МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ ИМЕНИ К.Г. РАЗУМОВСКОГО (ПЕРВЫЙ КАЗАЧИЙ УНИВЕРСИТЕТ)»
Смоленский казачий институт промышленных технологий и бизнеса (филиал)

УТВЕРЖДАЮ
Председатель ПЦК
_____Максаков С. А.
«10» апреля 2026 г.

Рабочая программа дисциплины
МДК.01.03 Сети и системы передачи информации

Закреплена за **ПЦК общепрофессиональных дисциплин; профессиональных модулей специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем**

Специальность: **10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Направленность

на базе основного общего образования

Квалификация **техник по защите информации**

Форма обучения **очная**

Общая трудоемкость **136 часов**

Часов по учебному плану 136

в том числе:

контактная работа 128

самостоятельная работа 8

Виды контроля в семестрах:

Контрольная работа - 4,5

Распределение часов дисциплины по семестрам

Вид учебной работы	Трудоемкость, часов					
	семестр 4		**семестр 5**		Итого	
	УП	РП	УП	РП	УП	РП
Лекции	44	44	14	14	58	58
Лабораторные	20	20	14	14	34	34
Практические	22	22	14	14	36	36
В т.ч. в форме практ. подгот.	0	0	0	0	0	0
Контактная работа	86	86	42	42	128	128
Сам. работа	4	4	4	4	8	8
Часы на контроль						

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00F5 665F CCDB 5046 05DD 6E08 EBCB D00A DC
Действителен: с 21 октября 2025 г. по 14 января 2027 г.
Владелец: Коржикова Надежда Сергеевна
Должность: Директор

Москва, 2026

Программу составил:
Преподаватель Долотовский Алексей Игоревич _____

Рабочая программа дисциплины
Сети и системы передачи информации

Разработана в соответствии с:
Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ (приказ Минобрнауки России от 09.12.2016 г. № 1553)
06.033. Профессиональный стандарт "СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ", утверждённый приказом Министерства труда и социальной защиты Российско Федерации от 14 сентября 2022 г. N 525н (зарегистрирован Министерством юстиции Российской Федерации 14 октября 2022 г., регистрационный N 70543)

Разработана на основании учебного плана, утвержденного Учёным советом ФГБОУ ВО "МГУТУ им. К.Г. Разумовского (ПКУ)" от 26.03.2026 протокол №9.

СОДЕРЖАНИЕ

1. МЕСТО ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2. ЦЕЛИ, ЗАДАЧИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (УЧЕБНОГО ПРЕДМЕТА)

8. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	П

Дисциплина Сети и системы передачи информации является частью неопознанный объект и обязательна для изучения.

Требования к предварительной подготовке обучающегося:	
1	Технические средства информатизации
Дисциплины (модули) и практики, для которых освоение данной дисциплины необходимо как предшествующее:	
1	Экономика и управление
2	Эксплуатация компьютерных сетей
3	Производственная практика (эксплуатация автоматизированных (информационных) систем в защищенном исполнении)
4	Учебная практика (эксплуатация автоматизированных (информационных) систем в защищенном исполнении)
5	Экзамен по модулю (эксплуатация автоматизированных (информационных) систем в защищенном исполнении)

2. ЦЕЛИ, ЗАДАЧИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

Цели освоения: Формирование у студентов системных знаний в области архитектуры компьютерных сетей, сетевых протоколов, методов адресации, а также практических навыков администрирования, диагностики, настройки средств защиты информации и обеспечения бесперебойной работы автоматизированных систем в защищенном исполнении.
Задачи: 1. Изучить теоретические основы эталонной модели взаимодействия открытых систем (OSI), стеков протоколов TCP/IP, принципов маршрутизации и глобальной адресации.
2. Освоить методы конфигурирования и монтажа физических и логических компонентов локальных и распределенных вычислительных сетей.
3. Сформировать умения по диагностике отказов, восстановлению работоспособности и техническому обслуживанию активного сетевого оборудования.
4. Овладеть практическими навыками настройки программно-аппаратных средств криптографической и межсетевой защиты информации в автоматизированных системах.
5. Изучить регламенты эксплуатации, порядок ввода в действие средств защиты и методы мониторинга состояния информационной безопасности сетей.
Изучение дисциплины направлено на формирование у обучающихся следующих компетенций:

ПК 1.2.: Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении
ПК 1.2.1: Знать теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации
ПК 1.2.2: Уметь организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы
ПК 1.2.3: Иметь практический опыт администрирования автоматизированных систем в защищенном исполнении
ПК 1.3.: Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
ПК 1.3.1: Знать порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях
ПК 1.3.2: Уметь настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам
ПК 1.3.3: Иметь практический опыт эксплуатации компонентов систем защиты информации автоматизированных систем
ПК 1.4.: Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
ПК 1.4.1: Знать принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации
ПК 1.4.2: Уметь обеспечивать работоспособность, обнаруживать и устранять неисправности
ПК 1.4.3: Иметь практический опыт диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении

2.3	**Иметь практический опыт:**
2.3.1	ПК 1.1: Иметь навыки установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

2.3.2	ПК 1.2: Иметь навыки администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении.
2.3.3	ПК 1.3: Иметь навыки обеспечения бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
2.3.4	ПК 1.4: Иметь навыки и опыт деятельности по проверке технического состояния, техническому обслуживанию, текущему ремонту, устранению отказов и восстановлению работоспособности автоматизированных (информационных) систем в защищенном исполнении.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов, тем и содержание занятий /вид занятия/	Семестр / Курс	Часов/ в том числе	Компетен-ции	Виды контроля
	1. РАЗДЕЛ 1. БАЗОВЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ				
1. 1	Тема 1.1. Классификация и архитектура компьютерных сетей Виды сетей по территориальному признаку (PAN, LAN, MAN, WAN). Топологии физических и логических соединений (шина, звезда, кольцо, ячеистая). Принципы коммутации каналов, пакетов и ячеек. Сравнительная характеристика сетей с выделенным сервером и одноранговых сетей. Знать: определения локальной, региональной и глобальной сети; основные топологии и их свойства; различия между коммутацией каналов и пакетов; преимущества и недостатки одноранговых сетей и сетей на основе сервера; физические среды передачи данных (витая пара, оптоволокно, радиоэфир). /Лек/	4	4/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос
1. 2	Тема 1.2. Эталонная модель OSI и стек TCP/IP Семиуровневая модель взаимодействия открытых систем. Функции каждого уровня: физического, канального, сетевого, транспортного, сеансового, представительского и прикладного. Стек протоколов TCP/IP, его четырехуровневая структура и соответствие модели OSI. Инкапсуляция данных и PDU (блоки данных протокола). Знать: названия и функции всех 7 уровней OSI; соответствие уровней TCP/IP модели OSI; структуру заголовков основных протоколов (Ethernet, IP, TCP, UDP); понятие инкапсуляции и деинкапсуляции; назначение портов транспортного уровня. /Лек/	4	6/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос
1. 3	Практическая работа 1.1. Анализ инкапсуляции данных в модели OSI/TCP/IP Уметь: определять блоки данных на каждом уровне, сопоставлять протоколы с уровнями модели. Владеть: навыками использования справочных материалов для идентификации протоколов. /Пр/	4	4/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по практической работе
	2. РАЗДЕЛ 2. ФИЗИЧЕСКИЙ И КАНАЛЬНЫЙ УРОВНИ				
2. 1	Тема 2.1. Физическая среда передачи и кодирование сигналов Характеристики медных и оптических кабелей, беспроводных сред. Методы цифрового кодирования (NRZ, Manchester, 4B/5B). Помехоустойчивость, затухание и перекрестные помехи. Стандарты структурированных кабельных систем (EIA/TIA-568). Знать: типы кабелей (UTP, STP, коаксиальный,	4	4/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос

	одномодовое/многомодовое волокно); принципы кодирования сигналов; факторы, влияющие на качество передачи; категории витой пары; назначение коннекторов (RJ-45, LC, SC). /Лек/				
2. 2	Тема 2.2. Технологии локальных сетей на канальном уровне (Ethernet, Wi-Fi) Семейство стандартов IEEE 802.3 (Ethernet), форматы кадров (Ethernet II и 802.3). Технология коммутации, прозрачные мосты и алгоритм Spanning Tree Protocol (STP). Работа беспроводных сетей IEEE 802.11 (Wi-Fi), режимы инфраструктуры и Ad-Hoc, методы доступа CSMA/CD и CSMA/CA. Знать: структуру MAC-адреса; принцип работы коммутатора (свитча); алгоритм обучения таблицы MAC-адресов; различия между хабом, мостом и коммутатором; особенности протоколов 802.11a/b/g/n/ac. /Лек/	4	4/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос
2. 3	Практическая работа 2.1. Расчет параметров Ethernet-сегментов Уметь: рассчитывать максимальную длину сегмента с учетом задержек (PDV), подбирать типы кабелей. Владеть: методикой расчетов коллизионных доменов. /Пр/	4	4/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчёт по практической работе
2. 4	Лабораторная работа 2.1. Настройка коммутатора и просмотр MAC-таблицы Уметь: подключаться к управляемому коммутатору, просматривать и очищать таблицу MAC-адресов, отключать/включать порты. Владеть: навыками работы с командной строкой оборудования Cisco/Eltex. /Лаб/	4	4/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по лабораторной работе
	3. РАЗДЕЛ 3. СЕТЕВОЙ УРОВЕНЬ И ПРОТОКОЛ IP				
3. 1	Тема 3.1. Протокол IP. Принципы адресации (IPv4) Структура заголовка IPv4. Классовые и бесклассовые схемы адресации (CIDR). Правила выделения адресов подсети, широковещательных адресов и адресов хостов. Публичные и частные адресные пространства (RFC 1918). Понятие маски подсети и префикса. Знать: размеры полей IPv4-адреса; диапазоны классов A, B, C; принцип деления сети на подсети; механизм работы ARP; алгоритм проверки принадлежности адреса подсети. /Лек/	4	6/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос
3. 2	Практическая работа 3.1. Конфигурирование статических IP-адресов на хостах Уметь: настраивать параметры IPv4 на ОС Windows/Linux, проверять связность командой ping. Владеть: навыками устранения конфликтов адресации. /Пр/	4	4/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по практической работе
3. 3	Лабораторная работа 3.1. Расчет подсетей и построение схемы адресации Уметь: производить бинарные и десятичные вычисления масок, разбивать сеть на заданное количество подсетей, назначать адреса интерфейсам. Владеть: навыками быстрого подсчета количества	4	6/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по лабораторной работе

	хостов в подсети. /Лаб/				
3. 4	Самостоятельная работа по теме «Бесклассовая адресация (CIDR) и агрегирование маршрутов» /СР/	4	4/0	ПК 1.2.1,ПК 1.2.2,ПК 1.2.3,ПК 1.3.1,ПК 1.3.2,ПК 1.3.3,ПК 1.4.1,ПК 1.4.2,ПК 1.4.3	Вопросы для самоподготовки
3. 5	Тема 3.2. Протоколы маршрутизации (RIP, OSPF) Цели и задачи маршрутизации. Дистанционно-векторные протоколы (RIP v1/v2) и протоколы состояния каналов (OSPF). Анализ метрик, алгоритмов подсчета стоимости маршрута, области маршрутизации. Принципы работы таблиц маршрутизации и механизмы предотвращения петель (Split Horizon, Poison Reverse). Знать: отличия статической и динамической маршрутизации; параметры RIP (хопы, 30 сек обновления); особенности OSPF (метрика на основе пропускной способности, иерархия); понятие административной дистанции. /Лек/	4	6/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос
3. 6	Практическая работа 3.2. Настройка статической маршрутизации на маршрутизаторах Уметь: прописывать статические маршруты, проверять трассировку маршрута (tracert). Владеть: навыками выбора next-hop адреса. /Пр/	4	4/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по практической работе
3. 7	Лабораторная работа 3.2. Активация динамической маршрутизации RIP Уметь: включать протокол RIP на интерфейсах, просматривать динамически построенную таблицу. Владеть: навыками отладки маршрутизации (debug ip rip). /Лаб/	4	4/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по лабораторной работе
	4. РАЗДЕЛ 4. ТРАНСПОРТНЫЙ УРОВЕНЬ И ПРИКЛАДНЫЕ ПРОТОКОЛЫ				
4. 1	Тема 4.1. Протоколы TCP и UDP Детальное изучение сегмента TCP: поля портов, порядковые номера, флаги (SYN, ACK, FIN, RST). Механизм установления соединения "трехэтапное рукопожатие" и закрытия соединения. Алгоритмы управления потоком (скользящее окно) и предотвращения перегрузок. Упрощенный заголовок UDP и его использование для мультимедиа и DNS. Знать: основные отличия TCP от UDP; структуру сегмента TCP; последовательность состояний соединения; принцип работы окна; порты известных служб (20,21,22,23,25,53,80,443,110). /Лек/	4	4/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос
4. 2	Практическая работа 4.1. Анализ дампов трафика TCP/UDP в Wireshark Уметь: захватывать трафик, фильтровать пакеты по протоколам, анализировать флаги TCP. Владеть: навыками работы с сетевым анализатором Wireshark. /Пр/	4	2/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по практической работе
4. 3	Тема 4.2. Базовые прикладные сервисы (DHCP, DNS, HTTP)	4	4/0	ПК 1.2.1,ПК	Устный опрос

	Принципы работы протокола динамической конфигурации хостов (DHCP) и его цикл DORA. Иерархическая система доменных имен (DNS), типы записей (A, AAAA, CNAME, MX). Работа протокола HTTP/HTTPS, методы запросов и коды состояния. Знать: назначение DHCP-сервера; этапы получения IP-адреса; структуру DNS-запроса; различие рекурсивного и итеративного запросов; основные методы HTTP (GET, POST) и группы кодов ошибок. /Лек/			1.3.1,ПК 1.4.1	
4. 4	Лабораторная работа 4.1. Настройка DHCP-сервера и статической привязки адресов Уметь: конфигурировать пулы адресов, исключать адреса, настраивать аренду (lease). Владеть: навыками диагностики проблем получения IP-адреса (ipconfig /renew). /Лаб/	4	4/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по лабораторной работе
	5. РАЗДЕЛ 5. ТЕХНОЛОГИИ ОБЪЕДИНЕНИЯ СЕТЕЙ И VPN				
5. 1	Тема 5.1. NAT и трансляция адресов Механизмы трансляции сетевых адресов (Static NAT, Dynamic NAT, PAT/Masquerading). Проблемы, решаемые с помощью NAT, и ограничения протокола. Анализ таблиц трансляции и методы проброса портов. Знать: различия между SNAT и DNAT; понятие перегруженного NAT; принцип работы NAT для протоколов, отличных от TCP/UDP (например, ICMP). /Лек/	4	2/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос
5. 2	Практическая работа 5.1. Организация выхода в интернет через NAT на маршрутизаторе Уметь: настраивать правило ip nat inside/outside, задавать список доступа для трансляции. Владеть: навыками проверки NAT-сессий (show ip nat translations). /Пр/	4	4/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по практической работе
5. 3	Тема 5.2. Основы виртуальных частных сетей (VPN) Концепции туннелирования, инкапсуляции трафика, шифрования. Протоколы PPTP, L2TP, IPSec. Режимы работы IPSec (транспортный и туннельный), аутентификация с использованием сертификатов и предварительных ключей. Знать: назначение VPN; функции ESP и AH в IPSec; отличия туннельного режима от транспортного; принципы работы IKE. /Лек/	4	4/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос
5. 4	Лабораторная работа 5.1. Настройка межсетевого экрана и VPN-туннеля Уметь: создавать политики безопасности, настраивать предложения (transform-set) для IPSec. Владеть: практическим опытом проверки статуса туннеля (show crypto isakmp sa). /Лаб/	4	2/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по лабораторной работе
	6. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ				
6. 1	Контрольная работа ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с	4	0/0	ПК 1.2.1,ПК 1.2.2,ПК 1.2.3,ПК 1.3.1,ПК 1.3.2,ПК 1.3.3,ПК 1.4.1,ПК	Вопросы для контрольной работы

	требованиями эксплуатационной документации ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении /К/			1.4.2,ПК 1.4.3	
	7. РАЗДЕЛ 6. БЕЗОПАСНОСТЬ СЕТЕЙ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ				
7. 1	Тема 6.1. Основы криптографической защиты в сетях Симметричные и асимметричные алгоритмы шифрования, их преимущества и недостатки. Хеш -функции и их роль в обеспечении целостности. Протоколы SSL/TLS, процесс рукопожатия и сертификаты X.509. Принципы работы электронной подписи. Знать: разницу между блочными и поточными шифрами; назначение алгоритмов AES, RSA, SHA; структуру цифрового сертификата; понятие инфраструктуры открытых ключей (PKI). /Лек/	5	2/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос
7. 2	Лабораторная работа 6.1. Анализ SSL-сертификатов веб-серверов Уметь: просматривать цепочку сертификатов, сроки действия, алгоритмы подписи. Владеть: навыками проверки подлинности сервера через браузер и openssl. /Лаб/	5	4/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по лабораторной работе
7. 3	Тема 6.2. Межсетевые экраны и политики доступа Виды межсетевых экранов (пакетные фильтры, stateful, прокси-серверы). Правила фильтрации на основе IP-адресов, портов и состояния соединения. Списки контроля доступа (ACL) расширенные и стандартные. Методы защиты от атак типа SYN-flood, IP-spoofing. Знать: логику обработки пакетов в межсетевом экране; структуру расширенного ACL; принцип работы stateful-инспекции; порядок применения правил (сверху вниз). /Лек/	5	4/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос
7. 4	Практическая работа 6.1. Конфигурирование расширенных ACL для ограничения трафика Уметь: создавать правила разрешающие/запрещающие протоколы (например, HTTP, ICMP). Владеть: навыками привязки ACL к интерфейсам и тестирования фильтрации. /Пр/	5	4/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по практической работе
7. 5	Лабораторная работа 6.2. Настройка систем обнаружения вторжений (IDS) Уметь: активировать базовые сигнатуры, просматривать логи срабатываний. Владеть: навыками анализа предупреждений о подозрительной активности. /Лаб/	5	4/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по лабораторной работе
	8. РАЗДЕЛ 7. АДМИНИСТРИРОВАНИЕ И ЗАЩИЩЕННОЕ ИСПОЛНЕНИЕ АС				
8. 1	Тема 7.1. Управление учетными записями и сетевой аутентификацией Протоколы RADIUS и TACACS+ для централизованной аутентификации, авторизации и учета (AAA). Методы хранения паролей (хеши, соль). Политики сложности паролей и многофакторная аутентификация. Разграничения	5	2/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос

	прав администраторов на сетевое оборудование. Знать: различия между RADIUS и TACACS+; принцип работы AAA-сервера; понятие привилегированных уровней доступа (Cisco privilege levels); требования к парольной политике. /Лек/				
8. 2	Практическая работа 7.1. Настройка локальной аутентификации на маршрутизаторе Уметь: устанавливать пароли на консоль, VTY, режим enable, шифровать пароли сервисом service password-encryption. Владеть: навыками восстановления доступа при потере пароля. /Пр/	5	4/0	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по практической работе
8. 3	Тема 7.2. Мониторинг и диагностика сетевых устройств Протоколы SNMP (версии v1, v2c, v3) для мониторинга состояния устройств. MIB-переменные, OID, работа системы оповещений (traps). Применение систем Syslog для централизованного сбора логов. Методы диагностики физических повреждений и логических ошибок (ping, traceroute, debugs). Знать: архитектуру SNMP (менеджер, агент); настройку community-строк; уровни логирования Syslog; признаки отказа интерфейсов. /Лек/	5	4/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос
8. 4	Лабораторная работа 7.1. Настройка SNMP-агента и сбор статистики интерфейсов Уметь: включать SNMP на оборудовании, настраивать traps для оповещения о падении порта. Владеть: навыками использования MIB-браузера для получения статуса портов. /Лаб/	5	6/4	ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	Отчет по лабораторной работе
8. 5	Самостоятельная работа по теме «Протоколы удаленного управления (SSH, Telnet) и безопасность управления» /СР/	5	4/0	ПК 1.2.1,ПК 1.2.2,ПК 1.2.3,ПК 1.3.1,ПК 1.3.2,ПК 1.3.3,ПК 1.4.1,ПК 1.4.2,ПК 1.4.3	Вопросы для самоподготовки
	9. РАЗДЕЛ 8. ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ВОССТАНОВЛЕНИЕ РАБОТОСПОСОБНОСТИ				
9. 1	Тема 8.1. Регламенты технического обслуживания и резервное копирование конфигураций Виды ТО (ежедневное, еженедельное, ежегодное). Методы резервирования конфигурационных файлов (startup-config/running-config), протокол TFTP/FTP для их сохранения. Планы аварийного восстановления (DRP), процедуры замены оборудования без остановки сети. Знать: перечень обязательных проверок для сетевого оборудования; команды для сохранения и копирования конфигурации; понятие версионности конфигураций; требования к документированию сети. /Лек/	5	2/0	ПК 1.2.1,ПК 1.3.1,ПК 1.4.1	Устный опрос
9. 2	Практическая работа 8.1. Архивирование и восстановление конфигурации через TFTP Уметь: копировать конфигурацию на внешний	5	6/0	ПК 1.2.2,ПК 1.2.3,ПК	Отчет по практической работе

	сервер, загружать конфигурацию при сбое. Владеть: навыками сравнения резервных и текущих конфигураций. /Пр/			1.3.2,ПК 1.3.3,ПК 1.4.2,ПК 1.4.3	
	10. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ				
10. 1	Контрольная работа ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении /К/	5	0/0	ПК 1.2.1,ПК 1.2.2,ПК 1.2.3,ПК 1.3.1,ПК 1.3.2,ПК 1.3.3,ПК 1.4.1,ПК 1.4.2,ПК 1.4.3	Вопросы для контрольной работы, итоговое тестирование

Список выбранных образовательный технологий:

Название	Описание
Информационные технологии	Личностно ориентированная технология, способ организации самостоятельной деятельности учащихся, направленный на решение задачи учебного проекта
Компьютерная технология обучения	Основана на использовании информационных технологий в учебном процессе. Реализация данной технологии осуществляется посредством компьютера и иных мультимедийных средств. Использование компьютерных технологий делает учебный процесс не только современным и познавательным, но интересным для обучающихся

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ

Оценочные средства текущего контроля успеваемости:

ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

РАЗДЕЛ 1. БАЗОВЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Тема 1.1. Классификация и архитектура компьютерных сетей
1. Какие типы сетей выделяются по территориальному охвату?
2. Чем топология "звезда" отличается от топологии "кольцо" в плане отказоустойчивости?
3. Какой тип коммутации используется в классической телефонной сети?
4. В чем преимущества пакетной коммутации перед канальной?
5. Назовите среды передачи данных, устойчивые к электромагнитным помехам.
6. Какую топологию чаще всего используют в современных корпоративных сетях с коммутаторами?
7. Что такое логическая топология и чем она отличается от физической?
8. Какие факторы влияют на выбор топологии сети?
9. В чем суть работы одноранговой сети?
10. Какова роль сетевого концентратора (хаба) в локальной сети?

Тема 1.2. Эталонная модель OSI и стек TCP/IP
1. Какой уровень модели OSI отвечает за сегментацию данных и управление потоком?
2. Какому уровню OSI соответствует протокол IP?
3. Назовите блок данных (PDU) канального уровня.
4. Что такое инкапсуляция и на каком уровне она начинается?
5. Какие протоколы входят в прикладной уровень стека TCP/IP?
6. Для чего нужен уровень представления (Presentation) в модели OSI?
7. Какую функцию выполняет протокол ARP в рамках сетевого уровня?
8. Чем отличается сеансовый уровень от транспортного?
9. Какой протокол стека TCP/IP является основным для передачи почтовых сообщений (SMTP)?
10. Каким образом уровни OSI взаимодействуют между собой на одной машине?

РАЗДЕЛ 2. ФИЗИЧЕСКИЙ И КАНАЛЬНЫЙ УРОВНИ

Тема 2.1. Физическая среда передачи и кодирование сигналов
1. Какие характеристики присущи витой паре категории 6?

2. В чем отличие многомодового оптоволокна от одномодового?
3. Какой метод кодирования использует манчестерский код?
4. Что такое затухание сигнала и как оно измеряется?
5. Какие виды помех возникают в медных кабелях?
6. Назовите максимальную длину сегмента для 10BASE-T.
7. Какие разъемы применяются для подключения оптоволокна?
8. Для чего используется экранирование в кабелях STP?
9. Какие частоты сигналов используются в стандарте 1000BASE-T?
10. Как влияет диаметр сердцевины оптоволокна на пропускную способность?

Тема 2.2. Технологии локальных сетей на канальном уровне (Ethernet, Wi-Fi)
1. Какую длину имеет MAC-адрес и в каких единицах он записывается?
2. Как коммутатор строит свою таблицу MAC-адресов?
3. Для чего необходим протокол STP?
4. В чем суть алгоритма CSMA/CA?
5. Какие виды кадров Ethernet существуют?
6. Что такое коллизионный домен?
7. Как коммутатор обрабатывает широковещательный фрейм?
8. Какой режим работы Wi-Fi подразумевает наличие точки доступа?
9. Какова максимальная скорость в стандарте 802.11ac?
10. Чем управляемый коммутатор отличается от неуправляемого?

РАЗДЕЛ 3. СЕТЕВОЙ УРОВЕНЬ И ПРОТОКОЛ IP

Тема 3.1. Протокол IP. Принципы адресации (IPv4)
1. Сколько октетов в адресе IPv4?
2. Какие адреса относятся к классу C?
3. Что обозначает маска подсети /24?
4. Какой адрес в подсети является широковещательным?
5. Для чего предназначен адрес 127.0.0.1?
6. Какие адреса выделены для частного использования (RFC 1918) в классе B?
7. Как работает протокол ARP в одной подсети?
8. Каким образом можно определить, принадлежат ли два адреса одной подсети?
9. Что такое CIDR и как он записывается?
10. Какая информация хранится в кэше ARP?

Тема 3.2. Протоколы маршрутизации (RIP, OSPF)
1. Что такое дистанционно-векторный протокол?
2. Назовите основную метрику в протоколе RIP.
3. Сколько хопов считается бесконечностью в RIP?
4. Что такое зона (area) в OSPF?
5. Как OSPF вычисляет стоимость маршрута?
6. Для чего используется механизм Split Horizon?
7. Какой протокол быстрее сходится при изменениях: RIP или OSPF?
8. Какой алгоритм лежит в основе OSPF?
9. Что такое административная дистанция протокола?
10. На каком уровне стека TCP/IP работает протокол OSPF?

РАЗДЕЛ 4. ТРАНСПОРТНЫЙ УРОВЕНЬ И ПРИКЛАДНЫЕ ПРОТОКОЛЫ

Тема 4.1. Протоколы TCP и UDP
1. Какие флаги устанавливаются в первом сегменте TCP при открытии соединения?
2. Какова функция поля "Sequence Number" в TCP?
3. Чем отличается закрытие соединения TCP от открытия?
4. Каков размер заголовка UDP в байтах?
5. Какой порт использует протокол HTTPS?
6. В каких случаях UDP предпочтительнее TCP?
7. Что такое механизм скользящего окна?
8. Как TCP предотвращает перегрузки сети?
9. Что произойдет, если получен ACK не на тот порядковый номер?
10. Какой протокол использует SNMP для передачи данных?

Тема 4.2. Базовые прикладные сервисы (DHCP, DNS, HTTP)
1. Что такое пул адресов в DHCP?
2. Какие сообщения входят в последовательность DORA?
3. Какую запись в DNS необходимо создать для привязки имени к IPv6 адресу?
4. Что означает код ответа HTTP 404?
5. Как работает рекурсивный запрос к DNS-серверу?

6. Как долго действует аренда (lease) IP-адреса по умолчанию?
7. Какие методы HTTP считаются небезопасными с точки зрения видимости данных?
8. Где в DNS хранится информация о почтовых серверах домена?
9. Что такое DHCP-опции и для чего они нужны?
10. Как браузер определяет IP-адрес сайта, если он не в кэше?

РАЗДЕЛ 5. ТЕХНОЛОГИИ ОБЪЕДИНЕНИЯ СЕТЕЙ И VPN

Тема 5.1. NAT и трансляция адресов
1. Какое основное назначение NAT?
2. В чем отличие статического NAT от динамического?
3. Что такое PAT и как он работает?
4. Какой адрес называют "inside global"?
5. Какие проблемы создания сквозных соединений создает NAT?
6. Для чего служит проброс портов (port forwarding)?
7. Какие протоколы не могут пройти через обычный NAT без дополнительных модулей?
8. Как настраивается NAT в сетях с несколькими WAN-интерфейсами?
9. Как проверить активные NAT-трансляции на маршрутизаторе?
10. Почему в IPv6 NAT не является обязательным механизмом?

Тема 5.2. Основы виртуальных частных сетей (VPN)
1. В чем суть туннелирования трафика?
2. На каких уровнях модели OSI работают протоколы PPTP и L2TP?
3. Какие протоколы входят в стек IPSec?
4. Чем транспортный режим IPSec отличается от туннельного?
5. Что такое IKE и зачем он нужен?
6. Какой протокол является более защищенным: PPTP или IPSec?
7. Что такое предварительный общий ключ (PSK)?
8. Какие алгоритмы шифрования можно использовать в IPSec?
9. Что такое фаза 1 (Main Mode) в IKE?
10. Как VPN обеспечивает защиту от прослушивания?

РАЗДЕЛ 6. БЕЗОПАСНОСТЬ СЕТЕЙ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 6.1. Основы криптографической защиты в сетях
1. Назовите основной недостаток симметричного шифрования.
2. Для каких целей применяется хеш-функция SHA-256?
3. Что такое цифровая подпись и что она гарантирует?
4. Какой порт использует протокол HTTPS?
5. Какой алгоритм используется для обмена ключами в SSL/TLS?
6. Что такое сертификат X.509?
7. Кто является центром сертификации (CA)?
8. Как происходит проверка срока действия сертификата?
9. Чем отличается асимметричный шифр от хеширования?
10. Что такое PVK и PBK (открытый/закрытый ключ)?

Тема 6.2. Межсетевые экраны и политики доступа
1. Какой межсетевой экран называется stateful?
2. Какие параметры проверяет стандартный ACL?
3. Что может делать расширенный ACL, чего не может стандартный?
4. Какой принцип обработки правил в ACL?
5. На каких уровнях модели OSI работает межсетевой экран, использующий прокси?
6. Как защититься от SYN-атаки?
7. Что такое неявный запрет (implicit deny)?
8. Какую команду нужно ввести, чтобы применить ACL к интерфейсу?
9. Что такое спуфинг IP-адреса?
10. Как фильтруются исходящие соединения на межсетевом экране?

РАЗДЕЛ 7. АДМИНИСТРИРОВАНИЕ И ЗАЩИЩЕННОЕ ИСПОЛНЕНИЕ АС

Тема 7.1. Управление учетными записями и сетевой аутентификацией
1. Что входит в концепцию AAA?
2. Для чего используется протокол TACACS+?
3. В чем преимущество RADIUS перед локальной аутентификацией?
4. Какой стандарт шифрования паролей рекомендуется на сетевых устройствах?
5. Что такое привилегированный режим EXEC?
6. Какой протокол позволяет передавать пароли в открытом виде и почему это опасно?
7. Какие факторы относятся к двухфакторной аутентификации?

8. Как задается пароль на консольном порту маршрутизатора?
9. Что такое таймаут сессии и зачем он нужен?
10. Где хранятся базы пользователей для локальной аутентификации?

Тема 7.2. Мониторинг и диагностика сетевых устройств
1. Что такое OID в контексте SNMP?
2. Для чего используются traps в SNMP?
3. Какая версия SNMP поддерживает шифрование?
4. Какую информацию можно получить через MIB-переменные?
5. Какой уровень логирования Syslog записывает критические ошибки?
6. Чем отличается ping от traceroute при диагностике?
7. Какой командой можно посмотреть загрузку процессора на маршрутизаторе?
8. Как настраивается отправка syslog-сообщений на удаленный сервер?
9. Что такое инвентаризация оборудования?
10. Какие данные содержатся в логах интерфейсов?

РАЗДЕЛ 8. ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ВОССТАНОВЛЕНИЕ РАБОТОСПОСОБНОСТИ

Тема 8.1. Регламенты технического обслуживания и резервное копирование конфигураций
1. Какие конфигурации существуют на сетевом устройстве?
2. Какой протокол чаще всего используется для резервного копирования конфигураций?
3. Какие действия входят в ежедневное техническое обслуживание?
4. Как восстановить конфигурацию при загрузке с нового устройства?
5. Зачем нужен план аварийного восстановления?
6. Как документируются изменения в сети?
7. Что такое "холодный резерв" оборудования?
8. Какие команды позволяют посмотреть изменения в конфигурации?
9. Как часто рекомендуется менять пароли доступа?
10. Как проверить целостность сохраненной конфигурации?

ВОПРОСЫ ДЛЯ САМОПОДГОТОВКИ

Самостоятельная работа по теме «Бесклассовая адресация (CIDR) и агрегирование маршрутов»
1. Каковы причины перехода от классовой адресации к бесклассовой?
2. Как рассчитывается длина префикса для агрегированного маршрута?
3. Что такое маршрут по умолчанию и в каких случаях он применяется?
4. Как работает алгоритм поиска наиболее точного совпадения?
5. В чем разница между VLSM и FLSM?
6. Как агрегирование маршрутов влияет на размер таблиц маршрутизации?
7. Возможно ли агрегирование сетей с разными длинами масок?
8. Приведите пример агрегированного маршрута для блоков 192.168.0.0/24 и 192.168.1.0/24.
9. Какие проблемы могут возникнуть при излишнем агрегировании?
10. Как агрегирование связано с концепцией суперсети?

Самостоятельная работа по теме «Протоколы удаленного управления (SSH, Telnet) и безопасность управления»
1. В чем принципиальное отличие SSH от Telnet с точки зрения безопасности?
2. Как осуществляется генерация ключевых пар для SSH на сетевом устройстве?
3. Какие версии SSH существуют и чем они различаются?
4. Почему рекомендуется отключать Telnet на всех управляемых устройствах?
5. Как ограничить круг IP-адресов, с которых разрешено SSH-подключение?
6. Какие алгоритмы шифрования используются в SSH-сессии?
7. Как выполняется аутентификация по открытому ключу в SSH?
8. Что такое SSH-туннелирование и для чего оно применяется?
9. Как настройка SSH связана с обеспечением защищенного исполнения АС (ПК 1.2.1)?
10. Какие команды используются для мониторинга активных SSH-сессий?

ЗАДАНИЯ НА ПРАКТИЧЕСКИЕ И ЛАБОРАТОРНЫЕ РАБОТЫ

РАЗДЕЛ 1. БАЗОВЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ
Практическая работа 1.1. Анализ инкапсуляции данных в модели OSI/TCP/IP
Задания:
1. По заданному прикладному протоколу (например, HTTP, FTP, SMTP) определите, на каких уровнях модели OSI и TCP/IP формируются соответствующие блоки данных, и запишите их названия (PDU) для каждого уровня.
2. Для указанного набора протоколов (Ethernet, IP, TCP, UDP) сопоставьте каждый протокол с соответствующим уровнем модели OSI и стека TCP/IP, обоснуйте свой выбор.
3. По описанию передачи данных от приложения-клиента к приложению-серверу определите последовательность инкапсуляции данных, перечислив все заголовки, добавляемые на каждом уровне, в порядке их добавления.
4. По заданному дампу (текстовому описанию) сетевого пакета определите, к какому уровню относится каждый

фрагмент заголовка, и объясните, какие поля указывают на принадлежность протоколу.
5. Для заданного сценария (передача файла по протоколу FTP) опишите, как изменяется блок данных при прохождении от прикладного уровня до физического на отправляющей стороне и обратно на принимающей стороне.
6. Используя справочные материалы (таблицы соответствия протоколов и уровней), определите, к какому уровню стека TCP/IP относятся указанные протоколы (например, ICMP, ARP, BGP, SNMP), и запишите результат.

РАЗДЕЛ 2. ФИЗИЧЕСКИЙ И КАНАЛЬНЫЙ УРОВНИ
Лабораторная работа 2.1. Настройка коммутатора и просмотр MAC-таблицы
Задания:
1. Подключитесь к управляемому коммутатору через консольный порт или Telnet/SSH и выполните вход в привилегированный режим.
2. Просмотрите текущую таблицу MAC-адресов коммутатора, определите, какие MAC-адреса и на каких портах зафиксированы.
3. Очистите динамическую таблицу MAC-адресов с использованием соответствующей команды и повторно просмотрите таблицу, чтобы убедиться в её очистке.
4. Включите и отключите один из портов коммутатора, затем проверьте состояние порта и убедитесь, что подключенное устройство исчезло из таблицы MAC-адресов.
5. Подключите к коммутатору новое устройство (или эмулируйте его подключение), дождитесь появления его MAC-адреса в таблице и запишите, к какому порту он привязан.
6. Выполните команду для просмотра возраста (времени жизни) динамических записей MAC-таблицы и объясните, что произойдет с записью по истечении этого времени.

Практическая работа 2.1. Расчет параметров Ethernet-сегментов
Задания:
1. Для заданной конфигурации Ethernet-сегмента (количество коммутаторов, длина кабелей) определите, превышает ли общая задержка распространения сигнала допустимое значение для коллизионного домена.
2. По заданному типу кабеля (витая пара категории 5e или оптоволокно) и длине сегмента определите, возможна ли работа сети в стандарте 10BASE-T или 100BASE-TX без использования повторителей.
3. Для предложенной схемы сети определите, какие устройства находятся в одном коллизионном домене, а какие – в разных, и объясните свой ответ.
4. Рассчитайте максимально допустимую длину сегмента для заданной топологии с учётом числа повторителей (концентраторов), используя справочные значения задержек для каждого элемента.
5. По заданным параметрам (тип кабеля, стандарт Ethernet, количество коммутаторов в цепочке) определите, возможно ли построение данного сегмента без нарушения требований к времени оборота сигнала (PDV).
6. Для заданной сети с несколькими сегментами определите, какой тип кабеля (экранированная или неэкранированная витая пара, оптоволокно) предпочтительнее использовать на каждом участке, и обоснуйте выбор с точки зрения помехозащищённости и расстояния.

РАЗДЕЛ 3. СЕТЕВОЙ УРОВЕНЬ И ПРОТОКОЛ IP
Лабораторная работа 3.1. Расчет подсетей и построение схемы адресации
Задания:
1. Для заданной сети (например, 192.168.1.0/24) и количества требуемых подсетей (например, 4 подсети) рассчитайте маску для каждой подсети, количество хостов в каждой и перечислите все подсети с их сетевыми адресами.
2. Для заданной маски подсети (например, /26) определите количество допустимых адресов хостов в этой подсети, а также широковещательный адрес и адрес сети.
3. Выполните бинарное преобразование IP-адреса и маски подсети для заданной пары, затем с помощью поразрядной операции AND определите адрес сети.
4. Разбейте заданную сеть (например, 10.0.0.0/16) на подсети с условием, что в каждой подсети должно быть не менее 500 хостов, и запишите все полученные подсети с их диапазонами адресов.
5. Для заданного набора IP-адресов и масок определите, какие из адресов принадлежат одной подсети, а какие – разным, и запишите адрес сети для каждой группы.
6. Назначьте адреса интерфейсам маршрутизаторов и хостов в спроектированной схеме адресации таким образом, чтобы в каждой подсети был использован первый адрес для шлюза, а последний – как широковещательный.
7. Для заданной сети с несколькими подсетями составьте таблицу распределения адресов, указав для каждой подсети: сетевой адрес, маску, диапазон адресов для хостов, широковещательный адрес и адрес шлюза.
8. Проверьте корректность назначенных адресов, определив для каждого интерфейса, не конфликтует ли его адрес с сетевым или широковещательным адресом подсети.

Практическая работа 3.1. Конфигурирование статических IP-адресов на хостах
Задания:
1. На операционной системе Windows настройте статический IP-адрес, маску подсети и шлюз по умолчанию в соответствии с заданными параметрами.
2. На операционной системе Linux (или в эмуляторе терминала) выполните настройку сетевого интерфейса с указанием статического адреса и маски через командную строку.
3. После настройки IP-адреса проверьте связность с указанным узлом в той же подсети с помощью команды ping, проанализируйте результаты.
4. Намеренно задайте IP-адрес, который уже используется другим устройством в сети, затем с помощью команды ping и просмотра ARP-таблицы определите наличие конфликта адресации и устраните его.

5. Настройте на хосте несколько сетевых интерфейсов (или виртуальных адаптеров) с разными IP-адресами из разных подсетей и проверьте, что они корректно взаимодействуют с соответствующими шлюзами.
6. Измените маску подсети на хосте таким образом, чтобы он перестал видеть соседние узлы, и объясните причину потери связности.
7. Проверьте таблицу маршрутизации хоста после настройки статического адреса, определите, какие маршруты были добавлены автоматически.
8. Удалите статическую конфигурацию IP-адреса и переключите интерфейс на автоматическое получение адреса (DHCP), затем проверьте, что адрес изменился.

Практическая работа 3.2. Настройка статической маршрутизации на маршрутизаторах
Задания:
1. На маршрутизаторе настройте статический маршрут к указанной удаленной сети с указанием следующего шлюза (next -hop) по заданному IP-адресу.
2. Пропишите статический маршрут с указанием исходящего интерфейса вместо IP-адреса next-hop, объясните разницу между двумя способами.
3. Проверьте добавленный статический маршрут в таблице маршрутизации, определите его административную дистанцию и метрику.
4. Настройте маршрут по умолчанию (default route) на маршрутизаторе, указав шлюз, через который должны направляться все пакеты для неизвестных сетей.
5. Выполните трассировку маршрута (tracert/traceroute) до удаленного узла, проанализируйте каждый шаг и определите, какие маршрутизаторы участвуют в передаче.
6. Удалите один из статических маршрутов и проверьте, изменилась ли достижимость удаленной сети, затем восстановите маршрут.
7. Создайте резервный статический маршрут к той же сети, но с большей метрикой, и проверьте, что основной маршрут используется до тех пор, пока он доступен.
8. Настройте суммированный (агрегированный) статический маршрут для нескольких подсетей и проверьте, что все они становятся достижимы через один шлюз.

Лабораторная работа 3.2. Активация динамической маршрутизации RIP
Задания:
1. Включите протокол RIP на маршрутизаторе и укажите сети, которые должны участвовать в обмене маршрутной информацией.
2. Просмотрите динамически построенную таблицу маршрутизации после активации RIP и определите, какие маршруты были получены от соседних маршрутизаторов.
3. Настройте на одном из интерфейсов запрет на отправку RIP-обновлений (пассивный интерфейс) и проверьте, как это повлияет на соседние маршрутизаторы.
4. Активируйте отладку событий RIP с помощью команды debug ip rip и проследите процесс обмена маршрутными обновлениями между маршрутизаторами.
5. Измените параметр таймера обновления RIP на одном маршрутизаторе и проверьте, как это отразится на синхронизации таблиц соседей.
6. Включите аутентификацию в RIP между двумя маршрутизаторами и убедитесь, что обмен маршрутами продолжается только при совпадении ключей.
7. Искусственно создайте петлю маршрутизации (например, неправильной настройкой) и с помощью команды debug проследите, как механизмы Split Horizon и Poison Reverse её предотвращают.
8. Сравните таблицы маршрутизации до и после активации RIP, опишите, какие маршруты были добавлены динамически, а какие остались статическими.

РАЗДЕЛ 4. ТРАНСПОРТНЫЙ УРОВЕНЬ И ПРИКЛАДНЫЕ ПРОТОКОЛЫ
Практическая работа 4.1. Анализ дампов трафика TCP/UDP в Wireshark
Задания:
1. Запустите захват трафика на сетевом интерфейсе и выполните простое действие (например, открытие веб-страницы), затем остановите захват.
2. Отфильтруйте захваченные пакеты по протоколу TCP и определите, сколько сегментов было передано при установлении TCP-соединения.
3. Выберите любой TCP-пакет из установленного соединения и проанализируйте значения флагов (SYN, ACK, FIN, RST), объясните их смысл в контексте текущей сессии.
4. Отфильтруйте трафик по протоколу UDP и найдите пакеты, относящиеся к DNS-запросам, определите, какие порты используются отправителем и получателем.
5. В дампе TCP-трафика найдите сегмент с установленным флагом ACK и определите, подтверждение какого порядкового номера он передаёт.
6. Проанализируйте последовательность пакетов при закрытии TCP-соединения, определите, какой из сторон было инициировано закрытие.

Лабораторная работа 4.1. Настройка DHCP-сервера и статической привязки адресов
Задания:
1. На DHCP-сервере создайте пул адресов (scope) для заданной подсети, указав диапазон адресов, маску подсети и шлюз по умолчанию.
2. Исключите из пула несколько адресов, которые должны быть зарезервированы для статических устройств (например,

для серверов).
3. Настройте время аренды (lease) для выдаваемых адресов, установив его в соответствии с заданным значением (например, 8 часов).
4. Настройте статическую привязку (резервирование) IP-адреса для устройства с указанным MAC-адресом, чтобы оно всегда получало один и тот же адрес.
5. На клиентской машине выполните принудительное обновление аренды адреса с помощью команды ipconfig /renew (или dhclient для Linux) и убедитесь, что получен адрес из настроенного пула.
6. Проверьте статус аренды на DHCP-сервере, определите, какие адреса сейчас выданы, и кому (по MAC-адресам).
7. Освободите адрес на клиенте командой ipconfig /release, затем проверьте на сервере, что аренда освобождена и адрес вернулся в пул доступных.
8. Измените настройки пула (например, измените диапазон адресов или шлюз) и проверьте, что клиент получает новые параметры после обновления аренды.

РАЗДЕЛ 5. ТЕХНОЛОГИИ ОБЪЕДИНЕНИЯ СЕТЕЙ И VPN
Практическая работа 5.1. Организация выхода в интернет через NAT на маршрутизаторе
Задания:
1. На маршрутизаторе определите внутренние и внешние интерфейсы для организации NAT с помощью команд ip nat inside и ip nat outside.
2. Создайте список доступа (ACL), который определяет, какие внутренние частные адреса будут транслироваться при выходе во внешнюю сеть.
3. Настройте динамическую трансляцию NAT (PAT) с использованием созданного ACL и укажите внешний интерфейс для трансляции.
4. Проверьте активные NAT-сессии на маршрутизаторе с помощью команды show ip nat translations и определите, какие внутренние адреса транслируются в какие внешние.
5. Настройте статическую трансляцию (Static NAT) для обеспечения доступа из внешней сети к внутреннему серверу с заданным портом (проброс порта).
6. Удалите одну из динамических трансляций и проверьте, как это повлияет на доступ в интернет для соответствующего хоста.
7. Настройте резервный пул внешних адресов для NAT на случай недоступности основного интерфейса.
8. Проверьте работу NAT для протокола ICMP, выполнив ping на внешний адрес, и убедитесь, что ответ проходит через трансляцию.

Лабораторная работа 5.1. Настройка межсетевого экрана и VPN-туннеля
Задания:
1. На межсетевом экране создайте политику безопасности, которая разрешает прохождение трафика между внутренней и внешней сетями только по протоколу HTTPS.
2. Создайте политику, запрещающую любой ICMP-трафик (ping) из внешней сети во внутреннюю, и проверьте её работоспособность.
3. Настройте VPN-туннель с использованием протокола IPSec в туннельном режиме, задав параметры шифрования (transform-set) с алгоритмами AES и SHA.
4. Укажите для туннеля предварительный общий ключ (PSK) и настройте интересующий трафик (защищаемые сети) с помощью списков доступа.
5. Проверьте статус IKE-ассоциаций на этапе первой и второй фазы с помощью команды show crypto isakmp sa.
6. Проверьте статус IPSec-туннеля с помощью show crypto ipsec sa и определите, сколько пакетов зашифровано и расшифровано.
7. Внесите изменения в политику безопасности, разрешающую прохождение только зашифрованного трафика, и проверьте, что незашифрованный трафик блокируется.
8. Отключите туннель, изменив настройки на одной из сторон, и затем восстановите его работоспособность, проанализировав ошибки.

РАЗДЕЛ 6. БЕЗОПАСНОСТЬ СЕТЕЙ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ
Лабораторная работа 6.1. Анализ SSL-сертификатов веб-серверов
Задания:
1. Откройте в браузере указанный веб-сайт с поддержкой HTTPS и просмотрите информацию о его SSL-сертификате.
2. Определите цепочку сертификатов: корневой сертификат, промежуточный и сертификат сервера, запишите их названия.
3. Проверьте срок действия сертификата, определите, является ли он действительным на текущий момент.
4. Определите алгоритм подписи и хеширования, используемый в сертификате (например, SHA-256 с RSA).
5. С помощью утилиты командной строки openssl получите информацию о сертификате удалённого сервера, не открывая браузер.
6. Сравните два сертификата (например, от разных сайтов) по их издателю, сроку действия и алгоритмам, запишите основные отличия.
7. Изучите расширения сертификата (Subject Alternative Name - SAN) и определите, для каких доменных имён он действителен.
8. Проверьте, был ли сертификат отозван, используя доступные механизмы (CRL или OCSP, если доступно).

Практическая работа 6.1. Конфигурирование расширенных ACL для ограничения трафика
Задания:

1. Создайте расширенный список доступа (ACL), который разрешает только HTTP-трафик (порт 80) от одной подсети к веб-серверу.
2. Добавьте в тот же ACL правило, запрещающее любые ICMP-запросы (echo-request) из указанной подсети.
3. Создайте ACL, который разрешает SSH-соединения (порт 22) только с одного конкретного IP-адреса администратора.
4. Примените созданный ACL к интерфейсу маршрутизатора, указав направление (in или out), и проверьте фильтрацию.
5. Проверьте работу ACL, выполнив тестовые запросы (HTTP, ping, SSH) с разрешённых и запрещённых адресов.
6. Добавьте новое правило в существующий ACL, которое разрешает доступ к FTP-серверу (порт 21) из дополнительной подсети, и убедитесь, что порядок правил не нарушил логику.
7. Удалите одно из правил ACL и проверьте, как изменилась доступность сервисов для разрешённых ранее адресов.
8. Создайте ACL, который разрешает доступ ко всем сервисам, кроме запрещённого (например, запрет на Telnet), и примените его к виртуальным терминальным линиям (VTY) для управления самим маршрутизатором.

Лабораторная работа 6.2. Настройка систем обнаружения вторжений (IDS)
Задания:
1. На системе IDS активируйте базовый набор сигнатур для обнаружения сканирования портов (portscan) из внешней сети.
2. Выполните тестовое сканирование портов с указанного хоста и проверьте, зафиксировала ли система данное событие.
3. Просмотрите логи срабатываний IDS и найдите запись о подозрительной активности, определите тип атаки и источник.
4. Настройте сигнатуру для обнаружения попыток подбора пароля по протоколу SSH и проверьте её работу при нескольких неудачных попытках входа.
5. Включите режим оповещения (алерты) для критических сигнатур и убедитесь, что при срабатывании генерируется уведомление.
6. Добавьте в белый список (исключения) IP-адрес администратора, чтобы его действия не считались подозрительными.
7. Проверьте, как IDS реагирует на легитимный трафик (например, обычный просмотр веб-страниц), чтобы убедиться в отсутствии ложных срабатываний.
8. Отключите одну из сигнатур и повторно выполните тест, который ранее вызывал срабатывание, чтобы проверить влияние изменений.

РАЗДЕЛ 7. АДМИНИСТРИРОВАНИЕ И ЗАЩИЩЕННОЕ ИСПОЛНЕНИЕ АС
Практическая работа 7.1. Настройка локальной аутентификации на маршрутизаторе
Задания:
1. Установите пароль на консольное подключение к маршрутизатору с использованием команды line console 0.
2. Установите пароль на виртуальные терминальные линии (VTY) для удалённого доступа по Telnet/SSH.
3. Настройте пароль для входа в привилегированный режим (enable), используя для его хранения алгоритм шифрования типа 5 (MD5).
4. Включите шифрование всех хранящихся паролей в конфигурации с помощью сервиса service password-encryption.
5. Настройте локального пользователя с определённым уровнем привилегий и проверьте, что вход возможен с его учётными данными.
6. Измените пароль на VTY-линиях и проверьте, что старый пароль больше не принимается при подключении.
7. Намеренно сбросьте пароль enable (или «забудьте» его) и выполните процедуру восстановления доступа через механизм перезагрузки и пропуска начальной конфигурации.
8. После восстановления доступа заново настройте все пароли и сохраните изменённую конфигурацию в постоянную память.

Лабораторная работа 7.1. Настройка SNMP-агента и сбор статистики интерфейсов
Задания:
1. На сетевом устройстве включите SNMP-агент и задайте community-строку только для чтения (read-only).
2. Настройте вторую community-строку с правами на чтение и запись (read-write) для выполнения изменений.
3. Настройте отправку SNMP-ловушек (traps) на указанный менеджер при изменении состояния порта (up/down).
4. Используя MIB-браузер (или аналогичный инструмент), подключитесь к SNMP-агенту и получите значения OID, соответствующие статусу и скорости всех интерфейсов.
5. В MIB-браузере найдите OID, отвечающий за количество входящих ошибок на интерфейсе, и запишите его текущее значение.
6. Измените состояние порта (отключите/включите) и проверьте, что на менеджер пришла trap-ловушка с соответствующим оповещением.
7. Используя SNMP, удалённо получите информацию об использовании процессора и памяти устройства.
8. Настройте на SNMP-агенте ограничение доступа по IP-адресу менеджера, затем проверьте, что запросы с других адресов игнорируются.

РАЗДЕЛ 8. ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ВОССТАНОВЛЕНИЕ РАБОТОСПОСОБНОСТИ
Практическая работа 8.1. Архивирование и восстановление конфигурации через TFTP
Задания:
1. На маршрутизаторе просмотрите текущую рабочую конфигурацию (running-config) и сохраните её в постоянную память (startup-config).
2. Скопируйте текущую конфигурацию на TFTP-сервер с использованием команды copy running-config tftp, указав адрес сервера и имя файла.
3. Скопируйте сохранённую конфигурацию (startup-config) на TFTP-сервер в отдельный файл с другим именем для

резервного копирования.
4. Намеренно измените рабочую конфигурацию (например, добавьте лишний маршрут) и затем восстановите предыдущую конфигурацию из копии на TFTP-сервере.
5. Загрузите конфигурационный файл с TFTP-сервера в оперативную память маршрутизатора и активируйте его без перезагрузки.
6. Сравните текущую конфигурацию с резервной копией, используя команду для просмотра различий (например, show archive config differences).
7. Скопируйте конфигурацию с TFTP-сервера на новый маршрутизатор (или в эмулятор) и проверьте, что после загрузки он работает с теми же параметрами.
8. Создайте текстовый файл с резервной копией конфигурации на локальной машине и загрузите его обратно на устройство, убедившись в полном восстановлении работоспособности.

Оценочные средства промежуточной аттестации:

КОНТРОЛЬНАЯ РАБОТА (4 СЕМЕСТР)

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении
1. Чем отличается одноранговая сеть от сети с выделенным сервером с точки зрения управления доступом к ресурсам?
2. Какие основные преимущества пакетной коммутации перед коммутацией каналов наблюдаются при передаче данных в компьютерных сетях?
3. Каково основное назначение уровня представления (Presentation Layer) в эталонной модели OSI?
4. Какой блок данных (PDU) используется на транспортном уровне модели OSI и как он называется в стеке TCP/IP?
5. Какие параметры цифрового сигнала влияют на помехоустойчивость передачи данных по медному кабелю?
6. В чем заключается основное различие между одномодовым и многомодовым оптическим волокном?
7. Какую функцию выполняет алгоритм Spanning Tree Protocol (STP) в коммутируемой локальной сети?
8. Какой метод доступа используется в беспроводных сетях Wi-Fi и чем он принципиально отличается от метода доступа в проводных Ethernet-сетях?

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
9. Как по IP-адресу и маске подсети определить, является ли адрес широковещательным для данной подсети?
10. Какую проблему решает механизм ARP (Address Resolution Protocol) в IP-сетях?
11. В чем заключается основное отличие протокола динамической маршрутизации OSPF от RIP?
12. Что такое административная дистанция протокола маршрутизации и для чего она используется?
13. Какие флаги в заголовке TCP используются для установления соединения и как называется эта последовательность?
14. Какое поле в заголовке UDP позволяет принимать данные нескольким приложениям одновременно на одном хосте?
15. Какие этапы включает в себя цикл DORA при получении IP-адреса от DHCP-сервера?

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
16. Какая запись в системе DNS используется для указания почтового сервера домена и как она работает?
17. В каком случае применяется статический NAT, а в каком – динамический NAT и чем они различаются?
18. Что такое PAT (Port Address Translation) и какую задачу он решает в сетях с недостатком публичных IPv4-адресов?
19. Какие основные протоколы используются для построения VPN-туннелей в современных сетях?
20. В чем разница между транспортным и туннельным режимами работы протокола IPSec?
21. В чем отличие протокола HTTPS от HTTP с точки зрения защиты передаваемых данных?
22. Какую информацию хранит таблица маршрутизации маршрутизатора и по какому принципу выбирается маршрут для доставки пакета?

КОНТРОЛЬНАЯ РАБОТА (5 СЕМЕСТР)

Индикатор ЗНАТЬ

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении
1. Установите правильную последовательность этапов инкапсуляции данных при передаче от прикладного уровня до физического в стеке TCP/IP
А) Инкапсуляция в сегмент транспортного уровня
Б) Инкапсуляция в кадр канального уровня с добавлением MAC-адресов
В) Инкапсуляция в дейтаграмму сетевого уровня с добавлением IP-адресов
Г) Преобразование в битовый поток для передачи по физической среде
2. Установите правильную последовательность этапов установления TCP-соединения (трехэтапное рукопожатие)
А) Клиент отправляет сегмент с флагом ACK для подтверждения получения SYN-ACK
Б) Сервер отправляет сегмент с флагами SYN и ACK, подтверждая запрос клиента
В) Клиент отправляет сегмент с флагом SYN, инициируя соединение
Г) Клиент и сервер переходят в состояние установленного соединения ESTABLISHED
3. Установите соответствие между уровнем модели OSI и его основной функцией

А) Физический уровень
Б) Канальный уровень
В) Сетевой уровень
Г) Транспортный уровень
1. Обеспечение сквозной доставки данных с управлением потоком и коррекцией ошибок
2. Передача битового потока по физической среде с кодированием сигналов
3. Маршрутизация пакетов в составной сети с выбором наилучшего пути
4. Управление диалогом между приложениями и синхронизация данных
5. Адресация на основе MAC-адресов, обнаружение и исправление ошибок в кадре
4. Установите соответствие между типом топологии сети и ее характеристикой
А) Шина
Б) Звезда
В) Кольцо
Г) Ячеистая
1. Все устройства соединены с центральным коммутационным узлом, отказ центра ведет к полной потере связи
2. Каждое устройство имеет отдельную связь с большинством других устройств, обеспечивая высокую отказоустойчивость
3. Все устройства подключены к общему кабелю, отказ кабеля приводит к остановке всей сети
4. Данные передаются последовательно от устройства к устройству по замкнутому контуру
5. Используется в беспроводных сетях с центральной точкой доступа

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
5. Установите правильную последовательность действий коммутатора при обработке кадра с неизвестным MAC-адресом назначения
А) Коммутатор добавляет исходный MAC-адрес и порт в свою таблицу MAC-адресов
Б) Коммутатор принимает кадр на входящем порту и проверяет его целостность
В) Коммутатор отправляет кадр на все порты, кроме входящего (flooding)
Г) Коммутатор проверяет таблицу MAC-адресов на наличие адреса назначения
6. Установите правильную последовательность действий маршрутизатора при обработке IP-пакета
А) Маршрутизатор проверяет TTL (Time to Live) в заголовке IP и уменьшает его значение
Б) Маршрутизатор получает IP-пакет на входящем интерфейсе
В) Маршрутизатор определяет исходящий интерфейс по таблице маршрутизации
Г) Маршрутизатор пересылает пакет на следующий узел (next hop) или в сеть назначения
7. Установите соответствие между протоколом или технологией и его назначением
А) ARP
Б) ICMP
В) DHCP
Г) NAT
1. Преобразование частных IP-адресов в публичные для выхода в Интернет
2. Определение MAC-адреса по известному IP-адресу в локальной сети
3. Автоматическое назначение IP-адресов и параметров сети клиентам
4. Обмен сообщениями об ошибках и диагностика сети (например, ping)
5. Шифрование трафика между двумя узлами в защищенном туннеле
8. Установите соответствие между прикладным протоколом и используемым транспортным портом
А) HTTP
Б) HTTPS
В) DNS
Г) FTP (управляющее соединение)
1. Порт 443
2. Порт 21
3. Порт 80
4. Порт 53
5. Порт 25
9. Установите соответствие между методом цифрового кодирования и его особенностью
А) NRZ
Б) Manchester
В) 4B/5B
Г) Кодирование с возвратом к нулю (RZ)
1. Каждый бит кодируется переходом уровня в середине битового интервала, что обеспечивает самосинхронизацию
2. Каждые 4 бита данных преобразуются в 5 битов для улучшения синхронизации и баланса постоянной составляющей
3. Уровень сигнала возвращается к нулю в середине каждого битового интервала
4. Логический ноль и единица кодируются разными уровнями напряжения, возможна потеря синхронизации при длинной серии одинаковых бит
5. Кодирование используется исключительно в оптоволоконных кабелях

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном

исполнении
10. Установите правильную последовательность обработки DNS-запроса при рекурсивном режиме
А) Локальный DNS-резолвер обращается к корневому DNS-серверу для получения информации о TLD-сервере
Б) DNS-резолвер получает IP-адрес от авторитативного сервера и возвращает его клиенту
В) DNS-резолвер обращается к авторитативному DNS-серверу для получения окончательного соответствия домена и IP-адреса
Г) Клиент отправляет DNS-запрос к локальному DNS-резолверу для разрешения доменного имени
11. Установите правильную последовательность этапов обработки пакета межсетевым экраном (stateful firewall) при установлении нового соединения
А) Межсетевой экран проверяет пакет на соответствие правилам безопасности и состоянию соединения
Б) Межсетевой экран получает первый пакет от внутреннего клиента к внешнему серверу
В) Межсетевой экран создает новую запись в таблице состояний для данного соединения
Г) Межсетевой экран разрешает прохождение пакета и запоминает параметры сессии (порты, адреса, номера последовательностей)
12. Установите правильную последовательность действий при восстановлении конфигурации сетевого устройства из резервной копии
А) Сетевой администратор подключается к устройству через консоль или SSH и загружает сохраненную конфигурацию
Б) Администратор выполняет резервное копирование текущей конфигурации на TFTP-сервер в штатном режиме
В) Администратор перезагружает устройство для применения загруженной конфигурации или копирует ее в startup-config
Г) Администратор проверяет работоспособность устройства и корректность примененных параметров
13. Установите соответствие между типом сетевого устройства и его уровнем функционирования в модели OSI
А) Коммутатор (свитч)
Б) Маршрутизатор
В) Хаб (концентратор)
Г) Межсетевой экран с прокси-функциями
1. Физический уровень
2. Канальный уровень
3. Сетевой уровень (и выше в случае stateful-инспекции)
4. Прикладной уровень (анализирует содержимое протоколов)
5. Сеансовый уровень
14. Установите соответствие между типом записи DNS и ее назначением
А) A
Б) CNAME
В) MX
Г) PTR
1. Сопоставление IP-адреса с доменным именем (обратное разрешение)
2. Сопоставление доменного имени с IPv4-адресом
3. Указание почтового сервера для домена
4. Создание псевдонима (алиаса) для другого доменного имени
5. Сопоставление доменного имени с IPv6-адресом
15. Установите соответствие между методом или механизмом VPN и его характеристикой
А) PPTP
Б) L2TP
В) IPSec в туннельном режиме
Г) IPSec в транспортном режиме
1. Шифруется только полезная нагрузка IP-пакета, исходный IP-заголовок остается открытым
2. Инкапсулируется весь исходный IP-пакет в новый IP-пакет с новым заголовком
3. Один из первых протоколов туннелирования, использует GRE для инкапсуляции, считается менее безопасным
4. Часто комбинируется с IPSec для обеспечения шифрования, работает поверх UDP
5. Протокол, обеспечивающий только сжатие данных без шифрования

Индикатор УМЕТЬ

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении
1. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. В стеке протоколов TCP/IP инкапсуляция данных происходит последовательно сверху вниз. Какой блок данных (PDU) формируется на сетевом уровне перед передачей на канальный уровень?
А) Сегмент
Б) Кадр
В) Дейтаграмма (пакет)
Г) Битовый поток
2. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. При передаче данных по локальной сети коммутатор получает кадр с MAC-адресом назначения, которого нет в его таблице MAC-адресов. Какое действие выполнит коммутатор?
А) Отбросит кадр и отправит уведомление об ошибке отправителю
Б) Сохранит кадр в буфере и запросит у всех устройств их MAC-адреса

В) Перешлет кадр на все свои порты, кроме порта, с которого кадр был получен
Г) Перенаправит кадр только на порт, подключенный к маршрутизатору
3. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. Администратор настраивает сеть с использованием частных IP-адресов согласно RFC 1918 и планирует организовать выход нескольких десятков компьютеров в Интернет через один публичный IP-адрес. Какой механизм трансляции адресов следует применить?
А) Static NAT с отдельным публичным адресом для каждого компьютера
Б) PAT (Port Address Translation) с перегрузкой портов
В) Динамический NAT без перегрузки портов
Г) Трансляция адресов только для исходящих ICMP-запросов

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
4. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. Протокол OSPF относится к протоколам состояния каналов и использует метрику, основанную на пропускной способности интерфейсов. Какое преимущество дает этот подход по сравнению с дистанционно-векторными протоколами типа RIP?
А) OSPF быстрее сходится и требует меньше вычислительных ресурсов процессора
Б) OSPF не использует широковещательные обновления и не подвержен петлям маршрутизации
В) OSPF использует только статические маршруты, что упрощает настройку
Г) OSPF передает полную таблицу маршрутизации каждые 30 секунд для обеспечения актуальности
5. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. При установлении TCP-соединения клиент отправляет сегмент с флагом SYN, сервер отвечает сегментом с флагами SYN и ACK, после чего клиент отправляет сегмент с флагом ACK. Что произойдет, если клиент не отправит третий сегмент с ACK в ответ на SYN-ACK?
А) Соединение будет считаться установленным, и сервер начнет передачу данных
Б) Сервер немедленно разорвет соединение и отправит RST-сегмент клиенту
В) Сервер повторно отправит SYN-ACK через определенный интервал времени до истечения таймаута
Г) Клиент автоматически получит IP-адрес от DHCP-сервера для завершения установки

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
6. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. На межсетевом экране настроены списки доступа (ACL) с правилами, которые обрабатываются сверху вниз. Входящий пакет соответствует первому правилу разрешения, но также подпадает под третье правило запрета. Какое решение примет межсетевой экран?
А) Пропустит пакет, так как первое совпавшее правило имеет приоритет над последующими
Б) Отбросит пакет, так как правило запрета является более строгим
В) Отправит пакет на анализ прокси-серверу для принятия окончательного решения
Г) Запросит подтверждение у администратора перед применением любого правила
7. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. При мониторинге сетевого оборудования с использованием протокола SNMP администратор настраивает систему оповещений о критических событиях, которые генерируются агентом без запроса со стороны менеджера. Как называется такой тип сообщений в SNMP?
А) GET-запрос
Б) SET-команда
В) Trap-сообщение
Г) Inform-уведомление с подтверждением

Индикатор ИМЕТЬ НАВЫКИ И (ИЛИ) ОПЫТ ДЕЯТЕЛЬНОСТИ

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении
1. Прочитайте текст и запишите развернутый ответ. В офисе компании установлена локальная сеть из 50 компьютеров, объединенных через один коммутатор. Администратор замечает, что при передаче больших файлов между компьютерами в одной подсети скорость падает, а широковещательный трафик создает избыточную нагрузку. Предложите способ решения проблемы с минимальными финансовыми затратами, объяснив, какое сетевое устройство и на каком уровне модели OSI следует добавить.
2. Прочитайте текст и запишите ответ. В сети используется IPv4-адрес 192.168.10.0 с маской подсети 255.255.255.240. Сколько хостов может быть подключено в каждой подсети (исключая сетевой и широковещательный адреса)? Разрешается использовать калькулятор.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
3. Прочитайте текст и запишите развернутый ответ. Системный администратор настраивает удаленный доступ к серверу видеонаблюдения из Интернета. Сервер имеет частный IP-адрес 192.168.1.10 и работает по протоколу RTSP на порту 554. Внешний интерфейс маршрутизатора имеет публичный IP-адрес 85.140.10.5. Опишите механизм, который необходимо настроить на маршрутизаторе, чтобы внешний клиент мог подключиться к серверу по адресу 85.140.10.5:5554. Укажите название технологии и перечислите параметры, которые требуется задать.
4. Прочитайте текст и запишите ответ. Администратор настроил статический NAT для сервера с внутренним адресом

10.0.1.5 на внешний адрес 203.0.113.10. Сколько уникальных внешних IP-адресов потребуется для одновременного доступа к этому серверу из внешней сети, если используется только статический NAT без PAT? Разрешается использовать калькулятор.
5. Прочитайте текст и запишите развернутый ответ. На предприятии произошел сбой электропитания, после перезагрузки сетевые устройства загрузились, но сотрудники из удаленного филиала не могут подключиться к центральному офису по VPN. При этом локальная сеть в центральном офисе работает исправно, пинг до внешнего шлюза проходит. Администратор проверил логи и обнаружил, что IPSec-туннель не установлен. Назовите две наиболее вероятные причины проблемы, связанные с конфигурацией, и предложите действия для их проверки.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
6. Прочитайте текст и запишите ответ. В сети работает DHCP-сервер с пулом адресов от 192.168.1.100 до 192.168.1.150 включительно. Какое максимальное количество клиентов может одновременно получить IP-адрес от этого сервера (исключая зарезервированные адреса)? Разрешается использовать калькулятор.
7. Прочитайте текст и запишите развернутый ответ. В сетевом журнале Syslog отмечены повторяющиеся сообщения об ошибке «Duplicate IP address detected» для устройства с MAC-адресом AA:BB:CC:11:22:33. Администратор знает, что в сети используется DHCP-сервер для автоматической раздачи адресов, но некоторые пользователи имеют статические настройки. Опишите последовательность действий администратора для поиска и устранения источника конфликта без отключения всего сегмента сети.
8. Прочитайте текст и запишите ответ. При настройке OSPF на интерфейсе маршрутизатора задана пропускная способность 100 Мбит/с. Метрика вычисляется как отношение опорной пропускной способности (100 000 000 бит/с) к текущей. Чему будет равна метрика для данного интерфейса? Разрешается использовать калькулятор.

ИТОГОВЫЙ ТЕСТ

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении
1. Какое утверждение о стеке протоколов TCP/IP и эталонной модели OSI является верным?
А) Уровень представления модели OSI отвечает за маршрутизацию пакетов в составной сети
Б) Канальный уровень модели OSI соответствует сетевому уровню стека TCP/IP
В) Прикладной уровень стека TCP/IP объединяет функции сеансового, представительского и прикладного уровней модели OSI
Г) Транспортный уровень модели OSI отсутствует в стеке TCP/IP
2. Какие характеристики соответствуют протоколу UDP по сравнению с TCP?
А) Гарантирует доставку данных с повторной передачей потерянных сегментов
Б) Не устанавливает предварительное логическое соединение перед передачей данных
В) Использует механизм скользящего окна для управления потоком
Г) Имеет упрощенный заголовок и подходит для потоковых мультимедийных приложений
3. Какие типы записей используются в системе доменных имен DNS?
А) Только записи A для сопоставления домена с IPv4-адресом
Б) Записи A, AAAA, CNAME, MX и другие
В) Только записи A и CNAME
Г) Записи CNAME и PTR, остальные не поддерживаются
4. Какие утверждения о работе протокола DHCP верны?
А) Процесс получения IP-адреса состоит из четырех этапов: Discover, Offer, Request, Acknowledge
Б) DHCP-сервер всегда назначает один и тот же IP-адрес клиенту на основе его MAC-адреса
В) Клиент отправляет широковещательный запрос DHCP Discover для обнаружения доступных серверов
Г) DHCP может предоставлять клиенту не только IP-адрес, но и маску подсети, адрес шлюза и DNS-серверов
5. Какое описание технологии NAT является корректным?
А) Static NAT выполняет сопоставление нескольких внутренних адресов с одним внешним адресом с использованием разных портов
Б) PAT (Port Address Translation) позволяет множеству устройств во внутренней сети использовать один публичный IP-адрес
В) DNAT изменяет исходный IP-адрес пакета при выходе из внутренней сети
Г) При использовании NAT таблица трансляции хранит соответствие между внутренним и внешним адресами (и портами)
6. Какие функции выполняет протокол IPSec в VPN-соединениях?
А) Протокол ESP обеспечивает шифрование полезной нагрузки и аутентификацию
Б) Протокол AH обеспечивает только аутентификацию и целостность, но не шифрование
В) Туннельный режим IPSec инкапсулирует весь исходный IP-пакет целиком
Г) IPSec использует только предварительные ключи и не поддерживает сертификаты

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
7. Какие алгоритмы шифрования и хеширования относятся к криптографическим методам защиты?
А) AES является симметричным блочным алгоритмом шифрования
Б) RSA относится к алгоритмам симметричного шифрования

В) SHA используется для вычисления хеш-кода и обеспечения целостности данных
Г) Алгоритм 3DES не применяется в современных протоколах безопасности
8. Какие виды межсетевых экранов (брандмауэров) существуют?
А) Пакетные фильтры, анализирующие только заголовки IP и TCP/UDP без учета состояния соединения
Б) Stateful-межсетевые экраны, отслеживающие состояние соединений и разрешающие обратные пакеты
В) Прокси-серверы, работающие на прикладном уровне и способные анализировать содержимое протоколов
Г) Все перечисленные виды межсетевых экранов являются программными и не реализуются аппаратно
9. Какие утверждения о протоколах маршрутизации RIP и OSPF верны?
А) RIP использует метрику на основе пропускной способности канала
Б) OSPF является протоколом состояния каналов и поддерживает иерархическую структуру с областями
В) RIP v2 поддерживает бесклассовую адресацию (CIDR) в отличие от RIP v1
Г) OSPF использует дистанционно-векторный алгоритм Беллмана-Форда
10. Какие особенности технологии Ethernet на канальном уровне являются правильными?
А) Коммутатор (свитч) строит таблицу MAC-адресов на основе анализа исходных MAC-адресов в кадрах
Б) Хаб (концентратор) передает кадр только на тот порт, к которому подключен адресат
В) Мост (bridge) уменьшает домен коллизий по сравнению с хабом
Г) Протокол STP используется для устранения петель на уровне L2 при наличии резервных связей
11. Какие утверждения о физической среде передачи данных верны?
А) Одномодовое оптоволокно обеспечивает большую дальность передачи, чем многомодовое
Б) Кабель UTP категории 5e поддерживает частоты до 100 МГц и используется в сетях Fast Ethernet
В) В беспроводных сетях затухание сигнала не зависит от расстояния и препятствий
Г) Коаксиальный кабель в современных локальных сетях используется чаще витой пары

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
12. Какие принципы адресации IPv4 являются корректными?
А) В классовой адресации адрес класса C имеет маску по умолчанию /24
Б) Широковещательный адрес подсети вычисляется путем установки всех бит хостовой части в единицу
В) Частные адреса, описанные в RFC 1918, не маршрутизируются в глобальной сети Интернет
Г) Адрес хоста в подсети получается путем установки всех бит хостовой части в ноль
13. Какие утверждения о сетевой аутентификации и протоколах AAA верны?
А) Протокол RADIUS использует UDP-транспорт и шифрует только пароль в пакете
Б) TACACS+ использует TCP-транспорт и шифрует весь пакет целиком
В) Протоколы RADIUS и TACACS+ выполняют только аутентификацию и не поддерживают авторизацию
Г) Многофакторная аутентификация требует использования двух и более независимых факторов
14. Какие методы мониторинга и диагностики сетей являются стандартными?
А) SNMP v3 обеспечивает шифрование и аутентификацию в отличие от предыдущих версий
Б) Syslog используется для централизованного сбора и хранения журналов событий
В) Утилита traceroute позволяет определить маршрут до узла и время прохождения пакетов
Г) Команда ping отправляет SNMP-запросы для проверки доступности устройства
15. Какие мероприятия относятся к техническому обслуживанию и восстановлению сети?
А) Ежедневное резервное копирование всей оперативной памяти коммутатора
Б) Сохранение running-config и startup-config на TFTP-сервер для архивации конфигураций
В) План аварийного восстановления описывает порядок действий при отказе основного оборудования
Г) Версионность конфигураций не требуется, если ведется журнал изменений вручную

Темы индивидуальных проектов, курсовых работ (проектов), индивидуальных заданий на практику:

Учебным планом не предусмотрено

Описание критериев оценивания успеваемости

НЕДОСТАТОЧНЫЙ УРОВЕНЬ Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	ПОРОГОВЫЙ УРОВЕНЬ Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.	ПРОДВИНУТЫЙ УРОВЕНЬ Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала; - способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной обоснованной позиции по обсуждаемым вопросам; - незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	ВЫСОКИЙ УРОВЕНЬ Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
Оценка «незачет», «неудовлетворительно»	Оценка «зачтено/удовлетворительно» ,«удовлетворительно»	Оценка «зачтено/хорошо», «хорошо»	Оценка «зачтено/отлично», «отлично»

ПК 1.2.: Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении

Недостаточный уровень:
Знает отдельные названия сетевых устройств (коммутатор, маршрутизатор, сетевой кабель), базовые понятия (IP -адрес, протокол, сеть), понимает назначение сети (обмен данными), а также знает 1-2 протокола (TCP, IP).

Умеет под руководством преподавателя выполнять обжим витой пары по образцу, подключать сетевые устройства по схеме, вводить IP-адрес в настройках ОС, запускать ping для проверки связи, а также устанавливать антивирус по инструкции и включать брандмауэр.

Имеет практический опыт создания нового пользователя в локальной системе под контролем, изменения пароля по инструкции, просмотра журнала событий по образцу, запуска резервного копирования по шаблону, а также включения антивирусной проверки по инструкции.

Пороговый уровень:
Знает теоретические основы компьютерных сетей (определение, классификация, топологии, среда передачи); аппаратные компоненты сетей (сетевые карты, коммутаторы, маршрутизаторы, точки доступа, модемы, повторители, мосты); сетевые модели (OSI – 7 уровней, TCP/IP – 4 уровня), их функции и взаимосвязь; основные сетевые протоколы (Ethernet, IP, TCP, UDP, HTTP, HTTPS, FTP, DNS, DHCP, ARP, ICMP); принципы адресации (MAC-адреса, IPv4-адреса (классы, маски подсети, CIDR), IPv6-адреса, порты, назначение адресов (статическая, динамическая DHCP), NAT).

Умеет самостоятельно организовывать простую локальную сеть (выбирать топологию, подключать коммутаторы и маршрутизаторы, назначать IP-адреса), выполнять монтаж сети (обжим кабеля, прокладка, маркировка), конфигурировать сетевое оборудование (коммутаторы, точки доступа), диагностировать типовые неисправности (ping, traceroute, проверка кабеля) и устранять их (замена кабеля, исправление IP-конфликта, перезагрузка), работать с сетевыми протоколами (настройка DHCP, DNS), конфигурировать и настраивать компоненты СЗИ (межсетевой экран, антивирус, контроль доступа), а также устанавливать, адаптировать и сопровождать типовое ПО СЗИ (лицензирование, обновление, настройка политик).

Имеет практический опыт администрирования автоматизированных систем в защищённом исполнении: создания, изменения и удаления учётных записей и групп (локальных и доменных), назначения прав доступа,

Имеет практический опыт администрирования автоматизированных систем в защищённом исполнении: создания, изменения и удаления учётных записей и групп (локальных и доменных), назначения прав доступа, настройки политик безопасности (парольной, блокировки, аудита), установки и обновления ПО и СЗИ, мониторинга событий безопасности (журналы, оповещения), резервного копирования и восстановления данных, а также применения нормативных требований к администрированию.

Продвинутый уровень:
Знает детальные характеристики аппаратных компонентов (производительность, буферы, таблицы маршрутизации), особенности работы протоколов (заголовки, флаги, поля), методы расчёта подсетей (маски переменной длины, VLSM), принципы маршрутизации (статическая, динамическая, RIP, OSPF, BGP), а также знает способы диагностики сетей на основе теоретических знаний.

Умеет самостоятельно организовывать и конфигурировать корпоративную сеть (VLAN, агрегация каналов, статическая и динамическая маршрутизация (RIP/OSPF)), производить монтаж и пусконаладку сети, осуществлять углублённую диагностику и устранение сложных неисправностей (анализ трафика, мониторинг SNMP, проверка журналов), настраивать сертифицированные СЗИ для требуемого класса защищённости, интегрировать СЗИ с сетевым оборудованием (VPN, фильтрация), а также адаптировать и сопровождать ПО СЗИ в рамках системы защиты информации (обновление политик, аудит).

Имеет практический опыт настройки мандатного контроля доступа (SELinux, AppArmor), централизованного управления защищёнными АС (групповые политики, системы управления конфигурациями), расследования инцидентов по журналам аудита, оптимизации производительности защищённых систем, интеграции СЗИ с SIEM-системами, а также планового обслуживания и обновления с учётом требований ФСТЭК.

Высокий уровень:
Знает современные сетевые технологии (SDN, NFV, VLAN, VPN, MPLS, беспроводные стандарты Wi-Fi 6/7), модели адресации в IPv6 (типы, префиксы), протоколы следующего поколения (QUIC, HTTP/3), архитектуру высоконагруженных сетей, а также методы оптимизации сетевых протоколов и адресации для различных сценариев.

Умеет самостоятельно проектировать и оптимизировать сетевую инфраструктуру (QoS, MPLS, SDN), внедрять современные методы диагностики и прогнозирования отказов, настраивать продвинутые протоколы (BGP, OSPF), конфигурировать комплексные СЗИ (EDR, NGFW, SIEM, DLP) и интегрировать их с сетью, автоматизировать установку, адаптацию и сопровождение ПО СЗИ (DevOps, CI/CD), а также обучать других организации, настройке, диагностике и сопровождению сетей и СЗИ.

Имеет практический опыт администрирования защищённых АС в распределённых и гетерогенных средах, внедрения современных платформ управления безопасностью (EDR, XDR, SOAR), автоматизации задач администрирования (DevSecOps, Ansible для защищённых систем), интерпретации нормативных требований для нестандартных конфигураций, а также обучения других администрированию защищённых автоматизированных систем.

ПК 1.3.: Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

Недостаточный уровень:
Знает отдельные названия средств защиты информации (СЗИ) для сетей (межсетевой экран, VPN, антивирус), понимает необходимость защиты сети, знает 1-2 этапа установки (подготовка, настройка), а также знает, что такое ввод в эксплуатацию (проверка работы).

Имеет практический опыт просмотра журнала событий антивируса по инструкции, ручного запуска обновления баз под контролем, проверки статуса активности брандмауэра по образцу, блокировки пользователя в простой системе контроля доступа по шаблону, а также сообщения о подозрительном событии.

Умеет под руководством преподавателя добавлять правило разрешения/запрета в простом межсетевом экране (например, Windows Firewall), проверять статус VPN-соединения (иконка), перезапускать службу СЗИ по инструкции, а также сообщать о неисправности (нет доступа) по образцу.

Пороговый уровень:
Имеет практический опыт эксплуатации компонентов СЗИ: мониторинга работоспособности (журналы, статус), обновления баз и версий ПО СЗИ (антивирус, брандмауэр, контроль доступа), управления учётными записями и правами, аудита событий безопасности, резервного копирования настроек и ключей, реагирования на типовые инциденты, а также формирования отчётности по эксплуатации.

Умеет самостоятельно настраивать программно-аппаратные СЗИ по заданным правилам (правила фильтрации для межсетевого экрана, политики VPN, настройки IDS/IPS, антивирусного шлюза), диагностировать типовые неисправности (проверка логов, тестирование правил, ping, traceroute, анализ трафика, проверка сертификатов), устранять неисправности (корректировка правил, перезапуск служб, обновление ПО, замена сертификатов, аппаратная перезагрузка), а также проверять работоспособность после устранения.

Знает порядок установки средств защиты информации в компьютерных сетях (планирование, подготовка оборудования и ПО, установка, конфигурирование, тестирование, ввод в эксплуатацию); требования к совместимости СЗИ с сетевым оборудованием и ОС; этапы настройки различных типов СЗИ (межсетевые экраны, системы обнаружения вторжений (IDS/IPS), VPN-шлюзы, антивирусная защита сетевого уровня, средства фильтрации контента, DLP-системы на сетевом уровне); методы проверки работоспособности СЗИ перед вводом в эксплуатацию; а также документальное оформление ввода в эксплуатацию (акты, протоколы,

Знает порядок установки средств защиты информации в компьютерных сетях (планирование, подготовка оборудования и ПО, установка, конфигурирование, тестирование, ввод в эксплуатацию); требования к совместимости СЗИ с сетевым оборудованием и ОС; этапы настройки различных типов СЗИ (межсетевые экраны, системы обнаружения вторжений (IDS/IPS), VPN-шлюзы, антивирусная защита сетевого уровня, средства фильтрации контента, DLP-системы на сетевом уровне); методы проверки работоспособности СЗИ перед вводом в эксплуатацию; а также документальное оформление ввода в эксплуатацию (акты, протоколы, отчёты).

Продвинутый уровень:
Умеет самостоятельно настраивать СЗИ для сложных сетевых архитектур (сегментированные сети, удалённые филиалы, виртуальные среды), проводить углублённую диагностику (анализ дампов трафика, SNMP-мониторинг, корреляция событий), устранять сложные неисправности (восстановление конфигурации после сбоя, восстановление туннелей, разрешение конфликтов правил), а также оптимизировать настройки под требования производительности и безопасности.

Знает детальные инструкции по установке сертифицированных СЗИ для различных сетевых архитектур (корпоративная сеть, сегментированная, с удалёнными филиалами), особенности установки в виртуальной среде и облачных платформах, способы тестирования эффективности СЗИ (пентесты, нагрузочное тестирование), а также требования нормативных документов (ФСТЭК) к вводу в эксплуатацию СЗИ в защищённых сетях.

Имеет практический опыт эксплуатации СЗИ в различных классах защищённости, использования централизованных консолей управления и SIEM для мониторинга, расследования инцидентов на основе данных СЗИ, оптимизации производительности СЗИ при эксплуатации, а также применения требований нормативных документов (ФСТЭК) в процессе эксплуатации.

Высокий уровень:
Умеет самостоятельно настраивать и оптимизировать СЗИ в динамических сетях (SDN, облака), внедрять автоматизированную диагностику и самовосстановление (скрипты, AI/ML), разрабатывать стратегии предотвращения неисправностей и обеспечения отказоустойчивости, проводить анализ профилей угроз для адаптации настроек, а также обучать других настройке и диагностике СЗИ.

Имеет практический опыт эксплуатации комплексных СЗИ в гетерогенных и распределённых АС (EDR, XDR, SOAR), автоматизации задач эксплуатации (скрипты, автообновление, автореагирование), анализа эффективности СЗИ и разработки мер по повышению надёжности, управления жизненным циклом СЗИ, а также обучения других эксплуатации компонентов СЗИ.

Знает методологию интеграции СЗИ в комплексные системы безопасности сетей (SIEM, SOAR, NGFW с функцией IPS), современные подходы к автоматизации установки и развёртывания СЗИ (DevSecOps, Infrastructure as Code), требования к вводу в эксплуатацию СЗИ для объектов КИИ и государственных информационных систем, а также способы оценки экономической эффективности внедрения СЗИ.

ПК 1.4.: Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении

Недостаточный уровень:
Знает отдельные понятия (техническое обслуживание, профилактика, диагностика), может назвать 1-2 вида обслуживания (ежедневное, плановое), понимает важность чистки и проверки оборудования, знает, что нужно удалять пыль и проверять соединения.

Умеет под руководством преподавателя выполнять перезагрузку компьютера, проверять подключение кабелей, запускать встроенную диагностику (POST), интерпретировать звуковые сигналы BIOS по таблице, а также заменять простой расходный материал (батарейка CMOS, кабель).

Имеет практический опыт просмотра журнала событий антивируса по инструкции, перезапуска службы СЗИ под контролем, проверки статуса лицензии по образцу, а также выполнения восстановления конфигурации из резервной копии по шаблону.

Пороговый уровень:
Знает принципы основных методов организации и проведения технического обслуживания (ТО) вычислительной техники и технических средств информатизации: виды ТО (ежедневное, планово-предупредительное (ППР), сезонное, обслуживание по состоянию, по регламенту); методы ТО (профилактический, диагностический, восстановительный, ремонтный); порядок организации ТО (планирование, подготовка, выполнение, учёт, контроль); основные регламентные работы (чистка от пыли, проверка систем охлаждения, диагностика компонентов (процессор, память, диск, блок питания), проверка электропитания, заземления, обновление ПО и прошивок, тестирование работоспособности, замена расходных материалов); а также правила техники безопасности при проведении ТО.

Имеет практический опыт диагностики компонентов СЗИ (журналы, тестирование, целостность, обновления, политики), устранения типовых отказов (перезапуск служб, восстановление конфигураций, переустановка, корректировка политик, замена сертификатов/лицензий, откат обновлений), а также восстановления работоспособности АС в защищённом исполнении (восстановление из резервной копии, проверка целостности, аудит, документирование) с соблюдением требований нормативных документов.

Умеет самостоятельно обеспечивать работоспособность технических средств (профилактика, мониторинг температуры и SMART), обнаруживать неисправности (визуальный осмотр, анализ журналов событий, запуск

Умеет самостоятельно обеспечивать работоспособность технических средств (профилактика, мониторинг температуры и SMART), обнаруживать неисправности (визуальный осмотр, анализ журналов событий, запуск диагностических утилит (memtest, проверка диска, тест стабильности)), устранять типовые неисправности (перезагрузка, замена кабелей, переустановка драйверов, замена компонентов (блок питания, память, диск, кулер), восстановление ПО, настройка BIOS, обновление драйверов и прошивок), а также проверять работоспособность после устранения и вести документацию.

Продвинутый уровень:
Имеет практический опыт углублённой диагностики для различных типов СЗИ (СКЗИ, DLP, IDS/IPS, EDR, SIEM), устранения сложных отказов (восстановление базы данных политик, синхронизация ключей, устранение конфликтов с системными обновлениями, восстановление криптоконтейнеров), а также восстановления работоспособности АС в защищённом исполнении после инцидентов (компрометация, атака) с применением мер форензики.

Знает детальные методики ППР для различных типов оборудования (серверы, рабочие станции, сетевое оборудование, СХД, периферия), методы прогнозирования отказов на основе мониторинга (температура, SMART, частота ошибок), способы организации ТО в критических инфраструктурах (горячая замена, резервирование), а также требования нормативных документов к периодичности и объёму ТО (ГОСТ, ведомственные нормы).

Умеет самостоятельно проводить углублённую диагностику для серверов, СХД и сетевого оборудования (анализ логов SMART, ECC, журналов RAID), прогнозировать отказы на основе данных мониторинга, устранять сложные неисправности (восстановление BIOS, перепрошивка контроллеров, замена компонентов на материнской плате (конденсаторы, MOSFET), восстановление RAID-массивов), а также применять методы горячей замены и резервирования для обеспечения работоспособности в критических инфраструктурах.

Высокий уровень:
Знает методологию оптимизации системы ТО на основе анализа надёжности и экономической эффективности, современные подходы к автоматизации ТО (мониторинг, удалённая диагностика, предиктивная аналитика), принципы построения систем управления ТО (CMMS, ITIL), а также стратегии технического обслуживания для высокодоступных и территориально распределённых систем.

Умеет самостоятельно внедрять предиктивную диагностику (AI/ML, анализ больших данных), автоматизировать обнаружение и устранение неисправностей (скрипты, откат, переключение на резерв), проектировать стратегии обеспечения работоспособности для распределённых и высоконагруженных систем, проводить анализ корневых причин отказов, а также обучать других методам обеспечения работоспособности, обнаружения и устранения неисправностей.

Имеет практический опыт внедрения автоматизированной диагностики и самовосстановления СЗИ (DevSecOps, AI/ML), проектирования стратегий обеспечения отказоустойчивости и непрерывности защищённых АС, анализа корневых причин сложных отказов, восстановления систем после APT-атак, а также обучения других диагностике, устранению отказов и восстановлению защищённых АС.

Перечень практических навыков, приобретаемых при изучении дисциплины:

ПК 1.1: Иметь навыки установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2: Иметь навыки администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3: Иметь навыки обеспечения бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4: Иметь навыки и опыт деятельности по проверке технического состояния, техническому обслуживанию, текущему ремонту, устранению отказов и восстановлению работоспособности автоматизированных (информационных) систем в защищенном исполнении.

Методы оценки	Критерии оценки
Экспертное наблюдение за решением обучающимися проблемно-ситуационных задач в рамках практической подготовки	Оценка «отлично» – задание выполнено полностью, в рамках регламента, установленного на публичную презентацию, студент(ы) приводит (подготовили) полную четкую аргументацию выбранного решения на основе качественно сделанного анализа задания. Демонстрируются хорошие теоретические знания, имеется собственная обоснованная точка зрения на проблему(ы) и причины ее (их) возникновения. В случае ряда выявленных проблем четко определяет их иерархию. При устной презентации уверенно и быстро отвечает на заданные вопросы, выступление сопровождается приемами визуализации. В случае письменного отчета-презентации по выполнению кейс-задания сделан структурированный и детализированный анализ, представлены возможные варианты решения (3-5), четко и аргументировано обоснован окончательный выбор одного из альтернативных решений. Оценка «хорошо» – задание выполнено полностью, но в рамках установленного на выступление регламента, студент(ы) не приводит (не подготовили) полную четкую аргументацию выбранного решения. Имеет место излишнее теоретизирование, или наоборот, теоретическое обоснование ограничено, имеется собственная точка зрения на проблемы, но не все причины ее возникновения установлены. При устной презентации на дополнительные вопросы выступающий отвечает с некоторым затруднением, подготовленная устная презентации выполненного задания не очень структурирована. При письменном отчете-презентации по выполнению задания сделан неполный анализ, без учета ряда фактов, выявлены не все возможные проблемы, для решения могла быть выбрана второстепенная, а

	не главная проблема, количество представленных возможных вариантов решения – 2-3, затруднена четкая аргументация окончательного выбора одного из альтернативных решений. Оценка «удовлетворительно» – задание выполнено более чем на 2/3, но в рамках установленного на выступление регламента, студент(ы) расплывчато раскрывает решение, не может четко аргументировать сделанный выбор, показывает явный недостаток теоретических знаний. Выводы слабые, свидетельствуют о недостаточном анализе фактов, в основе решения может иметь место интерпретация фактов или предположения, собственная точка зрения на причины возникновения проблемы не обоснована или отсутствует. При устной презентации на вопросы отвечает с трудом или не отвечает совсем. Подготовленная презентация выполненного задания не структурирована. В случае письменной презентации по выполнению кейсзадания не сделан детальный анализ, далеко не все факты учтены, для решения выбрана второстепенная, а не главная проблема, количество представленных возможных вариантов решения – 1-2, отсутствует четкая аргументация окончательного выбора решения. Оценка «неудовлетворительно» – задание не выполнено, или выполнено менее чем на треть. Отсутствует детализация при анализе задания, изложение устное или письменное не структурировано. Если решение и обозначено в выступлении или отчете-презентации, то оно не является решением проблемы, которая заложена в задании.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Рекомендуемая литература

5.1.1. Основная литература

Л.1.1	Акмаров П. Б. Компьютерные сети. Лабораторный практикум [Электронный ресурс]:учебное пособие для вузов. - Санкт-Петербург: Лань, 2024. - 120 с. – Режим доступа: https://e.lanbook.com/book/362876
Л.1.2	Тарасов И. Е. Вычислительные машины, комплексы и компьютерные сети [Электронный ресурс]:учебно-методическое пособие. - Москва: РТУ МИРЭА, 2021. - 89 с. – Режим доступа: https://e.lanbook.com/book/176541
Л.1.3	Акмаров П. Б. Компьютерные сети. Лабораторный практикум [Электронный ресурс]:учебное пособие для спо. - Санкт-Петербург: Лань, 2024. - 120 с. – Режим доступа: https://e.lanbook.com/book/362873

5.1.2. Дополнительная литература

Л.2.1	Вотинов М. В. Вычислительные машины, системы и компьютерные сети [Электронный ресурс]:. - Мурманск: МГТУ, 2018. - 156 с. – Режим доступа: https://e.lanbook.com/book/142639
Л.2.2	Гаврилова Т. И. Компьютерные сети и телекоммуникационные системы [Электронный ресурс]:конспект лекций для студ.подготовки 40.03.01. - Нижний Новгород: ВГУВТ, 2018. - 48 с. – Режим доступа: https://e.lanbook.com/book/130695

5.2. Перечень программного обеспечения

Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition

5.3. Перечень информационных справочных систем

Электронно-библиотечная система "Лань"
Электронно-библиотечная система "Университетская библиотека онлайн"
ПЛАТФОРМА ОНЛАЙН-ОБРАЗОВАНИЯ «РАЗУМ»

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1312 - Лаборатория
Учебная аудитория для проведения занятий лекционного типа, лабораторных и практических занятий; занятий семинарского типа; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Маркерная доска; 15 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Учебно-наглядные пособия

Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1302 - Лаборатория
Учебная аудитория для проведения занятий лекционного типа; занятий семинарского типа, лабораторных и практических занятий; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочее место преподавателя; маркерная доска; 10 рабочих мест обучающихся, оснащенных ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду;

Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1310 - Лаборатория Учебная аудитория для проведения занятий лекционного типа; занятий семинарского типа, лабораторных и практических занятий; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Классная доска; 15 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Ноутбук переносной; Переносной проектор; Переносной экран; Учебно-наглядные пособия

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Методические рекомендации по организации самостоятельной работы

СРС – планируемая учебная, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (возможно частичное непосредственное участие преподавателя при сохранении ведущей роли студентов). Целью СРС является овладение фундаментальными знаниями, профессиональными умениями и навыками по профилю будущей специальности, опытом творческой, исследовательской деятельности, развитие самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровней. Задачи СРС: систематизация и закрепление полученных теоретических знаний и практических умений студентов; углубление и расширение теоретической подготовки; формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу; развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности; формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации; развитие исследовательских умений; использование материала, собранного и полученного в ходе самостоятельных занятий на практических занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к текущей и промежуточной аттестации. Функции СРС: развивающая (повышение культуры умственного труда, приобщение к 10 творческим видам деятельности, обогащение интеллектуальных способностей студентов); информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится мало результативной); ориентирующая и стимулирующая (процессу обучения придается ускорение и мотивация); воспитательная (формируются и развиваются профессиональные качества специалиста и гражданина); исследовательская (новый уровень профессионально-творческого мышления).

Самостоятельная работа студентов является обязательным компонентом учебного процесса для каждого студента и определяется учебным планом. Самостоятельная работа определяется как индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства педагога, но по его заданиям и под его контролем. Самостоятельная работа – это познавательная учебная деятельность, когда последовательность мышления студента, его умственных и практических операций и действий зависит и определяется самим студентом.

Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня, что в итоге приводит к развитию навыка самостоятельного планирования и реализации деятельности. Целью самостоятельной работы студентов является овладение необходимыми компетенциями по своему направлению подготовки, опытом творческой и исследовательской деятельности. На основании компетентностного подхода к реализации профессиональных образовательных программ, видами заданий для самостоятельной работы являются:

- для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы), составление плана текста, графическое изображение структуры текста, конспектирование текста, выписки из текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа, использование аудио- и видеозаписей, компьютерной техники и информационно-телекоммуникационной сети Интернет и др.
- для закрепления и систематизации знаний: работа с конспектом лекции, обработка текста (учебника, первоисточника, дополнительной литературы, аудио и видеозаписей), повторная работа над учебным материалом, составление плана, составление таблиц для систематизации учебного материала, ответ на контрольные вопросы, заполнение рабочей тетради, аналитическая обработка текста (аннотирование, рецензирование, реферирование, конспект-анализ и др.), завершение аудиторных практических работ и оформление отчётов по ним, подготовка мультимедиа сообщений/докладов к выступлению на семинаре (конференции), материалов-презентаций, подготовка реферата, составление библиографии, тематических кроссвордов, тестирование и др.
- для формирования умений: решение задач и упражнений по образцу, решение вариативных задач, выполнение чертежей, схем, выполнение расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, рефлексивный анализ профессиональных умений с использованием аудио- и видеотехники и др.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Методические рекомендации по освоению дисциплины (учебного предмета)

Методические рекомендации по подготовке к лекционным занятиям

Просмотрите конспект сразу после занятий. Пометьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю. Каждую неделю рекомендуется отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.

Работа с рекомендованной литературой:

При работе с основной и дополнительной литературой целесообразно придерживаться такой последовательности.

Сначала прочитать весь заданный текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом материале, понять общий смысл прочитанного. Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом. Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать. План – это схема прочитанного материала, перечень вопросов, отражающих структуру и последовательность материала. Конспект – это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов:
- план-конспект – это развернутый детализированный план, в котором по наиболее сложным вопросам даются подробные пояснения,
- текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника,
- свободный конспект – это четко и кратко изложенные основные положения в результате глубокого изучения материала, могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом,
- тематический конспект – составляется на основе изучения ряда источников и дает ответ по изучаемому вопросу. В процессе изучения материала источника и составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную структуру конспекта. Это делает конспект легко воспринимаемым и удобным для работы.

Методические рекомендации по подготовке к практическим занятиям

Практические занятия представляют особую форму сочетания теории и практики. Их назначение – углубление проработки теоретического материала предмета путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к практическим занятиям включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение практического занятия предполагает, например:
 индивидуальные выступления студентов с сообщениями по какому-либо вопросу изучаемой темы;
 фронтальное обсуждение рассматриваемой проблемы, обобщения и выводы;
 решение задач и упражнений по образцу;
 решение вариантных задач и упражнений;
 решение ситуационных производственных (профессиональных) задач;
 проектирование и моделирование разных видов и компонентов профессиональной деятельности.
 выполнение контрольных работ;
 работу с тестами.
При подготовке к практическим занятиям студентам рекомендуется: внимательно ознакомиться с тематикой практического занятия; прочесть конспект лекции по теме, изучить рекомендованную литературу;
составить краткий план ответа на каждый вопрос практического занятия; проверить свои знания, отвечая на вопросы для самопроверки; если встретятся незнакомые термины, обязательно обратиться к словарю и зафиксировать их в тетради. Все письменные задания выполнять в рабочей тетради. Практические занятия развивают у студентов навыки самостоятельной работы по решению конкретных задач.

Методические рекомендации по подготовке к лабораторным работам

Лабораторные работы представляют одну из форм освоения теоретического материала с одновременным формированием практических навыков в изучаемой дисциплине. Их назначение – углубление проработки теоретического материала, формирование практических навыков путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к лабораторным работам включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение лабораторной работы предполагает:
 изучение теоретического материала по теме лабораторной работы (по вопросам изучаемой темы);
 выполнение необходимых расчетов и экспериментов;
 оформление отчета с заполнением необходимых таблиц, построением графиков, подготовкой выводов по проделанным экспериментам и теоретическим расчетам;
 по каждой лабораторной работе проводится контроль: проверяется содержание отчета, проверяется усвоение теоретического материала. Контроль усвоения теоретического материала является индивидуальным.

Методические указания по выполнению отчёта к лабораторным работам

Основным требованием по выполнению лабораторных и практических работ является полное исчерпывающее описание всей проделанной работы, позволяющее судить о полученных результатах, степени выполнения и профессиональной подготовки студентов.
Методические указания обеспечивают комплексный подход в учебной работе студентов, единство и преемственность требований к оформлению результатов работы на разных этапах обучения. С единых позиций приведены основные требования по структуре, оформлению и содержанию отчета по лабораторным и практическим работам.
Структура отчёта:
- цель работы;
- краткие теоретические сведения;
- ход выполнения работы;
- выводы.

Дополнительными элементы:
- приложения;
- библиографический список.
Требования к содержанию отчёта:
1. Титульный лист
В верхнем поле листа указывают полное наименование учебного заведения.
В среднем поле указывается вид работы, в данном случае лабораторная или практическая работа с указанием курса, по которому она выполнена, и ниже ее название. Название работы приводится без слова тема и в кавычки не заключается.
Далее ближе к правому краю титульного листа указывают фамилию, инициалы и группу учащегося, выполнившего работу, а также фамилию, инициалы преподавателя, принявшего работу.
В нижнем поле листа указывается место выполнения работы и год ее написания (без слова год).
2. Цель работы должна отражать тему работы, а также конкретные задачи, поставленные студенту на период выполнения работы. По объему цель работы в зависимости от сложности и многозадачности работы составляет от нескольких строк до 0,5 страницы.
3. Краткие теоретические сведения. В этом разделе излагается краткое теоретическое описание изучаемой в работе темы. Материал раздела не должен копировать содержание методического пособия или учебника по данной теме, а ограничивается изложением основных понятий, требующихся для дальнейшей обработки полученных результатов. Объем литературного обзора не должен превышать 1/3 части всего отчета.
4. Ход выполнения работы. В данном разделе подробно излагается методика выполнения работы, процесс получения данных и способ их обработки. Если используются стандартные пакеты компьютерных программ для обработки экспериментальных результатов, то необходимо обосновать возможность и целесообразность их применения, а также подробности обработки данных с их помощью.
5. Выводы по работе - кратко излагаются результаты работы, полученные в результате выполнения работы, а также краткий анализ полученных результатов.
Для защиты лабораторной работы студент должен подготовить отчет, провести самостоятельную работу, иметь отметку о проверенном отчете.
Результаты определяются по пятибалльной системе оценок.

Методические рекомендации по выполнению реферата

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы. Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора. Функции реферата. Информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и для каких целей их использует. Требования к языку реферата.
Должен отличаться точностью, краткостью, ясностью и простотой.
Структура реферата:
1. Титульный лист
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных. Общие требования к построению, содержанию и оформлению».
При проверке реферата оцениваются:
- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.

Методические рекомендации по устному опросу/самоподготовке

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, используя лист опорных сигналов, воспроизвести по памяти определения, выводы формул, формулировки основных положений и доказательств. В случае необходимости следует рекомендовать еще раз внимательно разобраться в материале. Иногда недостаточность

усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение решать задачи или пройти тестирование по пройденному материалу. Однако преподавателю следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

Методические рекомендации по подготовке к семинарским занятиям

Одним из видов внеаудиторной самостоятельной работы является подготовка к семинарским занятиям. Семинар – форма учебно-практических занятий, при которой студенты обсуждают сообщения, доклады и рефераты, выполненные ими по результатам учебных или научных исследований под руководством преподавателя. Преподаватель в этом случае является координатором обсуждений темы семинара, подготовка к которому является обязательной. Поэтому тема семинара и основные источники обсуждения предъявляются до обсуждения для детального ознакомления, изучения. Цели обсуждений направлены на формирование навыков профессиональной полемики и закрепление обсуждаемого материала. Семинар – это такая форма организации обучения, при которой на этапе подготовки доминирует самостоятельная работа учащихся с
учебной литературой и другими дидактическими средствами над серией вопросов, проблем и задач, а в процессе семинара идут активное обсуждение, дискуссии и выступления учащихся, где они под руководством преподавателя делают обобщающие выводы и заключения. Семинар предназначен для углубленного изучения дисциплины, овладения методологией научного познания, то главная цель семинарских занятий – обеспечить студентам возможность овладеть навыками и умениями использования теоретического знания применительно к особенностям изучаемой отрасли.

Методические рекомендации по подготовке эссе

Одним из видов самостоятельной работы студентов является написание творческой работы по заданной либо согласованной с преподавателем теме. Творческая работа (эссе) представляет собой оригинальное произведение объемом 500-700 слов, посвященное какой-либо значимой классической либо современной проблеме в определенной теоретической и практической области. Творческая работа не является рефератом и не должна носить описательный характер, большое место в ней должно быть уделено аргументированному представлению своей точки зрения студентами, критической оценке рассматриваемого материала и проблематики, что должно способствовать раскрытию творческих и аналитических способностей. Цели написания эссе – научиться логически верно и аргументировано строить устную и письменную речь;
работать над углублением и систематизацией своих философских знаний; овладеть способностью использовать основы знаний для формирования мировоззренческой позиции. Приступая к написанию эссе, изложите в одном предложении, что именно вы будете утверждать и доказывать (свой тезис).

Методические рекомендации по подготовке к докладу

Для подготовки доклада необходимо выбрать актуальную тему. Желательно, чтобы тема была интересна докладчику и вызывала желание качественно подготовить материалы. Подготовка доклада предполагает: определение цели доклада; подбор необходимого материала, определяющего содержание доклада; составление плана доклада, распределение собранного материала в необходимой логической последовательности.
Композиция доклада имеет вступление, основную часть и заключение.
Вступление должно содержать: название доклада; сообщение основной идеи; современную оценку предмета изложения; краткое перечисление рассматриваемых вопросов; интересную для слушателей форму изложения. Основная часть, в которой необходимо раскрыть суть темы, обычно строится по принципу отчёта. Задача основной части: представить достаточно данных для того, чтобы слушатели заинтересовались темой.
Заключение – чёткое обобщение и краткие выводы по излагаемой теме.

Методические рекомендации по подготовке к собеседованию

Собеседование – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.
Цель собеседования: проверка усвоения знаний; умений применять знания; сформированности профессионально значимых личностных качеств.
Подготовка к собеседованию предполагает повторение пройденного материала и приобретение навыка свободного владения терминологией и фактическими данными по определенному разделу дисциплины.

Методические рекомендации по подготовке к тестированию/ итоговому тестированию

Тестирование/итоговое тестирование – это система стандартизированных заданий, определенного содержания и упорядоченных в рамках определенной стратегии предъявления, позволяющая качественно оценить структуру и эффективно измерить уровень знаний, умений и навыков по учебной дисциплине (разделу). Тестирование/итоговое тестирование позволяет оценить у студентов уровень знаний фактического материала, умения логически мыслить, способности к рефлексии и творческому подходу к решению поставленной задачи на каждом этапе их обучения.
При самостоятельной подготовке к тестированию/итоговому тестированию студенту необходимо:
- четко выяснить все условия тестирования/итогового тестирования заранее (сколько тестов будет предложено, сколько времени отводится на тестирование/итоговое тестирование, какова система оценки результатов);
- проконсультироваться с преподавателем по вопросу выбора учебной литературы;
- проработать информационный материал по разделу дисциплине;
- конспективно выписать из соответствующих разделов учебной дисциплины основные понятия, ключевые идеи,

теоретические концепции и подходы;
- повторить теоретический материал лекций, самостоятельно изученной учебной и научной литературы, семинарских занятий.
При выполнении тестовых заданий рекомендуется:
- внимательно полностью прочитать вопрос и предлагаемые варианты ответов, выбрать правильные из них (их может быть несколько);
- при затруднении при ответе на сложный для студента вопрос целесообразно переходить к другим вопросам теста. По завершению ответов на все последующие вопросы теста необходимо вернуться к трудному вопросу и дать на него продуманный ответ;
- по окончании тестирования/итогового тестирования следует проверить правильность данных ответов на вопросы теста, чтобы избежать механических ошибок.

Методические рекомендации по подготовке к экзамену

Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине. Экзаменационная сессия – это серия экзаменов, установленных учебным планом. Между экзаменами интервал 2-4 дня, в течение студент систематизирует уже имеющиеся знания. На консультации перед экзаменом студенты должны
быть ознакомлены с основными требованиями и получить ответы на возникающие в процессе подготовки вопросы. Необходимо ориентировать студентов на систематическую подготовку к занятиям в течение семестра, что позволит использовать время экзаменационной сессии для систематизации знаний.

Методические рекомендации по подготовке к зачету/ зачету с оценкой

В ходе подготовки к зачету/зачету с оценкой студент, в первую очередь, должен систематизировать знания, полученные в ходе изучения дисциплины. К зачету/зачету с оценкой необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомьтесь со следующей учебно- методической документацией:
- программой дисциплины;
- перечнем знаний, умений и навыков, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- учебниками, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету/зачету с оценкой.
После этого у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и лабораторных занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета/зачета с оценкой.

Методические рекомендации по выполнению курсовой работы/ курсового проекта

Курсовая работа/курсовой проект - это учебно-исследовательский труд студента, выполняемый по определённой дисциплине под руководством научного руководителя. Её цель - закрепить и углубить теоретические знания, развить навыки самостоятельного анализа, работы с научной литературой и эмпирическими данными, а также сформировать умения структурировать информацию и формулировать обоснованные выводы.
Курсовая работа/курсовой проект – письменная работа объемом 30–50 страниц, выполняется в несколько этапов:
1. Подготовительный этап
2. Сбор и анализ информации
3. Написание работы
Структура курсовой работы/курсового проекта:
1. Титульный лист – по шаблону вуза.
2. Содержание – разделы с номерами страниц.
3. Введение: актуальность, цель, задачи, объект, предмет, методы, значимость, структура.
4. Основная часть:
o Глава 1 (теоретическая) – анализ концепций, выводы.
o Глава 2 (аналитическая/практическая) – анализ объекта, расчёты, данные, выводы.
o Глава 3 (рекомендательная, если нужно) – предложения, прогнозы, выводы.
5. Заключение – выводы по задачам, итоги, перспективы.
6. Список литературы – группируйте по типам, оформляйте по ГОСТ, указывайте только использованные источники.
7. Приложения (если нужно) – таблицы, графики, анкеты и т. д. (нумеруются, есть ссылки в тексте).
4. Оформление
5. Проверка и доработка
6. Подготовка к защите
• Доклад (5–7 мин.):
• Презентация.

Методические рекомендации по подготовке к зачету/ зачету с оценкой

В ходе подготовки к зачету/зачету с оценкой студент, в первую очередь, должен систематизировать знания, полученные в ходе изучения дисциплины. К зачету/зачету с оценкой необходимо готовиться целенаправленно, регулярно,

систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомьтесь со следующей учебно- методической документацией:
- программой дисциплины;
- перечнем знаний, умений и навыков, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- учебниками, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету/зачету с оценкой.
После этого у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и лабораторных занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета/зачета с оценкой.

8. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.
Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка учебных материалов производится с учетом индивидуальных особенностей.
Предусмотрена возможность обучения по индивидуальному графику, при составлении которого возможны различные варианты проведения занятий: в академической группе и индивидуально, на дому с использованием дистанционных образовательных технологий.
Основной формой в дистанционном обучении является индивидуальная форма обучения. Главным достоинством индивидуального обучения для инвалидов и лиц с ограниченными возможностями здоровья является то, что оно позволяет полностью индивидуализировать содержание, методы и темпы учебной деятельности инвалида, следить за каждым его действием и операцией при решении конкретных задач; вносить вовремя необходимые коррекции как в деятельность студента-инвалида, так и в деятельность преподавателя. Дистанционное обучение также обеспечивает возможности коммуникаций не только с преподавателем, но и с другими обучаемыми, сотрудничество в процессе познавательной деятельности.
При изучении дисциплины используются следующие организационные мероприятия:

- использование возможностей сети «Интернет» для обеспечения связи с обучающимися, предоставления им необходимых материалов для самостоятельного изучения, контроля текущей успеваемости и проведения тестирования;

- проведение видеоконференций, лекций, консультаций, и т.д. с использованием программ, обеспечивающих дистанционный контакт с обучающимся в режиме реального времени.
- предоставление электронных учебных пособий, включающих в себя основной материал по дисциплинам, включенным в ОП;

- проведение занятий, консультаций, защит курсовых работ и т.д. на базе консультационных пунктов, обеспечивающих условия для доступа туда лицам с ограниченными возможностями;
- предоставление видеолекций, позволяющих изучать материал курса дистанционно.
- использование программного обеспечения и технических средств, имеющих функции адаптации для использования лицами с ограниченными возможностями.

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2026 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2027 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2028 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2029 г. № __
Председатель ПЦК _____

==========