа (тема 6.1)

Критерии оценки практической работы

Оценка	Показатели
«5»	Все шаги выполнены самостоятельно и верно; результат проверен командами диагностики; расчёты подтверждены сценарием; отчёт оформлен полностью, пароли, ключи и адреса реальных сетей в нём отсутствуют; обучающийся объясняет назначение каждой настройки и риск при её отсутствии; при использовании ИИ-ассистента представлены обезличенные запросы и результаты проверки ответа.
«4»	Работа выполнена полностью, есть неточности в отчёте или пояснениях; замечания устраняются после наводящих вопросов.
«3»	Выполнено не менее 70 % шагов; проверка результата неполная; пояснения недостаточные.
«2»	Выполнено менее 70 % шагов либо нарушены правила безопасной работы (выход за пределы стенда, потеря доступа к узлу из-за непроверенных правил, передача данных реальных сетей ИИ-сервису); обучающийся не может объяснить результаты.

5.3.5 Компьютерные программы для контроля знаний студентов

Банки тестовых заданий размещены в системе дистанционного обучения колледжа (Moodle) и импортируются в формате Moodle XML. Контрольные работы выполняются письменно, экзамен проводится устно; практическое задание выполняется письменно по предложенному расчёту, фрагменту конфигурации, журналу или выводу утилит. Использование ИИ-ассистентов, сети Интернет и посторонних материалов на контрольных работах и экзамене не допускается.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
1 подпись
Сведения о подписях — на листе подписей. Проверка подлинности — по QR-коду.
ГАПОУ СО «Нижнетагильский торгово-экономический колледж»

Лист подписей

ГАПОУ СО «Нижнетагильский торгово-экономический колледж»
SHA-256 исходного документа: 4f766d6e539383fedf76a3e73c28b3066f5720f35ad39982c042f50a928bfa27
Документ: 46 страниц
Проверка подписей: https://sig.nttek.ru/v/NoLjvP4gb24r4S7Qez0mYH1VsGrPiMy5OwEmcbsTud4cBgfi
Печатная форма сформирована: 15.10.2026 09:45

№	Роль в подписи	Подписант	Сертификат	Дата и время подписания	Результат проверки
1	Утверждаю	Дмитриева Марина Георгиевна Заместитель директора по учебной работе	№ 7E9C18960643A37EF2C929CD1E513CCD, действителен с 08.10.2026 по 08.10.2027	15.10.2026 09:43:03	**подпись действительна** роль и должность подтверждены подписью

Печатная форма не подписывается и служит для удобства чтения. Юридическую силу имеют исходный PDF-документ и файлы электронных подписей (.sig). Подпись — усиленная неквалифицированная электронная подпись (ч. 3 ст. 5 Федерального закона № 63-ФЗ), выданная удостоверяющим центром колледжа.
Время указано по часовому поясу колледжа (Asia/Yekaterinburg, UTC+5).