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.01.05 Эксплуатация компьютерных сетей

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 **266 часов**

Часов по учебному плану 266

в том числе:

контактная работа 234

самостоятельная работа 32

Виды контроля в семестрах:

Контрольная работа - 6,7,8

**Распределение часов дисциплины по семестрам**

| Вид учебной работы | Трудоемкость, часов | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **семестр 6** | | **семестр 7** | | **семестр 8** | | Итого | |
| | УП | РП | УП | РП | УП | РП | УП | РП |
| Лекции | 38 | 38 | 20 | 20 | 42 | 42 | 100 | 100 |
| Лабораторные | 18 | 18 | 20 | 20 | 28 | 28 | 66 | 66 |
| Практические | 20 | 20 | 20 | 20 | 28 | 28 | 68 | 68 |
| В т.ч. в форме практ. подгот. | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Контактная работа | 76 | 76 | 60 | 60 | 98 | 98 | 234 | 234 |
| Сам. работа | 4 | 4 | 10 | 10 | 18 | 18 | 32 | 32 |
| 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 Гришкова Майя Фёдоровна _____

Рабочая программа дисциплины

**Эксплуатация компьютерных сетей**

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 Эксплуатация компьютерных сетей является частью неопознанный объект и обязательна для изучения.

| Требования к предварительной подготовке обучающегося: | |
|---|---|
| 1 | Сети и системы передачи информации |
| 2 | Электроника и схемотехника |
| 3 | Технические средства информатизации |

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

Цели освоения: Формирование у обучающихся системных знаний и практических навыков в области эксплуатации, администрирования и технического обслуживания компьютерных сетей как компонентов автоматизированных (информационных) систем в защищенном исполнении, обеспечивающих их бесперебойную работу, целостность и доступность информации в условиях действия угроз безопасности.
Задачи: 1. Изучить архитектуру, состав и функциональное назначение программных и программно-аппаратных компонентов автоматизированных информационных систем (АИС) в защищенном исполнении.
2. Освоить методы и средства администрирования сетевых операционных систем, сервисов и служб, обеспечивающих защиту информации.
3. Сформировать умения по настройке параметров сетевого оборудования и программного обеспечения в соответствии с требованиями эксплуатационной документации и политик безопасности.
4. Овладеть навыками мониторинга технического состояния, диагностики отказов и восстановления работоспособности сетевых компонентов АИС.
5. Развить способности по организации планового технического обслуживания, текущего ремонта и ведения эксплуатационной документации.
6. Приобрести компетенции по оперативному устранению аварийных ситуаций и сбоев в работе сетей с сохранением заданного уровня защищенности.
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 И ЭКСПЛУАТАЦИИ КОМПЬЮТЕРНЫХ СЕТЕЙ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ** | | | | |
| 1. 1 | Тема 1.1. Классификация, структура и функции компьютерных сетей как компонента АИС<br>Основные виды компьютерных сетей (локальные, распределённые, корпоративные), их топологии, эталонная модель взаимодействия открытых систем (OSI), стек протоколов TCP/IP. Функции сетевого уровня, транспортного уровня и прикладного уровня применительно к задачам автоматизированных систем. Требования к сетям в защищенном исполнении.<br>Знать: определение компьютерной сети как составной части АИС; базовые топологии и их характеристики; уровневую модель OSI и стек TCP/IP; функции основных протоколов (IP, ICMP, ARP, TCP, UDP); критерии отнесения сети к защищенному исполнению.<br>/Лек/ | 6 | 4/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 1. 2 | Тема 1.2. Нормативно-правовая и эксплуатационная документация на сетевые компоненты АИС<br>Состав эксплуатационной документации (руководство администратора, руководство пользователя, инструкции по техническому обслуживанию, регламенты). Требования нормативных документов по защите информации (приказы ФСТЭК, ГОСТы) к эксплуатации сетевого оборудования и ПО. Порядок ведения журналов учёта, паспортов средств вычислительной техники и сетевых устройств.<br>Знать: перечень основных эксплуатационных документов для сетевых компонентов; требования к содержанию разделов документации; порядок учёта и хранения технической документации; ответственность должностных лиц за соблюдение регламентов.<br>/Лек/ | 6 | 4/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 1. 3 | Лабораторная работа №1<br>Тема: «Изучение состава эксплуатационной документации и сетевых конфигураций».<br>Уметь: различать типы эксплуатационных документов; сопоставлять разделы документации с реальными сетевыми настройками; фиксировать параметры сетевых интерфейсов.<br>Владеть: навыками чтения технической документации; методами первичной идентификации сетевого оборудования и его характеристик.<br>/Лаб/ | 6 | 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 |
| 1. 4 | Практическая работа №1<br>Тема: «Анализ топологии и состава оборудования корпоративной сети по документации».<br>Уметь: восстанавливать логическую схему сети по описанию в документации; определять | 6 | 4/0 | ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК | Отчет по практической работе |

| | | | | | |
|---|---|---|---|---|---|
| | критичные узлы и каналы связи.<br>Владеть: методикой анализа структуры сети для последующего планирования обслуживания<br>/Пр/ | | | 1.4.2,ПК 1.4.3 | |
| | **2. РАЗДЕЛ 2. ОСНОВЫ АДМИНИСТРИРОВАНИЯ СЕТЕВЫХ ОПЕРАЦИОННЫХ СИСТЕМ И СЛУЖБ** | | | | |
| 2. 1 | Тема 2.1. Установка, настройка и базовое администрирование сетевых ОС (Windows Server, Linux)<br>Этапы установки серверных операционных систем, настройка сетевых интерфейсов, назначение статических и динамических IP-адресов, настройка DNS-клиента, маршрутизация. Встроенные средства управления пользователями, группами, политиками безопасности. Системные журналы и инструменты мониторинга производительности.<br>Знать: системные требования и порядок установки серверных ОС; способы конфигурирования сетевых адаптеров; основные команды для проверки связности и маршрутов; структуру локальной учётной записи и группы; назначение системных журналов.<br>/Лек/ | 6 | 6/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 2. 2 | Тема 2.2. Администрирование сетевых служб (DHCP, DNS, Active Directory, NFS, SMB)<br>Принципы работы служб динамической конфигурации хостов (DHCP), системы доменных имён (DNS), службы каталогов (Active Directory), сетевых файловых систем (NFS, SMB). Настройки зон DNS, области DHCP, организационных единиц AD, общих ресурсов. Вопросы безопасности служб (аутентификация, шифрование, ограничение доступа).<br>Знать: назначение и порты служб DHCP, DNS, AD, NFS, SMB; структуру зон и записей DNS; принцип аренды адресов DHCP; схему работы контроллера домена; способы разграничения доступа к файловым ресурсам.<br>/Лек/ | 6 | 6/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 2. 3 | Лабораторная работа №2<br>Тема: «Установка серверной ОС и настройка базовых сетевых служб (DHCP, DNS)».<br>Уметь: выполнять установку ОС с сетевыми компонентами; назначать статические адреса; настраивать область DHCP и проверять выдачу адресов; создавать прямые и обратные зоны DNS.<br>Владеть: навыками работы с консольными утилитами (ipconfig, ping, nslookup, netstat); методами проверки работоспособности служб.<br>/Лаб/ | 6 | 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 |
| 2. 4 | Практическая работа №2<br>Тема: «Конфигурирование доменной структуры и групповых политик в Active Directory».<br>Уметь: устанавливать роль контроллера домена; создавать организационные единицы, пользователей и группы; применять групповые политики для ограничений.<br>Владеть: навыками администрирования через оснастки MMC; методикой проверки применения политик.<br>/Пр/ | 6 | 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 практической работе |
| | **3. РАЗДЕЛ 3. МОНИТОРИНГ И ДИАГНОСТИКА СОСТОЯНИЯ СЕТЕВЫХ КОМПОНЕНТОВ** | | | | |
| 3. 1 | Тема 3.1. Методы и средства мониторинга | 6 | 4/0 | ПК | Устный опрос |

| | | | | | |
|---|---|---|---|---|---|
| | производительности и доступности сети Инструменты мониторинга (SNMP, WMI, системные счётчики, утилиты ping, tracert, pathping). Показатели загрузки каналов, задержек, потери пакетов. Пороговые значения и настройка оповещений. Понятия SLA (уровень обслуживания) и KPI для сетевых служб. Знать: основные параметры мониторинга сети (доступность, задержка, джиттер, потеря пакетов); протокол SNMP и структуру MIB; встроенные счётчики производительности ОС; методику расчёта средней загрузки канала. /Лек/ | | | 1.2.1,ПК 1.3.1,ПК 1.4.1 | |
| 3. 2 | Тема 3.2. Диагностика отказов и неисправностей сетевого оборудования и кабельных систем Типичные отказы активного и пассивного сетевого оборудования (коммутаторы, маршрутизаторы, патч-панели, кабели). Методы локализации неисправностей (замена кабеля, проверка портов, тестирование оптических линий, анализ логов оборудования). Алгоритмы поиска неисправностей по модели OSI. Знать: признаки неисправностей на физическом, канальном и сетевом уровнях; методику прозвона кабелей; алгоритм «снизу-вверх» и «сверху-вниз» при диагностике; типовые коды ошибок коммутаторов и маршрутизаторов. /Лек/ | 6 | 4/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 3. 3 | Лабораторная работа №3 Тема: «Применение диагностических утилит и тестирование кабельной системы». Уметь: запускать мониторинг с помощью SNMP-клиентов; интерпретировать показатели трассировки и пинга; измерять затухание и целостность витой пары с помощью тестера. Владеть: навыками работы с консольными диагностическими средствами; методами первичной проверки физической целостности линий. /Лаб/ | 6 | 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. 4 | Практическая работа №3 Тема: «Разработка протокола мониторинга ключевых сетевых узлов». Уметь: составлять перечень контрольных точек; задавать пороговые значения; формировать отчёт о доступности за сутки. Владеть: методикой планирования периодичности проверок; навыками заполнения журналов мониторинга. /Пр/ | 6 | 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. 5 | Самостоятельная работа по теме «Сравнительный анализ бесплатных и коммерческих систем мониторинга (Zabbix, Nagios, PRTG)» /СР/ | 6 | 2/0 | 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 самоподготовки |
| 3. 6 | Тема 3.3. Ведение эксплуатационной документации по результатам диагностики Формы актов технического состояния, журналов регистрации отказов, протоколов проверок. Правила заполнения карточек учёта оборудования, отчётов о профилактических работах. Требования к хранению и архивации | 6 | 2/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |

| | | | | | |
|---|---|---|---|---|---|
| | документации.<br>Знать: перечень обязательных документов при диагностике; сроки хранения актов; правила внесения исправлений в документацию; порядок уведомления руководства о критических отказах.<br>/Лек/ | | | | |
| | **4. РАЗДЕЛ 4. ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ТЕКУЩИЙ РЕМОНТ СЕТЕВОГО ОБОРУДОВАНИЯ** | | | | |
| 4. 1 | Тема 4.1. Виды технического обслуживания (ТО) сетевых компонентов (ежедневное, еженедельное, планово-предупредительное)<br>Регламенты ежедневного контроля (внешний осмотр, проверка индикации), еженедельного (чистка, проверка вентиляции, резервирование конфигураций), планово-предупредительного ТО (замена термопасты, обновление прошивок, проверка источников бесперебойного питания). Периодичность и объём работ согласно эксплуатационной документации.<br>Знать: виды ТО и их периодичность; состав работ для каждого вида; критерии оценки состояния оборудования; порядок замены расходных материалов.<br>/Лек/ | 6 | 4/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 4. 2 | Тема 4.2. Алгоритмы восстановления работоспособности при отказах (замена модулей, перезагрузка, восстановление из резервной копии) Типовые сценарии отказов (зависание, сбой питания, ошибка конфигурации, повреждение файловой системы). Пошаговые инструкции по горячей и холодной замене компонентов, загрузке с резервного образа, восстановлению конфигураций из текстовых файлов. Порядок действий при частичной и полной потере функциональности.<br>Знать: алгоритмы аварийного восстановления для разных типов устройств; критерии «горячей» и «холодной» замены; способы создания и проверки резервных копий конфигураций; минимальный набор инструментов для восстановления.<br>/Лек/ | 6 | 4/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 4. 3 | Лабораторная работа №4<br>Тема: «Проведение планового ТО коммутатора и восстановление конфигурации из резервной копии».<br>Уметь: выполнять чистку и проверку вентиляции; создавать резервную копию конфигурации (startup -config); восстанавливать конфигурацию после сброса.<br>Владеть: навыками работы через консольный порт; методами проверки целостности файлов прошивки.<br>/Лаб/ | 6 | 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. 4 | Практическая работа №4<br>Тема: «Разработка графика ТО и плана аварийного восстановления для сегмента сети».<br>Уметь: рассчитывать трудоёмкость ТО на основе документации; составлять план действий при типовых отказах.<br>Владеть: навыками планирования ремонтных работ с учётом критичности узлов; методикой оценки времени восстановления.<br>/Пр/ | 6 | 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 практической работе |
| 4. 5 | Самостоятельная работа теме «Анализ типовых | 6 | 2/0 | ПК | Вопросы для |

| | | | | | |
|---|---|---|---|---|---|
| | отказов сетевого оборудования и способы их предотвращения»<br>/СР/ | | | 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 | самоподготовки |
| | **5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ (6 СЕМЕСТР)** | | | | |
| 5. 1 | Контрольная работа<br>ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении<br>ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации<br>ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении<br>/К/ | 6 | 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 |
| | **6. РАЗДЕЛ 5. АДМИНИСТРИРОВАНИЕ ЗАЩИЩЕННЫХ СЕТЕВЫХ СОЕДИНЕНИЙ И СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ** | | | | |
| 6. 1 | Тема 5.1. Настройка защищённых каналов (VPN, IPsec, SSL/TLS) в корпоративной сети<br>Протоколы IPsec (режимы транспортный и туннельный), SSL/TLS для защищённого веб-доступа. Способы организации VPN на основе маршрутизаторов и серверов доступа. Параметры шифрования, аутентификации, обмена ключами (IKE). Уделяется внимание совместимости с межсетевыми экранами.<br>Знать: назначение протоколов IPsec, SSL, IKE; различия между туннельным и транспортным режимами; способы распространения сертификатов; параметры политик безопасности для VPN.<br>/Лек/ | 7 | 4/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 6. 2 | Тема 5.2. Управление средствами криптографической защиты информации (СКЗИ) на сетевом уровне<br>Сертифицированные СКЗИ (например, VipNet, КриптоПро, отечественные VPN-шлюзы). Установка, настройка ключевых носителей, генерация и обмен ключами, контроль целостности модулей. Журналы аудита СКЗИ и порядок действий при компрометации ключей.<br>Знать: перечень разрешённых СКЗИ для государственных информационных систем; правила хранения ключевых носителей; порядок генерации ключей; признаки несанкционированного доступа к криптооборудованию.<br>/Лек/ | 7 | 4/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 6. 3 | Лабораторная работа №5<br>Тема: «Настройка VPN-соединения на базе IPsec между двумя сегментами сети».<br>Уметь: создавать политики безопасности; настраивать параметры IKE (фаза 1 и 2); | 7 | 6/0 | ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК | Отчет по лабораторной работе |

| | | | | | |
|---|---|---|---|---|---|
| | проверять установленное соединение через захват трафика (Wireshark).<br>Владеть: навыками конфигурирования VPN-шлюзов; методами диагностики неработающих туннелей.<br>/Лаб/ | | | 1.4.2,ПК 1.4.3 | |
| 6. 4 | Практическая работа №5<br>Тема: «Разработка схемы криптозащиты для распределённой АИС с несколькими филиалами».<br>Уметь: выбирать тип VPN для каждого филиала; составлять таблицу ключей и политик; оценивать пропускную способность после шифрования.<br>Владеть: методикой планирования криптозащиты с учётом нормативных требований.<br>/Пр/ | 7 | 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 практической работе |
| | **7. РАЗДЕЛ 6. ОБЕСПЕЧЕНИЕ БЕСПЕРЕБОЙНОЙ РАБОТЫ СЕТЕЙ (ОТКАЗОУСТОЙЧИВОСТЬ И БЕКАП)** | | | | |
| 7. 1 | Тема 6.1. Резервное копирование конфигураций и данных сетевых устройств<br>Методы резервирования (полное, инкрементное, дифференциальное) на примере сетевых ОС и коммутаторов. Протоколы копирования (TFTP, FTP, SCP, RSYNC), автоматизация резервного копирования через cron или планировщик задач. Требования к частоте копирования и месту хранения (локальный и удалённый репозиторий).<br>Знать: виды резервного копирования и их применимость; команды для сохранения и восстановления конфигураций; способы проверки целостности резервных копий.<br>/Лек/ | 7 | 4/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 7. 2 | Тема 6.2. Организация отказоустойчивых решений (агрегация каналов, резервирование маршрутов, протоколы VRRP/HSRP)<br>Механизмы повышения доступности: объединение портов (LACP), балансировка нагрузки (ECMP), протоколы резервирования шлюзов (VRRP, HSRP, GLBP). Настройка приоритетов, таймеров отслеживания, аварийное переключение. Сценарии двойного отказа и способы их минимизации.<br>Знать: принципы работы LACP, VRRP, HSRP; различия между протоколами; параметры аварийного переключения (таймеры hello, dead); влияние на сетевую топологию.<br>/Лек/ | 7 | 2/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 7. 3 | Лабораторная работа №6<br>Тема: «Настройка резервного шлюза по протоколу VRRP и автоматическое резервирование конфигураций».<br>Уметь: настраивать виртуальный IP-адрес и приоритеты; проверять переключение при отказе основного шлюза; организовывать автоматическое копирование конфигураций на сервер.<br>Владеть: навыками тестирования отказоустойчивости; методами восстановления при переключении.<br>/Лаб/ | 7 | 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 |
| 7. 4 | Практическая работа №6<br>Тема: «Расчёт показателей доступности сети при внедрении резервирования».<br>Уметь: рассчитывать коэффициент доступности с учётом MTBF и MTTR; сравнивать варианты с одним и двумя маршрутизаторами. | 7 | 6/0 | ПК 1.2.2,ПК 1.2.3,ПК 1.3.2,ПК 1.3.3,ПК 1.4.2,ПК | Отчет по практической работе |

| | | | | | |
|---|---|---|---|---|---|
| | Владеть: методикой оценки экономической эффективности резервирования.<br>/Пр/ | | | 1.4.3 | |
| | **8. РАЗДЕЛ 7. АДМИНИСТРИРОВАНИЕ В УСЛОВИЯХ ДЕЙСТВИЯ УГРОЗ (ОБНАРУЖЕНИЕ АТАК И РЕАГИРОВАНИЕ)** | | | | |
| 8. 1 | Тема 7.1. Средства обнаружения сетевых атак (IDS/IPS), настройка сигнатур<br>Системы обнаружения вторжений (Snort, Suricata) и предотвращения (IPS) на сетевом уровне. Типы сигнатур (для атак DoS, сканирования, эксплуатации уязвимостей). Режимы работы (inline, promiscuous), интеграция с системами управления событиями (SIEM).<br>Знать: принципы работы IDS/IPS; структуру правил (сигнатур); методы обхода обнаружения (фрагментация, туннелирование); порядок обновления баз сигнатур.<br>/Лек/ | 7 | 4/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 8. 2 | Тема 7.2. Реагирование на инциденты в сети (блокировка, изоляция, сбор артефактов)<br>Процедуры реагирования: изоляция заражённого хоста через VLAN или ACL, блокировка IP-адресов, отключение портов коммутатора. Порядок сбора сетевых журналов, pcap-файлов, дампов памяти. Шаги по эскалации инцидента и взаимодействию с отделом информационной безопасности.<br>Знать: алгоритм реагирования на сетевую атаку; способы изоляции без отключения всей сети; перечень сохраняемых артефактов; требования к сохранению доказательной базы.<br>/Лек/ | 7 | 2/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 8. 3 | Лабораторная работа №7<br>Тема: «Настройка IDS на базе Snort и отработка сценария блокировки атакующего хоста».<br>Уметь: устанавливать и настраивать Snort в режиме NIDS; создавать простые правила; анализировать предупреждения; изолировать хост через ACL на коммутаторе.<br>Владеть: навыками работы с консолью Snort; методами захвата и фильтрации трафика.<br>/Лаб/ | 7 | 8/0 | 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. 4 | Практическая работа №7<br>Тема: «Разработка плана реагирования на типовые сетевые инциденты (DoS, сканирование, подбор паролей)».<br>Уметь: составлять поэтапный план действий для каждого типа инцидента; определять ответственных и сроки.<br>Владеть: методикой документирования инцидентов; навыками составления отчётов о расследовании.<br>/Пр/ | 7 | 8/0 | 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. 5 | Самостоятельная работа по теме «Обзор современных угроз для корпоративных сетей и методов их обнаружения (MITRE ATT&CK для сетей)»<br>/СР/ | 7 | 6/0 | 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 |
| 8. 6 | Самостоятельная работа по теме «Сравнение протоколов VRRP и HSRP: особенности реализации в разных вендорских ОС» | 7 | 4/0 | ПК 1.2.1,ПК 1.2.2,ПК | Вопросы для самоподготовки |

| | | | | | |
|---|---|---|---|---|---|
| | /СР/ | | | 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 | |
| | **9. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ (7 СЕМЕСТР)** | | | | |
| 9. 1 | Контрольная работа<br>ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении<br>ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации<br>ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении<br>/К/ | 7 | 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 |
| | **10. РАЗДЕЛ 8. КОМПЛЕКСНОЕ АДМИНИСТРИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ** | | | | |
| 10. 1 | Тема 8.1. Интеграция сетевой инфраструктуры с общей системой защиты информации (СЗИ) Сопряжения сетевых компонентов с межсетевыми экранами, системами антивирусной защиты, средствами доверенной загрузки. Политики фильтрации на стыках сетей, правила трансляции адресов (NAT), маршрутизация через защищённые шлюзы. Схемы сегментации сети по уровням конфиденциальности.<br>Знать: принципы взаимодействия сетевого уровня с СЗИ; правила построения периметра безопасности; варианты размещения прокси-серверов и шлюзов; методы контроля целостности сетевых настроек.<br>/Лек/ | 8 | 6/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 10. 2 | Тема 8.2. Администрирование виртуальных частных сетей (VPLS, MPLS L3VPN) и SDN-решений<br>Технологии виртуализации сетей (VPLS, MPLS L3VPN), архитектура программно-определяемых сетей (SDN), протокол OpenFlow. Управления потоками, изоляции трафика разных клиентов, QoS-политики. .<br>Знать: отличия VPLS от L3VPN; базовые компоненты SDN (контроллер, коммутаторы); возможности динамической маршрутизации; ограничения безопасности в SDN.<br>/Лек/ | 8 | 8/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 10. 3 | Лабораторная работа №8<br>Тема: «Настройка политик доступа на пограничном маршрутизаторе и проверка VLAN-изоляции».<br>Уметь: создавать access-списки с учётом политик безопасности; проверять изоляцию трафика между VLAN; настраивать статическую маршрутизацию через шлюз СЗИ.<br>Владеть: навыками применения расширенных ACL; методами тестирования прохождения | 8 | 14/2 | 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 |

| | | | | | |
|---|---|---|---|---|---|
| | трафика.<br>/Лаб/ | | | | |
| 10. 4 | Практическая работа №8<br>Тема: «Проектирование сетевой архитектуры АИС с учётом требований к защищённым сегментам».<br>Уметь: проектировать схему адресации с учётом сегментации; определять точки размещения средств контроля.<br>Владеть: методикой обоснования выбора сетевого оборудования под задачи защищённой АИС.<br>/Пр/ | 8 | 10/0 | 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 |
| 10. 5 | Самостоятельная работа по теме «Интеграция межсетевых экранов, NAT и политик фильтрации в условиях виртуализированных и программно-определяемых сетей (VPLS/MPLS L3VPN и SDN)»»<br>/СР/ | 8 | 8/0 | 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 |
| | **11. РАЗДЕЛ 9. ПЛАНОВОЕ ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ТЕКУЩИЙ РЕМОНТ В ЗАЩИЩЁННОЙ АИС** | | | | |
| 11. 1 | Тема 9.1. Организация планового ТО с учётом режима защищённости (ограничение доступа, регламентные окна)<br>Особенности проведения ТО в системах с ограниченным доступом: согласование времени, оформление допусков, контроль действий персонала, ведение протоколов обслуживания. Регламентные окна, резервирование на время работ, оповещение пользователей.<br>Знать: нормативы по проведению ТО в защищённых АИС; требования к оформлению нарядов-допусков; процедуру ввода/вывода оборудования из эксплуатации; порядок оповещения.<br>/Лек/ | 8 | 8/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 11. 2 | Тема 9.2. Методы восстановления работоспособности при аппаратных сбоях с сохранением защищённости (замена без нарушения контура безопасности)<br>Сценарии замены вышедших из строя коммутаторов, маршрутизаторов, серверов с сохранением целостности криптографических ключей и сертификатов. Процедуры переноса ключевой информации, синхронизация часов, проверка контрольных сумм после замены. Риски нарушения режима защищённости при неквалифицированной замене.<br>Знать: алгоритм замены оборудования в защищённой системе; способы переноса ключей и сертификатов; методы верификации после замены; типовые ошибки при восстановлении.<br>/Лек/ | 8 | 10/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 11. 3 | Лабораторная работа №9<br>Тема: «Замена сетевого оборудования с переносом ключей и проверкой работоспособности СЗИ».<br>Уметь: выполнять миграцию конфигурации и ключей на новое устройство; проверять прохождение защищённого трафика; заполнять акт замены.<br>Владеть: навыками безопасной замены узлов в действующей сети; методами проверки | 8 | 14/2 | 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 |

| | | | | | |
|---|---|---|---|---|---|
| | целостности после замены.<br>/Лаб/ | | | | |
| 11. 4 | Практическая работа №9<br>Тема: «Составление регламента выполнения планового ТО для сегмента сети с критической информацией».<br>Уметь: определять перечень необходимых действий и их приоритет; рассчитывать длительность регламентного окна.<br>Владеть: методикой разработки регламентов с учётом требований защищённости.<br>/Пр/ | 8 | 8/0 | 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 |
| 11. 5 | Самостоятельная работа по теме «Организация технического обслуживания и восстановления оборудования в защищённых автоматизированных информационных системах»<br>/СР/ | 8 | 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 |
| | **12. РАЗДЕЛ 10. ПРОВЕРКА ТЕХНИЧЕСКОГО СОСТОЯНИЯ И КОНТРОЛЬ РАБОТОСПОСОБНОСТИ АИС** | | | | |
| 12. 1 | Тема 11.1. Состав и порядок ведения эксплуатационной документации для защищённых АИС<br>Формы журналов учёта средств защиты, протоколов технического обслуживания, актов проверки, отчётов о восстановлении, карточек оборудования. Требования к электронному и бумажному документообороту, срокам хранения, порядку корректировки.<br>Знать: перечень обязательных документов в защищённой АИС; правила присвоения грифов; порядок уничтожения устаревших документов; ответственность за ведение.<br>/Лек/ | 8 | 10/0 | ПК 1.2.1,ПК 1.3.1,ПК 1.4.1 | Устный опрос |
| 12. 2 | Практическая работа №11<br>Тема: «Заполнение комплекта эксплуатационных документов за отчётный период (журнал отказов, акты ТО, отчёт о восстановлении)».<br>Уметь: заполнять все разделы документов согласно требованиям; сверять фактические данные с документацией.<br>Владеть: навыками ведения документации в электронной системе документооборота; методикой проверки полноты документации.<br>/Пр/ | 8 | 10/0 | 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 |
| 12. 3 | Самостоятельная работа по теме «Разработка шаблонов всех необходимых эксплуатационных документов для гипотетической АИС в защищённом исполнении».<br>/СР/ | 8 | 6/0 | 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 |
| | **13. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ (8 СЕМЕСТР)** | | | | |
| 13. 1 | Контрольная работа.<br>ПК 1.2.: Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении | 6 | 0/0 | ПК 1.2.1,ПК 1.2.2,ПК 1.2.3,ПК 1.3.1,ПК | Вопросы для контрольной работы, итоговое тестирование |

| | | | | | |
|---|---|---|---|---|---|
| | ПК 1.2.1: Знать теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации<br>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<br>ПК 1.2.3: Иметь практический опыт администрирования автоматизированных систем в защищенном исполнении<br>ПК 1.3.: Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации<br>ПК 1.3.1: Знать порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях<br>ПК 1.3.2: Уметь настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам<br>ПК 1.3.3: Иметь практический опыт эксплуатации компонентов систем защиты информации автоматизированных систем<br>ПК 1.4.: Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении<br>ПК 1.4.1: Знать принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации<br>ПК 1.4.2: Уметь обеспечивать работоспособность, обнаруживать и устранять неисправности<br>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<br>/СР/ | | | 1.3.2,ПК 1.3.3,ПК 1.4.1,ПК 1.4.2,ПК 1.4.3 | |

Список выбранных образовательный технологий:

| Название | Описание |
|---|---|
| Информационные технологии | Личностно ориентированная технология, способ организации самостоятельной деятельности учащихся, направленный на решение задачи учебного проекта |
| Кейс-технология | Технология включает в себя: индивидуальную самостоятельную работу обучаемых с материалами кейса (идентификация проблемы, формулирование ключевых альтернатив, предложение решения или рекомендуемого действия); работу в малых группах по согласованию видения ключевой проблемы и ее решений; презентацию и экспертизу результатов малых групп на общей дискуссии (в |

| | |
|---|---|
| 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 И ЭКСПЛУАТАЦИИ КОМПЬЮТЕРНЫХ СЕТЕЙ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Тема 1.1. Классификация, структура и функции компьютерных сетей как компонента АИС
1. Что представляет собой компьютерная сеть как составная часть автоматизированной информационной системы?
2. Каковы основные отличия локальных, распределенных и корпоративных сетей друг от друга?
3. Какие базовые топологии компьютерных сетей вы знаете, и в чем заключаются их ключевые характеристики?
4. Для чего предназначена эталонная модель взаимодействия открытых систем (OSI), и из скольких уровней она состоит?
5. Какие уровни модели OSI соответствуют функциям стека протоколов TCP/IP?
6. Какие функции выполняет сетевой уровень применительно к задачам автоматизированных систем?
7. Каковы основные функции транспортного и прикладного уровней в рамках АИС?
8. Для чего предназначены протоколы IP, ICMP, ARP, TCP и UDP, и какова их роль в сети?
9. Какие критерии позволяют отнести компьютерную сеть к сети в защищенном исполнении?
10. Какие требования предъявляются к компьютерным сетям, функционирующим в защищенном исполнении?

Тема 1.2. Нормативно-правовая и эксплуатационная документация на сетевые компоненты АИС
1. Каков перечень основных эксплуатационных документов для сетевых компонентов АИС?
2. Какие разделы должны содержаться в руководстве администратора и руководстве пользователя сетевого компонента?
3. Какие требования нормативных документов по защите информации (приказы ФСТЭК, ГОСТы) регламентируют эксплуатацию сетевого оборудования?
4. Какой порядок ведения журналов учёта сетевых устройств и средств вычислительной техники установлен в организации?
5. Какие сведения должны содержаться в паспорте средства вычислительной техники и сетевого устройства?
6. Каков порядок учёта и хранения технической документации на сетевые компоненты?
7. Кто несет ответственность за соблюдение регламентов эксплуатации сетевого оборудования, и какова мера этой ответственности?
8. В каком порядке вносятся изменения и исправления в эксплуатационную документацию?
9. Какие требования предъявляются к содержанию инструкций по техническому обслуживанию сетевых компонентов?
10. Каков срок хранения эксплуатационной документации, и каков порядок её архивации?

РАЗДЕЛ 2. ОСНОВЫ АДМИНИСТРИРОВАНИЯ СЕТЕВЫХ ОПЕРАЦИОННЫХ СИСТЕМ И СЛУЖБ

Тема 2.1. Установка, настройка и базовое администрирование сетевых ОС (Windows Server, Linux)
1. Каковы системные требования и основные этапы установки серверных операционных систем (Windows Server и Linux)?
2. Как производится настройка сетевых интерфейсов и назначение статических IP-адресов в серверных ОС?
3. В чем разница между назначением статического и динамического IP-адреса, и как настраивается DNS-клиент?
4. Какие основные команды используются для проверки связности и маршрутов в сетевых ОС?
5. Какова структура локальной учётной записи и групп пользователей в Windows Server и Linux?
6. Какие встроенные средства управления пользователями, группами и политиками безопасности доступны в серверных ОС?
7. Для чего предназначены системные журналы, и какие инструменты мониторинга производительности встроены в ОС?
8. Каков порядок настройки статической маршрутизации на сервере под управлением Windows Server и Linux?
9. Какие действия необходимо выполнить для конфигурирования сетевого адаптера с использованием командной строки?
10. Какие ключевые параметры производительности сервера необходимо контролировать в первую очередь?

Тема 2.2. Администрирование сетевых служб (DHCP, DNS, Active Directory, NFS, SMB)
1. Каково назначение и какие стандартные порты используют службы DHCP, DNS, AD, NFS и SMB?
2. Какова структура зон и типы записей DNS, и для чего каждая из них предназначена?
3. Каков принцип аренды IP-адресов протоколом DHCP, и из каких этапов состоит этот процесс?
4. Как настраиваются области и параметры области в службе DHCP?
5. Какова схема работы контроллера домена Active Directory, и какую роль он выполняет в сети?
6. Как организованы организационные единицы (OU) в Active Directory, и для чего они используются?
7. Какие способы разграничения доступа к файловым ресурсам через SMB и NFS вы знаете?
8. Как настраиваются общие сетевые ресурсы (SMB-шары) и экспортируемые файловые системы (NFS)?
9. Какие вопросы безопасности (аутентификация, шифрование, ограничение доступа) критичны для служб AD, DNS и DHCP?

10. В чем различия между сетевыми файловыми системами NFS и SMB с точки зрения администрирования и безопасности?

РАЗДЕЛ 3. МОНИТОРИНГ И ДИАГНОСТИКА СОСТОЯНИЯ СЕТЕВЫХ КОМПОНЕНТОВ

Тема 3.1. Методы и средства мониторинга производительности и доступности сети
1. Какие основные параметры мониторинга сети (доступность, задержка, джиттер, потеря пакетов) являются ключевыми?
2. Для чего предназначен протокол SNMP, и какова структура базы управляющей информации (MIB)?
3. Какие встроенные счётчики производительности операционных систем используются для мониторинга сети?
4. С какой целью применяются утилиты ping, tracert и pathping, и какую информацию они предоставляют?
5. Как рассчитывается средняя загрузка канала, и какие единицы измерения при этом используются?
6. Каковы методики настройки пороговых значений и организации оповещений о превышении порогов?
7. Что такое WMI (Windows Management Instrumentation) и как он применяется для мониторинга сетевых компонентов?
8. Какие показатели включаются в понятие SLA (уровень обслуживания) для сетевых служб?
9. Какие KPI (ключевые показатели эффективности) наиболее важны для оценки работы сетевой инфраструктуры?
10. Как настроить системный мониторинг производительности сети с использованием стандартных средств ОС?

Тема 3.2. Диагностика отказов и неисправностей сетевого оборудования и кабельных систем
1. Каковы типичные признаки неисправностей на физическом, канальном и сетевом уровнях модели OSI?
2. Каковы основные причины отказов активного оборудования (коммутаторы, маршрутизаторы) и пассивного оборудования (кабели, патч-панели)?
3. Какова методика прозвона кабелей и проверки целостности оптических линий?
4. Какие методы локализации неисправностей (замена кабеля, проверка портов, анализ логов) применяются в первую очередь?
5. В чем суть алгоритма диагностики «снизу-вверх» (Bottom-Up) и «сверху-вниз» (Top-Down)?
6. Какие типовые коды ошибок коммутаторов и маршрутизаторов указывают на проблемы с аппаратной частью?
7. Какие инструменты используются для тестирования оптических линий связи и измерения затухания?
8. Каков порядок действий при обнаружении неисправности порта на коммутаторе?
9. Как анализируются системные логи сетевого оборудования для выявления причины отказа?
10. Как отличить программный сбой оборудования от аппаратной неисправности?

Тема 3.3. Ведение эксплуатационной документации по результатам диагностики
1. Каков перечень обязательных документов, которые должны оформляться при проведении диагностики неисправностей?
2. Какие сведения должны содержаться в акте технического состояния сетевого оборудования?
3. Как ведется журнал регистрации отказов, и какие записи в нем обязательны?
4. Каковы правила заполнения карточек учёта оборудования по результатам проверок и профилактики?
5. Какие требования предъявляются к хранению и архивации актов диагностики и протоколов проверок?
6. Каковы сроки хранения эксплуатационной документации по результатам диагностики?
7. Каков порядок внесения исправлений и дополнений в уже оформленную документацию?
8. Как оформляется отчёт о профилактических работах и какие разделы он должен содержать?
9. Каков порядок уведомления руководства о критических отказах, выявленных в ходе диагностики?
10. Кто отвечает за достоверность сведений, вносимых в протоколы диагностики?

РАЗДЕЛ 4. ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ТЕКУЩИЙ РЕМОНТ СЕТЕВОГО ОБОРУДОВАНИЯ

Тема 4.1. Виды технического обслуживания (ТО) сетевых компонентов (ежедневное, еженедельное, планово-предупредительное)
1. Какие виды технического обслуживания сетевых компонентов существуют, и какова их периодичность?
2. Каков состав работ при ежедневном контроле состояния сетевого оборудования?
3. Какие работы включаются в еженедельное техническое обслуживание (чистка, проверка вентиляции, резервирование конфигураций)?
4. Что входит в объём планово-предупредительного технического обслуживания (ППР)?
5. Какова периодичность замены термопасты и обновления прошивок сетевых устройств согласно регламенту?
6. Какие критерии используются для оценки состояния оборудования при проведении ТО?
7. Как проверяются источники бесперебойного питания в рамках планового ТО?
8. Каков порядок замены расходных материалов (вентиляторы, блоки питания) в сетевом оборудовании?
9. Какие документы оформляются по результатам каждого вида технического обслуживания?
10. Как часто необходимо проводить резервирование конфигурационных файлов сетевых устройств?

Тема 4.2. Алгоритмы восстановления работоспособности при отказах (замена модулей, перезагрузка, восстановление из резервной копии)
1. Каковы типовые сценарии отказов (зависание, сбой питания, ошибка конфигурации, повреждение ФС) сетевого оборудования?
2. Каков пошаговый алгоритм аварийного восстановления для коммутатора и маршрутизатора?
3. В чем отличие «горячей» замены компонентов от «холодной», и в каких случаях применяется каждый из способов?
4. Как осуществляется загрузка оборудования с резервного образа операционной системы?

5. Каков порядок восстановления конфигурации устройства из текстового файла резервной копии?
6. Какие способы создания и проверки целостности резервных копий конфигураций вы знаете?
7. Каковы действия администратора при частичной потере функциональности сетевого устройства?
8. Какой минимальный набор инструментов и запасных компонентов должен быть у администратора для восстановления?
9. Как восстановить работоспособность сетевого устройства при повреждении файловой системы?
10. Каков порядок действий при полной потере функциональности основного сетевого шлюза?

РАЗДЕЛ 5. АДМИНИСТРИРОВАНИЕ ЗАЩИЩЕННЫХ СЕТЕВЫХ СОЕДИНЕНИЙ И СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

Тема 5.1. Настройка защищённых каналов (VPN, IPsec, SSL/TLS) в корпоративной сети
1. Каково назначение протоколов IPsec, SSL/TLS и IKE в организации защищенных соединений?
2. В чем заключаются различия между туннельным и транспортным режимами работы протокола IPsec?
3. Какие параметры шифрования и аутентификации настраиваются при организации VPN-соединения?
4. Как происходит обмен ключами в протоколе IKE при установке IPsec-соединения?
5. Какие способы распространения сертификатов используются при организации SSL/TLS-каналов?
6. Как настраиваются политики безопасности для VPN на основе маршрутизаторов и серверов доступа?
7. Каковы особенности сопряжения VPN-шлюзов с межсетевыми экранами?
8. Какие типы аутентификации поддерживаются при настройке защищенных каналов?
9. Как проверить корректность работы IPsec-туннеля и выявить ошибки его настройки?
10. Какие параметры политик безопасности являются критическими для обеспечения совместимости VPN с существующей инфраструктурой?

Тема 5.2. Управление средствами криптографической защиты информации (СКЗИ) на сетевом уровне
1. Какие сертифицированные СКЗИ (например, VipNet, КриптоПро) разрешены для использования в государственных информационных системах?
2. Каков порядок установки и первоначальной настройки СКЗИ на сетевом уровне?
3. Как производится генерация ключей и обмен ключевой информацией между абонентами СКЗИ?
4. Каковы правила хранения ключевых носителей и обращения с ключевой документацией?
5. Как осуществляется контроль целостности модулей и программного обеспечения СКЗИ?
6. Какие признаки указывают на несанкционированный доступ к криптографическому оборудованию?
7. Какие сведения фиксируются в журналах аудита СКЗИ, и как часто они должны просматриваться?
8. Каков порядок действий администратора при компрометации ключевой информации?
9. Какие требования предъявляются к среде исполнения СКЗИ (защита от вирусов, контроль доступа)?
10. Каков порядок регулярной смены ключей шифрования в корпоративной сети?

РАЗДЕЛ 6. ОБЕСПЕЧЕНИЕ БЕСПЕРЕБОЙНОЙ РАБОТЫ СЕТЕЙ (ОТКАЗОУСТОЙЧИВОСТЬ И БЕКАП)

Тема 6.1. Резервное копирование конфигураций и данных сетевых устройств
1. В чем разница между полным, инкрементным и дифференциальным резервным копированием, и где каждый вид применим?
2. Какие протоколы (TFTP, FTP, SCP, RSYNC) используются для копирования конфигураций, и каковы их особенности?
3. Какие команды в сетевых ОС и на коммутаторах используются для сохранения и восстановления конфигураций?
4. Как организовать автоматическое резервное копирование с использованием cron или планировщика задач Windows?
5. Каковы требования к частоте резервного копирования конфигураций сетевых устройств?
6. Где должны храниться резервные копии (локальный и удалённый репозиторий) и почему?
7. Какими способами можно проверить целостность и пригодность резервных копий для восстановления?
8. Какие данные, помимо конфигураций устройств, подлежат резервированию в сетевой инфраструктуре?
9. Как защитить резервные копии от несанкционированного доступа?
10. Каков порядок тестирования процедуры восстановления из резервной копии?

Тема 6.2. Организация отказоустойчивых решений (агрегация каналов, резервирование маршрутов, протоколы VRRP/HSRP)
1. Каков принцип работы агрегации каналов (LACP) и для чего она применяется?
2. Как работает балансировка нагрузки с использованием протокола ECMP?
3. Каково назначение протоколов резервирования шлюзов (VRRP, HSRP, GLBP) и в чем их принципиальные различия?
4. Какие параметры приоритетов и таймеров отслеживания настраиваются в протоколах VRRP/HSRP?
5. Как происходит аварийное переключение (failover) при выходе из строя активного маршрутизатора в HSRP/VRRP?
6. Каково влияние протоколов резервирования на сетевую топологию и как избежать петель?
7. Какие сценарии двойного отказа могут возникнуть, и как минимизировать их последствия?
8. Как настраивается отслеживание интерфейсов (Interface Tracking) в VRRP/HSRP?
9. Каковы ограничения и недостатки использования протоколов VRRP и HSRP?
10. Как проверить корректность работы отказоустойчивого кластера шлюзов?

РАЗДЕЛ 7. АДМИНИСТРИРОВАНИЕ В УСЛОВИЯХ ДЕЙСТВИЯ УГРОЗ (ОБНАРУЖЕНИЕ АТАК И РЕАГИРОВАНИЕ)

Тема 7.1. Средства обнаружения сетевых атак (IDS/IPS), настройка сигнатур
1. Каковы принципы работы систем обнаружения вторжений (IDS) и предотвращения вторжений (IPS)?
2. В чем разница между режимами работы IDS/IPS (inline, promiscuous)?
3. Какие типы сигнатур используются для обнаружения атак DoS, сканирования портов и эксплуатации уязвимостей?
4. Какова структура правил (сигнатур) в системах типа Snort или Suricata?
5. Какие методы обхода систем обнаружения (фрагментация, туннелирование) существуют, и как с ними бороться?
6. Каков порядок обновления баз сигнатур для IDS/IPS и почему это критично?
7. Как осуществляется интеграция IDS/IPS с системами управления событиями (SIEM)?
8. Какие действия предпринимает IPS при срабатывании сигнатуры, и чем это отличается от IDS?
9. Как настраивается подавление ложных срабатываний (false positives) в системах обнаружения?
10. Какова роль IDS/IPS в общей системе защиты информации на сетевом уровне?

Тема 7.2. Реагирование на инциденты в сети (блокировка, изоляция, сбор артефактов)
1. Каков общий алгоритм реагирования на сетевую атаку (инцидент)?
2. Как осуществляется изоляция заражённого хоста через VLAN или ACL без отключения всей сети?
3. Какие способы блокировки IP-адресов и отключения портов коммутатора применяются при реагировании?
4. Каков порядок сбора сетевых журналов, pcap-файлов и дампов памяти для расследования?
5. Какие артефакты необходимо сохранить для доказательной базы, и каковы требования к их сохранности?
6. Каковы шаги по эскалации инцидента и порядок взаимодействия с отделом информационной безопасности?
7. Как проводится анализ перехваченного трафика (pcap) для выявления признаков атаки?
8. Какие действия запрещены при реагировании на инцидент, чтобы не повредить доказательную базу?
9. Как организовать удаленную изоляцию зараженного устройства, если оно находится в другой подсети?
10. Каков порядок восстановления работы изолированного сегмента сети после устранения угрозы?

РАЗДЕЛ 8. КОМПЛЕКСНОЕ АДМИНИСТРИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Тема 8.1. Интеграция сетевой инфраструктуры с общей системой защиты информации (СЗИ)
1. Каковы принципы взаимодействия сетевого уровня с межсетевыми экранами и системами антивирусной защиты?
2. Как строятся политики фильтрации на стыках сетей с различным уровнем конфиденциальности?
3. Каковы правила трансляции адресов (NAT) и их влияние на безопасность сети?
4. Как организуется маршрутизация трафика через защищённые шлюзы в сегментированной сети?
5. Какие схемы сегментации сети по уровням конфиденциальности используются в защищенных АИС?
6. Как настраивается сопряжение сетевых компонентов со средствами доверенной загрузки?
7. Каковы варианты размещения прокси-серверов и шлюзов безопасности в сетевой инфраструктуре?
8. Какие методы контроля целостности сетевых настроек и конфигураций применяются в СЗИ?
9. Как обеспечивается безопасность управления сетевым оборудованием в защищенной АИС?
10. Как интегрируются средства обнаружения вторжений с политиками фильтрации межсетевых экранов?

Тема 8.2. Администрирование виртуальных частных сетей (VPLS, MPLS L3VPN) и SDN-решений
1. В чем заключаются основные отличия технологий VPLS от MPLS L3VPN?
2. Каковы базовые компоненты архитектуры программно-определяемых сетей (SDN)?
3. Какую роль выполняет контроллер в SDN-архитектуре, и как происходит управление потоками?
4. Каков протокол OpenFlow и как он используется для взаимодействия контроллера и коммутаторов?
5. Как реализуется изоляция трафика разных клиентов в технологиях VPLS и L3VPN?
6. Какие политики качества обслуживания (QoS) применяются в виртуальных частных сетях?
7. Каковы возможности динамической маршрутизации в SDN-решениях по сравнению с классическими сетями?
8. Какие ограничения безопасности характерны для SDN-архитектур и как они нивелируются?
9. Как выполняется управление виртуальными маршрутизаторами и коммутаторами в среде MPLS?
10. Как организовать мониторинг и управление потоками в крупной MPLS/VPLS сети?

РАЗДЕЛ 9. ПЛАНОВОЕ ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ТЕКУЩИЙ РЕМОНТ В ЗАЩИЩЁННОЙ АИС

Тема 9.1. Организация планового ТО с учётом режима защищённости (ограничение доступа, регламентные окна)
1. Каковы нормативы и особенности проведения технического обслуживания в системах с ограниченным доступом?
2. Как производится согласование времени проведения ТО, и что такое «регламентное окно»?
3. Каков порядок оформления допусков и нарядов-допусков для персонала, проводящего ТО?
4. Как осуществляется контроль действий обслуживающего персонала во время работ в защищенной зоне?
5. Как организуется резервирование системы на время проведения плановых работ?
6. Каков порядок оповещения пользователей о проведении ТО и возможных перерывах в работе?
7. Как ведется протокол обслуживания, и какие записи в нем являются обязательными?
8. Каков порядок ввода оборудования в эксплуатацию и вывода из эксплуатации в защищенной АИС?
9. Какие меры предпринимаются для предотвращения утечки информации во время обслуживания?
10. Кто дает разрешение на начало работ по ТО в защищенной системе?

Тема 9.2. Методы восстановления работоспособности при аппаратных сбоях с сохранением защищённости (замена без нарушения контура безопасности)
1. Каков алгоритм замены вышедшего из строя коммутатора или маршрутизатора с сохранением целостности

криптографических ключей?
2. Как производится перенос ключевой информации и сертификатов на новое оборудование при замене?
3. Какие действия необходимо выполнить для синхронизации системного времени после замены оборудования?
4. Каким образом проверяются контрольные суммы и целостность ПО после замены устройств?
5. Каковы риски нарушения режима защищённости при неквалифицированной замене оборудования?
6. Как производится перенос конфигурации с отказавшего устройства на новое с сохранением политик безопасности?
7. Какие типовые ошибки допускаются при восстановлении оборудования в защищенной системе?
8. Как обеспечить сохранность криптографических ключей при физической замене сервера?
9. Какие проверки необходимо выполнить после замены для подтверждения работоспособности и защищенности?
10. Как документируется факт замены оборудования и перенос ключевой информации?

РАЗДЕЛ 10. ПРОВЕРКА ТЕХНИЧЕСКОГО СОСТОЯНИЯ И КОНТРОЛЬ РАБОТОСПОСОБНОСТИ АИС

Тема 10.1. Инструментальный контроль сетевых параметров (анализаторы спектра, тестеры кабелей, оптические рефлектометры)
1. Для чего предназначен оптический рефлектометр (OTDR), и какие параметры он позволяет измерить?
2. Каковы нормативные значения затухания и перекоса в кабельных системах?
3. Как работает тестер витой пары, и какие параметры целостности экранирования он проверяет?
4. Каков порядок оформления актов инструментального контроля физических параметров сети?
5. С какой периодичностью проводится инструментальный контроль сетевых параметров согласно регламенту?
6. Какова методика измерения затухания и отражения в оптических линиях связи?
7. Какие приборы используются для анализа спектра и поиска помех в сетях?
8. Каковы типичные ошибки при тестировании кабельных систем и как их избежать?
9. Как интерпретировать данные, полученные с помощью OTDR (рефлектограмму)?
10. Какие критерии позволяют считать кабельную линию годной к эксплуатации?

Тема 10.2. Комплексная проверка АИС в целом (сеть + СЗИ + прикладное ПО) по регламенту
1. Каков перечень контрольных точек при комплексной проверке автоматизированной системы в целом?
2. Как проводится тестирование сквозной доступности ресурсов с учетом работы средств защиты?
3. Какие методики используются для проверки корректности авторизации и разграничения доступа?
4. Как проверяется целостность системных и сетевых журналов в ходе комплексной проверки?
5. Какие сценарии имитации отказов (failover testing) отрабатываются при проверке АИС?
6. Как проводится нагрузочное тестирование сетевой инфраструктуры и прикладного ПО?
7. Какие требования предъявляются к оформлению итогового протокола комплексной проверки?
8. Каков порядок устранения отклонений и замечаний, выявленных в ходе проверки?
9. Как проверяется корректность фильтрации на межсетевых экранах и правил трансляции адресов?
10. Кто утверждает итоговый акт комплексной проверки, и какие приложения к нему оформляются?

РАЗДЕЛ 11. ЭКСПЛУАТАЦИОННАЯ ДОКУМЕНТАЦИЯ И ОТЧЁТНОСТЬ ПО РЕЗУЛЬТАТАМ ОБСЛУЖИВАНИЯ

Тема 11.1. Состав и порядок ведения эксплуатационной документации для защищённых АИС
1. Каков перечень обязательных эксплуатационных документов для защищённой АИС?
2. Какие формы журналов учёта средств защиты и протоколов технического обслуживания применяются?
3. Как оформляются акты проверок и отчёты о восстановлении работоспособности?
4. Какие сведения должны содержаться в карточке учёта сетевого оборудования?
5. Каков порядок ведения электронного и бумажного документооборота в защищенной системе?
6. Каковы сроки хранения эксплуатационной документации и порядок её архивации?
7. Как производится присвоение грифов секретности или конфиденциальности документам?
8. Каков порядок корректировки и внесения изменений в эксплуатационную документацию?
9. Каков порядок уничтожения устаревших документов и копий в защищенной системе?
10. Кто несет персональную ответственность за ведение эксплуатационной документации в подразделении?

ВОПРОСЫ ДЛЯ САМОПОДГОТОВКИ

РАЗДЕЛ 3. МОНИТОРИНГ И ДИАГНОСТИКА СОСТОЯНИЯ СЕТЕВЫХ КОМПОНЕНТОВ

Самостоятельная работа по теме «Сравнительный анализ бесплатных и коммерческих систем мониторинга (Zabbix, Nagios, PRTG)»
1. Каковы ключевые функциональные различия между системами мониторинга Zabbix, Nagios и PRTG?
2. Какие типы источников данных и методы сбора информации поддерживаются в Zabbix, Nagios и PRTG?
3. В чем заключаются преимущества и недостатки использования агентного и безагентного мониторинга в каждой из рассматриваемых систем?
4. Каковы архитектурные особенности построения Zabbix, Nagios и PRTG (сервер-агент, распределённый мониторинг)?
5. Как реализуется механизм оповещений (алертинга) в каждой из систем, и какие каналы уведомлений поддерживаются?
6. Какие показатели производительности и доступности сети могут быть измерены с помощью Zabbix, Nagios и PRTG?
7. Каковы лицензионные политики и модели ценообразования для Zabbix, Nagios и PRTG?
8. Каковы требования к ресурсам (CPU, RAM, дисковое пространство) для развертывания каждой системы мониторинга

в корпоративной сети?
9. Как реализуется визуализация данных (графики, дашборды, карты сети) в сравниваемых системах?
10. Какие критерии выбора системы мониторинга являются определяющими для защищённых автоматизированных систем?

РАЗДЕЛ 4. ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ТЕКУЩИЙ РЕМОНТ СЕТЕВОГО ОБОРУДОВАНИЯ

Самостоятельная работа по теме «Анализ типовых отказов сетевого оборудования и способы их предотвращения»
1. Каковы наиболее распространённые причины отказов коммутаторов и маршрутизаторов в корпоративных сетях?
2. Какие типовые отказы оптических модулей (SFP, SFP+) и оптических кабелей встречаются на практике?
3. Каковы основные причины перегрева активного сетевого оборудования и как их предотвратить?
4. Какие методы защиты от скачков напряжения и электропитания применяются для предотвращения отказов оборудования?
5. Как износ вентиляторов и систем охлаждения влияет на отказоустойчивость сетевых устройств?
6. Какие признаки указывают на деградацию портов коммутатора или маршрутизатора?
7. Каковы типовые ошибки конфигурирования, приводящие к программным сбоям сетевого оборудования?
8. Какие профилактические меры позволяют предотвратить повреждение файловой системы на сетевых устройствах?
9. Как влияет запылённость и влажность в серверных помещениях на надёжность работы сетевого оборудования?
10. Какие стратегии резервирования (аппаратного и программного) наиболее эффективны для предотвращения отказов?

РАЗДЕЛ 7. АДМИНИСТРИРОВАНИЕ В УСЛОВИЯХ ДЕЙСТВИЯ УГРОЗ (ОБНАРУЖЕНИЕ АТАК И РЕАГИРОВАНИЕ)

Самостоятельная работа по теме «Обзор современных угроз для корпоративных сетей и методов их обнаружения (MITRE ATT&CK для сетей)»
1. Что представляет собой матрица MITRE ATT&CK, и какова её структура применительно к сетевым угрозам?
2. Какие тактики (Tactics) и техники (Techniques) MITRE ATT&CK наиболее актуальны для сетевого уровня?
3. Каковы современные типы сетевых атак (APT, Ransomware, DDoS, атаки на маршрутизацию) и их особенности?
4. Как методы MITRE ATT&CK используются для разработки сигнатур систем обнаружения вторжений (IDS/IPS)?
5. Какие индикаторы компрометации (IOC) на сетевом уровне позволяют выявить атаки класса APT?
6. Как обнаруживаются атаки методом «человек посередине» (MiTM) и спуфинг (ARP, DNS) в корпоративной сети?
7. Какие методы противодействия атакам на уровне протоколов маршрутизации (BGP, OSPF) описаны в MITRE ATT&CK?
8. Как технологии машинного обучения и поведенческого анализа интегрируются с методами обнаружения MITRE ATT&CK?
9. Каковы этапы жизненного цикла атаки (Cyber Kill Chain) и их соотнесение с тактиками MITRE ATT&CK?
10. Как адаптируется матрица MITRE ATT&CK для защиты сетей в защищённом исполнении и государственных информационных систем?

Самостоятельная работа по теме «Сравнение протоколов VRRP и HSRP: особенности реализации в разных вендорских ОС»
1. Каковы основные принципы работы протоколов VRRP и HSRP для резервирования шлюзов?
2. В чем заключаются ключевые различия между протоколами VRRP (стандарт IETF) и HSRP (проприетарный протокол Cisco)?
3. Как реализована поддержка VRRP и HSRP в операционных системах различных вендоров (Cisco, Juniper, Huawei, Extreme)?
4. Какие параметры (приоритет, таймеры, отслеживание интерфейсов) настраиваются по-разному в VRRP и HSRP?
5. Как происходит процесс выбора активного шлюза (Master/Active) в протоколах VRRP и HSRP?
6. Каковы особенности работы протоколов в режимах отслеживания объектов (Object Tracking) в разных ОС?
7. Какие механизмы аутентификации поддерживаются в VRRP и HSRP, и как они влияют на безопасность?
8. Каковы ограничения по количеству групп и виртуальных маршрутизаторов в различных реализациях VRRP и HSRP?
9. Как осуществляется аварийное переключение (failover) и обратное переключение (preemption) в сравниваемых протоколах?
10. Как совмещаются протоколы VRRP/HSRP с технологиями балансировки нагрузки (GLBP) и динамической маршрутизации?

РАЗДЕЛ 8. КОМПЛЕКСНОЕ АДМИНИСТРИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Самостоятельная работа по теме «Интеграция межсетевых экранов, NAT и политик фильтрации в условиях виртуализированных и программно-определяемых сетей (VPLS/MPLS L3VPN и SDN)»
1. Каковы особенности размещения межсетевых экранов в архитектуре VPLS и MPLS L3VPN?
2. Как реализуется трансляция сетевых адресов (NAT) в программно-определяемых сетях (SDN) и виртуализированных средах?
3. Какие политики фильтрации применяются на стыках между виртуальными частными сетями VPLS и L3VPN?
4. Как интеграция SDN-контроллеров влияет на управление политиками безопасности и фильтрацию трафика?
5. Какие вызовы возникают при настройке межсетевых экранов в среде с динамической маршрутизацией MPLS?
6. Как осуществляется сегментация трафика и изоляция пользователей в VPLS/MPLS сетях с использованием политик

фильтрации?
7. Каковы методы централизованного управления политиками безопасности в SDN-архитектурах?
8. Как обеспечивается совместимость межсетевых экранов с протоколами туннелирования в VPLS и L3VPN?
9. Какие риски безопасности связаны с внедрением NAT в виртуализированных сетевых средах?
10. Как организовать мониторинг и аудит политик фильтрации в условиях динамически меняющейся топологии SDN/VPLS/MPLS?

РАЗДЕЛ 9. ПЛАНОВОЕ ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ТЕКУЩИЙ РЕМОНТ В ЗАЩИЩЁННОЙ АИС

Самостоятельная работа по теме «Организация технического обслуживания и восстановления оборудования в защищённых автоматизированных информационных системах»
1. Какие дополнительные требования предъявляются к организации технического обслуживания в защищённых АИС по сравнению с обычными системами?
2. Как оформляется допуск персонала к проведению ремонтных работ в зоне с ограниченным доступом?
3. Каковы особенности планирования регламентных окон в системах с непрерывным производственным циклом?
4. Как осуществляется резервирование критических функций на период проведения технического обслуживания в защищённой системе?
5. Какие меры предпринимаются для сохранения целостности и конфиденциальности данных при замене оборудования?
6. Как организуется взаимодействие с подразделениями безопасности при проведении внеплановых восстановительных работ?
7. Каков порядок ввода в эксплуатацию оборудования после замены с подтверждением всех параметров защищённости?
8. Какие документы строгой отчётности оформляются при проведении ТО в защищённой АИС?
9. Как обеспечивается сохранность криптографических ключей и сертификатов при плановой замене сетевых устройств?
10. Каков порядок действий при обнаружении признаков несанкционированного доступа во время технического обслуживания?

РАЗДЕЛ 11. ЭКСПЛУАТАЦИОННАЯ ДОКУМЕНТАЦИЯ И ОТЧЁТНОСТЬ ПО РЕЗУЛЬТАТАМ ОБСЛУЖИВАНИЯ

Самостоятельная работа по теме «Разработка шаблонов всех необходимых эксплуатационных документов для гипотетической АИС в защищённом исполнении»
1. Какие виды эксплуатационных документов являются обязательными для гипотетической АИС в защищённом исполнении?
2. Какова структура и обязательные разделы шаблона журнала учёта средств вычислительной техники и сетевых устройств?
3. Какие сведения должны содержаться в шаблоне паспорта сетевого устройства для защищённой системы?
4. Как разработать шаблон протокола технического обслуживания с учётом требований режима защищённости?
5. Какие графы должны присутствовать в журнале регистрации отказов и неисправностей сетевого оборудования?
6. Какова структура шаблона акта проверки технического состояния компонентов АИС?
7. Какие разделы должен содержать шаблон отчёта о восстановлении работоспособности после аварийного отказа?
8. Как разработать шаблон журнала учёта ключевых носителей и средств криптографической защиты?
9. Какие требования к грифам секретности и конфиденциальности должны быть учтены при разработке шаблонов документов?
10. Какой порядок согласования и утверждения разработанных шаблонов эксплуатационных документов в организации?

ЗАДАНИЯ ДЛЯ ПРАКТИЧЕСКИХ И ЛАБОРАТОРНЫХ РАБОТ

РАЗДЕЛ 1. БАЗОВЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ И ЭКСПЛУАТАЦИИ КОМПЬЮТЕРНЫХ СЕТЕЙ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Лабораторная работа №1
Тема: «Изучение состава эксплуатационной документации и сетевых конфигураций»
Задания:
1. Ознакомьтесь с предоставленным комплектом эксплуатационной документации на сетевой сегмент автоматизированной системы. Определите, какие типы документов входят в комплект (руководство администратора, руководство пользователя, инструкции по техническому обслуживанию, регламенты, паспорта оборудования).
2. Изучите раздел «Сетевые параметры» в руководстве администратора. Сопоставьте описанные в документации настройки сетевых интерфейсов (IP-адреса, маски подсети, шлюзы) с реальными параметрами, отображёнными в консоли управления сетевым оборудованием (например, на коммутаторах Eltex или Qtech).
3. По данным из паспортов средств вычислительной техники и сетевых устройств составьте перечень оборудования с указанием его серийных номеров, версий прошивок и дат ввода в эксплуатацию.
4. Используя руководство по техническому обслуживанию, определите регламентные сроки замены расходных материалов (вентиляторов, блоков питания) для каждого типа устройств в сегменте.
5. На основе инструкции по техническому обслуживанию составьте чек-лист ежедневного внешнего осмотра оборудования с указанием контролируемых индикаторов.
6. Найдите в документации описание процедуры резервного копирования конфигураций. Зафиксируйте, какие протоколы (TFTP, FTP, SCP) и периодичность копирования предписаны регламентом.
7. Сопоставьте реальные настройки VLAN на коммутаторе с топологической схемой, приведённой в документации.

Отметьте все несоответствия (при их наличии).
8. Ознакомьтесь с разделом документации, регламентирующим порядок действий при сбоях. Выпишите алгоритмы локализации неисправностей для физического, канального и сетевого уровней.
9. Изучите журнал учёта оборудования. Проверьте, все ли устройства, перечисленные в паспортах, занесены в журнал, и соответствуют ли данные в журнале фактическим.
10. Составьте краткую опись эксплуатационной документации для данного сегмента сети с указанием, какой документ за какой компонент системы отвечает.
Практическая работа №1
Тема: «Анализ топологии и состава оборудования корпоративной сети по документации»
Задания:
1. По предоставленной эксплуатационной документации (схемам связей, описанию сегментов) восстановите логическую схему корпоративной сети в виде графа, указав все узлы и каналы связи.
2. На восстановленной схеме выделите критические узлы (точки отказа, приводящие к потере связности больших сегментов) и критические каналы связи.
3. Определите, какое оборудование является резервным, а какое — основным. Оцените достаточность резервирования для обеспечения бесперебойной работы.
4. На основе документации составьте таблицу соответствия между сетевыми адресами (подсетями) и функциональными сегментами (отделы, серверные зоны, сегменты с разным уровнем конфиденциальности).
5. Проанализируйте, какие протоколы динамической маршрутизации (OSPF, BGP) используются в сети согласно документации, и на каких устройствах они настроены.
6. Оцените пропускную способность каналов связи, указанную в документации. Определите, какие каналы являются «узкими местами» при максимальной нагрузке.
7. На основе документации по системе защиты информации (СЗИ) определите, в каких точках сети установлены межсетевые экраны (например, UserGate NGFW, «Континент 4») и какие политики фильтрации на них применяются.
8. Составьте перечень оборудования, которое требует плановой замены в ближайший квартал, на основе паспортов и регламентов технического обслуживания.
9. Разработайте предложения по модернизации топологии для устранения выявленных единых точек отказа, обосновав каждое предложение.
10. Подготовьте краткий аналитический отчёт о структуре сети, её критических элементах и рекомендациях по повышению надёжности.

РАЗДЕЛ 2. ОСНОВЫ АДМИНИСТРИРОВАНИЯ СЕТЕВЫХ ОПЕРАЦИОННЫХ СИСТЕМ И СЛУЖБ

Лабораторная работа №2
Тема: «Установка серверной ОС и настройка базовых сетевых служб (DHCP, DNS)»
Задания:
1. Выполните установку российской серверной операционной системы (например, РЕД ОС «Сервер» или Astra Linux Special Edition) на виртуальную машину с настройкой сетевого интерфейса в соответствии с заданными параметрами (статический IP-адрес, маска подсети, шлюз по умолчанию).
2. Назначьте статический IP-адрес сетевому интерфейсу установленной ОС с использованием штатных средств (командной строки или графических утилит). Проверьте связность с соседними узлами с помощью утилиты ping.
3. Установите и настройте службу DHCP на сервере. Создайте область DHCP (пул адресов) для подсети, указав диапазон адресов, длительность аренды, адрес шлюза и DNS-серверов.
4. Подключите клиентский компьютер (виртуальную машину) к той же сети и настройте его на автоматическое получение IP-адреса. Проверьте факт получения адреса из созданной области с помощью команды ipconfig (или аналога в Linux).
5. Настройте службу DNS: создайте прямую зону для домена, указанного преподавателем. Добавьте A-записи для сервера и клиента.
6. Создайте обратную зону для подсети, в которой находятся ваши сервер и клиент. Добавьте PTR-записи для проверки обратного разрешения имён.
7. С помощью утилиты nslookup (или dig) проверьте разрешение имён в прямых и обратных зонах как с сервера, так и с клиентской машины.
8. Настройте на клиентской машине использование созданного DNS-сервера в качестве предпочтительного. Проверьте, что клиент успешно резолвит имена в вашем домене.
9. С помощью команды netstat (или ss) проанализируйте, какие сетевые порты и службы активны на сервере после настройки DHCP и DNS.
10. Создайте резервную копию конфигурационных файлов служб DHCP и DNS в отдельную директорию.
Практическая работа №2
Тема: «Конфигурирование доменной структуры и групповых политик в Active Directory»
Задания:
1. На сервере под управлением российской ОС (например, РЕД ОС или Astra Linux) установите роль контроллера домена с использованием службы каталогов (ALD Pro или «Альт Домен»).
2. Создайте домен с именем, указанным преподавателем. Настройте базовые параметры домена (имя NetBIOS, режим работы).
3. В созданном домене создайте организационные единицы (OU), соответствующие структуре гипотетической организации (например, «Бухгалтерия», «Отдел кадров», «ИТ-отдел»).
4. В каждой организационной единице создайте по 2-3 учётные записи пользователей с заданными именами и паролями.
5. Создайте группы безопасности (например, «Бухгалтеры», «Кадровики», «Администраторы») и добавьте в них

соответствующих пользователей.
6. Создайте групповую политику (GPO), которая запрещает доступ к панели управления для пользователей из OU «Бухгалтерия». Примените политику к этой OU.
7. Создайте групповую политику, которая назначает единую стартовую страницу в веб-браузере для всех пользователей домена.
8. Проверьте применение созданных групповых политик, зайдя в систему под учётной записью пользователя из OU «Бухгалтерия» и убедившись, что ограничения действуют.
9. Настройте доверительные отношения с доменом, созданным другим студентом (или с тестовым доменом), используя инструменты управления доверием.
10. Подготовьте отчёт о созданной доменной структуре с указанием созданных OU, пользователей, групп и применённых политик.

РАЗДЕЛ 3. МОНИТОРИНГ И ДИАГНОСТИКА СОСТОЯНИЯ СЕТЕВЫХ КОМПОНЕНТОВ

Лабораторная работа №3
Тема: «Применение диагностических утилит и тестирование кабельной системы»
Задания:
1. С помощью утилиты ping выполните проверку доступности всех основных сетевых устройств (шлюзов, серверов, коммутаторов) в заданном сегменте. Зафиксируйте значения времени отклика (RTT).
2. Выполните трассировку маршрута (tracert/traceroute) до внешнего узла (например, до сервера в другой подсети). Проанализируйте полученный путь и определите количество переходов (hops).
3. Используя утилиту pathping, оцените потери пакетов на каждом участке маршрута до удалённого узла. Определите участки с наибольшими потерями.
4. Настройте SNMP-клиент для опроса одного из коммутаторов (например, Eltex или Qtech) и получите значения счётчиков трафика на всех портах.
5. Проанализируйте полученные SNMP-данные: определите порты с наибольшей загрузкой и порты с большим количеством ошибок (CRC-ошибки, коллизии).
6. С помощью тестера витой пары (кабельного анализатора) выполните проверку целостности кабеля, соединяющего два сетевых устройства. Измерьте затухание сигнала и определите длину кабеля.
7. Проверьте правильность обжима коннекторов RJ-45 на тестовом патч-корде с помощью тестера. Определите, соответствует ли распиновка стандарту TIA/EIA-568B.
8. С помощью оптического тестера или рефлектометра (OTDR) выполните измерение затухания в оптическом патч-корде (если доступно оборудование). Сравните полученные значения с нормативными.
9. Используя консольные команды на коммутаторе, проверьте состояние портов (up/down), скорость и дуплексный режим. Выявите порты с нестандартными настройками.
10. Составьте протокол первичной проверки физической целостности линий, включив в него результаты всех выполненных измерений и выявленные несоответствия.
Практическая работа №3
Тема: «Разработка протокола мониторинга ключевых сетевых узлов»
Задания:
1. На основе схемы сети определите перечень ключевых контрольных точек (узлов и каналов), мониторинг которых обязателен для обеспечения бесперебойной работы.
2. Для каждой контрольной точки задайте пороговые значения критических показателей: доступность (время отклика), загрузка канала (в процентах), процент потерь пакетов.
3. Разработайте форму протокола мониторинга, в которой будут предусмотрены поля для фиксации: даты и времени проверки, имени узла, значений всех контролируемых параметров, отметки о превышении порогов.
4. На основе предложенной периодичности проверок (например, ежечасно, ежедневно) составьте график мониторинга для каждого типа узлов (критические — чаще, второстепенные — реже).
5. Заполните разработанный протокол за одни сутки, используя гипотетические (или реальные, полученные в лабораторной работе) данные мониторинга.
6. Проанализируйте заполненный протокол: выявите узлы, где были превышены пороговые значения, и укажите возможные причины.
7. Предложите корректировку пороговых значений для тех узлов, где, по вашему мнению, они были установлены неоправданно жёстко или слишком мягко.
8. Разработайте порядок действий оператора при получении сигнала о превышении порога для каждого типа инцидента (недоступность, перегрузка, потери).
9. Оформите итоговый документ «Протокол мониторинга ключевых сетевых узлов» с приложением графика проверок и порядка действий при инцидентах.
10. Подготовьте краткую памятку для дежурного администратора по заполнению журнала мониторинга.

РАЗДЕЛ 4. ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ТЕКУЩИЙ РЕМОНТ СЕТЕВОГО ОБОРУДОВАНИЯ

Лабораторная работа №4
Тема: «Проведение планового ТО коммутатора и восстановление конфигурации из резервной копии»
Задания:
1. Выполните внешний осмотр коммутатора: проверьте целостность корпуса, состояние индикаторов (LED) и наличие посторонних звуков от вентиляторов.
2. Остановите коммутатор, выполните чистку внутренних компонентов от пыли с использованием сжатого воздуха

(симулируйте процесс). Проверьте состояние вентиляционных решёток.
3. Подключитесь к коммутатору через консольный порт и выполните резервное копирование текущей конфигурации (startup-config или running-config) на TFTP-сервер (например, на базе российской ОС).
4. Сохраните резервную копию конфигурации также в текстовом файле на локальном компьютере для последующего анализа.
5. Выполните сброс коммутатора к заводским настройкам (erase startup-config или аналог) и перезагрузите устройство.
6. После перезагрузки восстановите конфигурацию коммутатора из ранее сохранённой резервной копии (через TFTP или копированием текста).
7. Проверьте, что все настройки (VLAN, IP-адреса, порты) восстановлены корректно. Выполните проверку связности с соседними устройствами.
8. Проверьте целостность файла прошивки (образ операционной системы) коммутатора с помощью встроенной команды проверки контрольной суммы (например, verify или аналог).
9. Настройте автоматическое резервное копирование конфигурации коммутатора на сервер по расписанию (симулируйте настройку cron или планировщика задач на сервере).
10. Заполните протокол проведённого технического обслуживания, указав все выполненные действия, выявленные замечания и результат проверки работоспособности.
Практическая работа №4
Тема: «Разработка графика ТО и плана аварийного восстановления для сегмента сети»
Задания:
1. На основе эксплуатационной документации на оборудование сегмента сети определите нормативные сроки и объёмы всех видов технического обслуживания (ежедневного, еженедельного, планово-предупредительного).
2. Рассчитайте трудоёмкость каждого вида ТО (в человеко-часах) для всего сегмента, учитывая количество единиц оборудования каждого типа.
3. Составьте годовой график проведения планово-предупредительных работ с указанием дат, видов работ и ответственных исполнителей.
4. Для каждого типа оборудования (коммутатор, маршрутизатор, сервер) разработайте пошаговый план (алгоритм) действий при типичных отказах: зависание, сбой питания, ошибка конфигурации.
5. Разработайте план аварийного восстановления для случая выхода из строя основного маршрутизатора сегмента с использованием резервного оборудования.
6. Оцените время восстановления (MTTR) для каждого сценария отказа, исходя из разработанных планов.
7. Определите критичность каждого узла сегмента и назначьте приоритеты восстановления (какие узлы восстанавливать в первую очередь).
8. Составьте список необходимых запасных частей и расходных материалов, которые должны храниться на складе для оперативного восстановления.
9. Разработайте форму акта о выполненном ремонте и восстановлении работоспособности для данного сегмента.
10. Подготовьте итоговый документ, включающий график ТО, планы восстановления для типовых отказов и перечень ЗИП (запасных частей и принадлежностей).

РАЗДЕЛ 5. АДМИНИСТРИРОВАНИЕ ЗАЩИЩЕННЫХ СЕТЕВЫХ СОЕДИНЕНИЙ И СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ

Лабораторная работа №5
Тема: «Настройка VPN-соединения на базе IPsec между двумя сегментами сети»
Задания:
1. На двух пограничных шлюзах (например, на основе российской ОС или на VPN-шлюзах ViPNet Coordinator) настройте базовые сетевые параметры интерфейсов для соединения с двумя разными сегментами.
2. Создайте политики безопасности IPsec для защиты трафика между этими двумя сегментами. Определите, какие сети будут шифроваться.
3. Настройте параметры фазы 1 (IKE): метод аутентификации (предварительный ключ или сертификаты), алгоритмы шифрования и хеширования, группу Диффи-Хеллмана.
4. Настройте параметры фазы 2 (IPsec): алгоритмы шифрования (например, ГОСТ 28147-89 при использовании российских СКЗИ) и аутентификации, время жизни ключей.
5. Выполните проверку установленного IPsec-соединения, используя встроенные команды мониторинга VPN (например, show crypto isakmp sa, show crypto ipsec sa).
6. Запустите захват трафика с помощью Wireshark на интерфейсе между шлюзами и убедитесь, что трафик между сегментами передаётся в зашифрованном виде (ESP-пакеты).
7. Проверьте доступность ресурсов в удалённом сегменте (ping, доступ к общим папкам) через установленный VPN-туннель.
8. Сымитируйте сбой одного из шлюзов (отключите его сетевой интерфейс) и проверьте, как поведёт себя VPN-соединение (при наличии резервирования).
9. Проанализируйте логи VPN-шлюза на предмет ошибок при установке соединения. Определите типовые причины неудачных подключений.
10. Создайте резервную копию конфигурации VPN-шлюзов, включая параметры IPsec и ключевую информацию (при работе с симуляцией).
Практическая работа №5
Тема: «Разработка схемы криптозащиты для распределённой АИС с несколькими филиалами»
Задания:
1. На основе предоставленной схемы распределённой АИС (головной офис и 3-4 филиала) определите, какие типы VPN

-соединений (site-to-site, удалённый доступ) требуются для каждого филиала.
2. Для каждого филиала выберите тип VPN-шлюза (например, ViPNet Coordinator, аппаратный или программный) с учётом требуемой производительности и численности пользователей.
3. Составьте таблицу распределения ключевой информации: для каждой пары «шлюз-шлюз» укажите используемые ключи (или идентификаторы сертификатов), алгоритмы шифрования и хеширования.
4. Разработайте политики безопасности для каждого VPN-соединения: какие подсети и сервисы доступны через туннель, а какие нет.
5. Оцените, как изменится пропускная способность каналов связи после внедрения шифрования (с учётом накладных расходов IPsec). Рассчитайте примерную полезную скорость для каждого канала.
6. Определите, какие нормативные требования (приказы ФСТЭК, требования к СКЗИ) необходимо выполнить при выборе и настройке средств криптозащиты для данной АИС.
7. Разработайте схему резервирования VPN-шлюзов в головном офисе для обеспечения отказоустойчивости.
8. Составьте инструкцию для администратора филиала по первоначальной настройке VPN-шлюза и проверке работоспособности туннеля.
9. Опишите порядок действий при компрометации ключевой информации: как производится отзыв ключей и генерация новых.
10. Подготовьте итоговый документ «Схема криптозащиты распределённой АИС», включающий топологию VPN, таблицу ключей и политик, а также инструкции по администрированию.

РАЗДЕЛ 6. ОБЕСПЕЧЕНИЕ БЕСПЕРЕБОЙНОЙ РАБОТЫ СЕТЕЙ (ОТКАЗОУСТОЙЧИВОСТЬ И БЕКАП)

Лабораторная работа №6
Тема: «Настройка резервного шлюза по протоколу VRRP и автоматическое резервирование конфигураций»
Задания:
1. На двух маршрутизаторах (или L3-коммутаторах, например, Eltex) настройте интерфейсы, подключённые к общей подсети клиентов, с разными IP-адресами.
2. На обоих маршрутизаторах настройте протокол VRRP: создайте виртуальный маршрутизатор (VRID), назначьте виртуальный IP-адрес, установите приоритеты (основной — выше, резервный — ниже).
3. Настройте параметры отслеживания (tracking) интерфейса на основном маршрутизаторе, чтобы при отказе uplink-интерфейса его приоритет автоматически понижался.
4. Выполните проверку: с клиентского компьютера выполните ping на виртуальный IP-адрес и убедитесь, что ответ приходит.
5. Сымитируйте отказ основного маршрутизатора (отключите его или выключите интерфейс в подсети клиентов). Проверьте, что клиент продолжает получать ответы на ping виртуального адреса (переключение произошло).
6. После восстановления основного маршрутизатора проверьте, произошло ли обратное переключение (preemption) согласно настройкам приоритетов.
7. Настройте автоматическое резервное копирование конфигураций обоих маршрутизаторов на центральный сервер с использованием SCP или TFTP по расписанию (например, ежедневно).
8. Сымитируйте потерю конфигурации на одном из маршрутизаторов и восстановите её из резервной копии с сервера.
9. Проанализируйте журналы событий (syslog) маршрутизаторов, чтобы убедиться, что переключения VRRP и резервное копирование фиксируются корректно.
10. Задокументируйте настройки VRRP и автоматического резервирования, включая параметры приоритетов, таймеров и отслеживания.
Практическая работа №6
Тема: «Расчёт показателей доступности сети при внедрении резервирования»
Задания:
1. Для заданного сегмента сети определите значения MTBF (средняя наработка на отказ) и MTTR (среднее время восстановления) для каждого типа оборудования на основе документации.
2. Рассчитайте коэффициент доступности (Availability) для сегмента без резервирования, используя формулу A = MTBF / (MTBF + MTTR).
3. Рассчитайте коэффициент доступности для того же сегмента при внедрении резервирования (два маршрутизатора в кластере VRRP/HSRP), учитывая, что отказ одного устройства не приводит к недоступности.
4. Сравните полученные значения доступности и определите, на сколько процентов повысилась доступность после внедрения резервирования.
5. Рассчитайте ожидаемое время простоя (downtime) в год для обоих вариантов (без резервирования и с резервированием).
6. Оцените экономический эффект от внедрения резервирования, если известна стоимость часа простоя сети для организации.
7. Рассмотрите сценарий резервирования каналов связи (два разных провайдера). Рассчитайте доступность при использовании двух независимых каналов.
8. Сравните различные варианты резервирования (оборудование, каналы, электропитание) по критерию «стоимость / прирост доступности».
9. На основе расчётов обоснуйте выбор наиболее эффективного варианта резервирования для данного сегмента сети.
10. Оформите отчёт с расчётами показателей доступности, выводами и рекомендациями по выбору схемы резервирования.

РАЗДЕЛ 7. АДМИНИСТРИРОВАНИЕ В УСЛОВИЯХ ДЕЙСТВИЯ УГРОЗ (ОБНАРУЖЕНИЕ АТАК И РЕАГИРОВАНИЕ)

Лабораторная работа №7
Тема: «Настройка IDS на базе Snort и отработка сценария блокировки атакующего хоста»
Задания:
1. Установите систему обнаружения вторжений Snort на выделенном сервере (или виртуальной машине) в режиме NIDS (Network IDS) с использованием российской ОС (например, РЕД ОС или Astra Linux).
2. Настройте Snort для захвата трафика на сетевом интерфейсе в режиме promiscuous (прослушивание). Убедитесь, что Snort запущен и обрабатывает пакеты.
3. Создайте простое правило Snort для обнаружения ICMP-эхо-запросов (ping) с определённого IP-адреса (или с любого адреса) и генерации предупреждения (alert).
4. Запустите сканирование портов с помощью утилиты nmap с тестового хоста в направлении защищаемого сегмента. Проанализируйте предупреждения, сгенерированные Snort.
5. Создайте правило Snort для обнаружения атаки типа «SYN-flood» (множество SYN-пакетов с одного источника за короткое время).
6. Сымитируйте атаку SYN-flood с помощью специализированной утилиты (например, hping3) и убедитесь, что Snort фиксирует это событие.
7. Настройте на коммутаторе (например, Eltex) ACL (Access Control List) для блокировки трафика с IP-адреса атакующего хоста, обнаруженного Snort.
8. Проверьте, что после применения ACL трафик с атакующего хоста действительно блокируется на коммутаторе (повторите ping или сканирование).
9. Проанализируйте журналы (логи) Snort и определите, какие типы атак были зафиксированы в процессе работы.
10. Составьте отчёт о настройке IDS, созданных правилах и результатах тестирования блокировки.
Практическая работа №7
Тема: «Разработка плана реагирования на типовые сетевые инциденты (DoS, сканирование, подбор паролей)»
Задания:
1. Для каждого типа инцидента (DoS-атака, сканирование портов, подбор паролей к сетевым сервисам) разработайте поэтапный план действий по обнаружению, локализации и устранению.
2. Для каждого этапа плана определите ответственных лиц (роли) и предельные сроки выполнения действий.
3. Разработайте форму первичного уведомления об инциденте, которая должна заполняться оператором при обнаружении признаков атаки.
4. Определите, какие сетевые журналы и артефакты (pcap-файлы, логи IDS/IPS, логи межсетевого экрана) необходимо сохранить для каждого типа инцидента.
5. Разработайте шаблон отчёта о расследовании инцидента, включив в него разделы: описание инцидента, действия по локализации, собранные доказательства, выводы и рекомендации.
6. Опишите порядок взаимодействия с отделом информационной безопасности и руководством при возникновении инцидента (эскалация).
7. Разработайте процедуру пост-инцидентного анализа: какие меры должны быть приняты для предотвращения подобных инцидентов в будущем.
8. Составьте чек-лист действий администратора при обнаружении DoS-атаки (от первичного обнаружения до полного восстановления сервиса).
9. Определите, какие средства российского производства (например, UserGate NGFW с IDS/IPS, ViPNet IDS HS) могут быть задействованы на каждом этапе реагирования.
10. Оформите итоговый документ «План реагирования на сетевые инциденты» для гипотетической организации, включив все разработанные процедуры и шаблоны.

РАЗДЕЛ 8. КОМПЛЕКСНОЕ АДМИНИСТРИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Лабораторная работа №8
Тема: «Настройка политик доступа на пограничном маршрутизаторе и проверка VLAN-изоляции»
Задания:
1. На пограничном маршрутизаторе (например, на базе российской ОС или на оборудовании Qtech) настройте интерфейсы для подключения к нескольким VLAN.
2. Создайте расширенные списки доступа (ACL), которые разрешают доступ из VLAN «Бухгалтерия» только к серверу баз данных и запрещают доступ в другие VLAN.
3. Создайте ACL, которые разрешают доступ из VLAN «ИТ-отдел» ко всем ресурсам сети, но запрещают доступ в сегмент управления сетевым оборудованием (management VLAN).
4. Примените созданные ACL к интерфейсам VLAN на маршрутизаторе (входящему или исходящему трафику).
5. Выполните проверку изоляции: с тестового хоста в VLAN «Бухгалтерия» попытайтесь получить доступ к хосту в другой VLAN (например, через ping или telnet). Убедитесь, что доступ запрещён.
6. С тестового хоста в VLAN «ИТ-отдел» проверьте доступ к разрешённым и запрещённым ресурсам согласно настроенным ACL.
7. Настройте статическую маршрутизацию на пограничном маршрутизаторе для направления трафика из внутренних VLAN в сторону шлюза системы защиты информации (СЗИ).
8. Проверьте, что трафик из внутренних сегментов проходит через шлюз СЗИ (например, через межсетевой экран «Континент 4» или UserGate NGFW) с помощью трассировки маршрута.
9. Проанализируйте журналы межсетевого экрана на предмет фиксации попыток несанкционированного доступа между VLAN.

10. Задокументируйте созданные ACL, правила маршрутизации и результаты проверки изоляции VLAN.
Практическая работа №8
Тема: «Проектирование сетевой архитектуры АИС с учётом требований к защищённым сегментам»
Задания:
1. На основе требований технического задания разработайте логическую схему сети АИС, включающую сегменты с разными уровнями конфиденциальности (например, общедоступный, для служебного пользования, секретный).
2. Разработайте схему IP-адресации для всех сегментов сети, предусмотрев резерв адресов для расширения. Используйте частные адреса из диапазонов RFC 1918.
3. Определите точки размещения средств контроля доступа (межсетевых экранов) на стыках между сегментами с разными уровнями конфиденциальности.
4. Обоснуйте выбор сетевого оборудования (коммутаторов, маршрутизаторов, VPN-шлюзов) для каждого сегмента с учётом требований к защищённости и производительности.
5. Разработайте схему резервирования критических узлов (основных маршрутизаторов, межсетевых экранов) для обеспечения отказоустойчивости.
6. Определите, какие средства криптографической защиты (например, ViPNet) необходимо установить для защиты каналов связи между удалёнными сегментами.
7. Разработайте политики фильтрации (ACL) для межсетевых экранов на стыках сегментов, указав разрешённые и запрещённые потоки трафика.
8. Оцените стоимость реализации предложенной архитектуры (приблизительно) на основе рыночных цен на оборудование и ПО.
9. Подготовьте обоснование выбора каждого компонента архитектуры с точки зрения соответствия требованиям ФСТЭК и других регуляторов.
10. Оформите итоговый проект «Сетевая архитектура защищённой АИС», включив логическую схему, схему адресации, спецификацию оборудования и политики безопасности.

РАЗДЕЛ 9. ПЛАНОВОЕ ТЕХНИЧЕСКОЕ ОБСЛУЖИВАНИЕ И ТЕКУЩИЙ РЕМОНТ В ЗАЩИЩЁННОЙ АИС

Лабораторная работа №9
Тема: «Замена сетевого оборудования с переносом ключей и проверкой работоспособности СЗИ»
Задания:
1. На тестовом стенде сымитируйте замену вышедшего из строя маршрутизатора (или VPN-шлюза) на новое устройство того же типа.
2. Перенесите конфигурацию с отказавшего устройства на новое (из резервной копии или путём ручного ввода). Убедитесь, что все сетевые параметры (IP-адреса, маршруты, ACL) скопированы корректно.
3. Выполните перенос ключевой информации (предварительных ключей IPsec, сертификатов) с отказавшего устройства на новое, используя штатные средства (например, экспорт/импорт ключевых контейнеров).
4. После замены выполните синхронизацию системного времени на новом устройстве с сервером точного времени (NTP).
5. Проверьте целостность программного обеспечения на новом устройстве, сверив контрольные суммы файлов прошивки с эталонными значениями.
6. Проверьте прохождение защищённого трафика через новый шлюз: установите IPsec-соединение с удалённым узлом и проверьте доступность ресурсов за туннелем.
7. Проверьте, что СЗИ (например, встроенный межсетевой экран или антивирусный модуль) на новом устройстве работает корректно и не блокирует легитимный трафик.
8. Заполните акт замены оборудования, указав причину замены, серийные номера старого и нового устройств, выполненные операции по переносу конфигурации и ключей.
9. Проанализируйте журналы безопасности нового устройства на предмет ошибок или предупреждений, возникших после замены.
10. Составьте инструкцию по безопасной замене аналогичного оборудования в действующей защищённой сети, указав все критические моменты.
Практическая работа №9
Тема: «Составление регламента выполнения планового ТО для сегмента сети с критической информацией»
Задания:
1. Определите состав сегмента сети с критической информацией (перечень оборудования, ПО, каналов связи).
2. Определите перечень всех необходимых видов технического обслуживания для данного сегмента с учётом требований защищённости (ограничение доступа, необходимость оформления допусков).
3. Для каждого вида ТО опишите пошаговый порядок действий, включая подготовительные мероприятия (согласование времени, оповещение пользователей, резервирование).
4. Рассчитайте длительность каждого регламентного окна, необходимого для выполнения ТО, с учётом времени на согласования и оформление допусков.
5. Разработайте график ТО на полугодие, указав конкретные даты и время начала/окончания работ.
6. Разработайте порядок действий при обнаружении нештатных ситуаций во время проведения ТО (например, отказ оборудования в процессе обслуживания).
7. Определите состав комиссии по приёмке оборудования после ТО и критерии успешного завершения работ.
8. Разработайте формы документов, которые должны заполняться на каждом этапе ТО (наряд-допуск, протокол обслуживания, акт приёмки).
9. Опишите порядок информирования руководства и подразделения безопасности о проведении ТО и его результатах.
10. Оформите итоговый регламент выполнения планового ТО для сегмента с критической информацией, включив все

разработанные процедуры, графики и формы документов.

РАЗДЕЛ 10. ПРОВЕРКА ТЕХНИЧЕСКОГО СОСТОЯНИЯ И КОНТРОЛЬ РАБОТОСПОСОБНОСТИ АИС

Лабораторная работа №10
Тема: «Измерение параметров кабельной системы с помощью тестера и анализ журналов СЗИ»
Задания:
1. С помощью тестера витой пары (кабельного анализатора) выполните измерения на предоставленном кабеле: определите длину, затухание сигнала, перекос (delay skew) и наличие обрывов/замыканий.
2. Сравните полученные значения с нормативными (например, согласно стандартам TIA/EIA). Определите, соответствует ли кабель требованиям для категории 5e или 6.
3. Если в распоряжении есть оптический рефлектометр (OTDR), выполните измерение затухания и отражений в оптическом кабеле. Постройте рефлектограмму.
4. Проанализируйте полученную рефлектограмму: определите наличие соединителей, сращиваний, изломов и их вклад в общее затухание.
5. Подключитесь к межсетевому экрану (например, UserGate NGFW или «Континент 4») и выполните экспорт системных журналов (логов) за последние 24 часа.
6. Проанализируйте логи межсетевого экрана: найдите записи о блокировках подозрительного трафика, попытках несанкционированного доступа, ошибках аутентификации.
7. Сопоставьте события из логов межсетевого экрана с результатами мониторинга сети (например, с данными SNMP о загрузке каналов) для выявления аномалий.
8. Проверьте целостность журналов аудита СЗИ: убедитесь, что нет пропусков в записях и что все события фиксируются с корректными временными метками.
9. Составьте протокол инструментального контроля кабельной системы, включив в него все измеренные параметры и заключение о соответствии нормам.
10. Подготовьте краткий отчёт по анализу журналов СЗИ, указав выявленные аномалии и рекомендации по их устранению.
Практическая работа №10
Тема: «Разработка программы комплексной проверки технического состояния АИС на квартал»
Задания:
1. На основе состава АИС (сеть, СЗИ, прикладное ПО) определите перечень всех компонентов, подлежащих проверке в рамках комплексной проверки.
2. Для каждого компонента определите виды проверок (инструментальный контроль, функциональное тестирование, проверка целостности, аудит журналов), которые необходимо выполнить.
3. Разработайте график проведения проверок на квартал с разбивкой по неделям, указав, какие компоненты и в какие сроки проверяются.
4. Для каждого вида проверки назначьте ответственного исполнителя (роль) и определите необходимые ресурсы (оборудование, ПО, документация).
5. Определите критические показатели (KPI) для каждого компонента, которые должны быть проверены в ходе комплексной проверки.
6. Разработайте форму итогового акта комплексной проверки, включив в него разделы по каждому компоненту и общее заключение.
7. Составьте перечень типовых отклонений и рекомендаций по их устранению для каждого компонента АИС.
8. Разработайте процедуру оповещения руководства о критических отклонениях, выявленных в ходе проверки.
9. Опишите порядок действий после завершения проверки: устранение замечаний, повторная проверка, утверждение акта.
10. Оформите итоговый документ «Программа комплексной проверки технического состояния АИС на квартал» со всеми приложениями (графики, формы актов, перечни показателей).

РАЗДЕЛ 11. ЭКСПЛУАТАЦИОННАЯ ДОКУМЕНТАЦИЯ И ОТЧЁТНОСТЬ ПО РЕЗУЛЬТАТАМ ОБСЛУЖИВАНИЯ

Практическая работа №11
Тема: «Заполнение комплекта эксплуатационных документов за отчётный период (журнал отказов, акты ТО, отчёт о восстановлении)»
Задания:
1. На основе предоставленных исходных данных (события, произошедшие в сети за месяц) заполните журнал регистрации отказов и неисправностей сетевого оборудования. Укажите дату, время, описание отказа, принятые меры и результат.
2. Используя записи из журнала отказов, составьте акт технического состояния для каждого устройства, которое выходило из строя или требовало обслуживания.
3. На основе актов технического состояния заполните карточки учёта оборудования, внеся в них информацию о проведённых ремонтах и заменах.
4. По данным о проведённых технических обслуживаниях (ежедневных, еженедельных, плановых) заполните протоколы технического обслуживания для каждого типа работ.
5. Для одного из инцидентов (например, замена коммутатора) составьте отчёт о восстановлении работоспособности, указав причину отказа, последовательность действий по восстановлению и время восстановления.
6. На основе всех заполненных документов сформируйте сводный отчёт о техническом состоянии сегмента сети за отчётный период.

7. Проверьте полноту документации: убедитесь, что на каждое оборудование есть актуальные паспорт и карточка учёта, а все отказы зарегистрированы в журнале.
8. Внесите исправления в один из документов (например, измените дату следующего ТО) с соблюдением правил внесения исправлений (зачёркивание, заверение подписью).
9. Подготовьте комплект документов для сдачи в архив в соответствии с требованиями к хранению (сформируйте дело, составьте опись).
10. Проанализируйте заполненные документы и выявите, какие меры необходимо принять для снижения числа отказов в следующем отчётном периоде.

**Оценочные средства промежуточной аттестации:**

КОНТРОЛЬНАЯ РАБОТА (6 СЕМЕСТР)

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении
1. Какие основные топологии компьютерных сетей используются в АИС?
2. Назовите функции протоколов IP, TCP, UDP и ICMP в стеке TCP/IP.
3. Какие эксплуатационные документы ведутся для сетевых компонентов и какие требования к их ведению?

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
4. Какие основные сетевые службы (DHCP, DNS, Active Directory) обеспечивают функционирование корпоративной сети?
5. Какие параметры мониторинга сети определяются с помощью SNMP и системных счётчиков?
6. Что такое SLA и какие показатели в него входят для сетевых служб?
7. Опишите алгоритм диагностики неисправностей по модели OSI (снизу-вверх).

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
8. Какие виды технического обслуживания сетевого оборудования существуют и какова их периодичность?
9. В чем отличие горячей замены компонентов от холодной при восстановлении работоспособности?
10. Каков порядок действий при восстановлении сетевого устройства из резервной копии конфигурации?

КОНТРОЛЬНАЯ РАБОТА (7 СЕМЕСТР)

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении
1. Какие основные протоколы используются для организации защищённых каналов VPN в корпоративной сети?
2. Чем отличаются транспортный и туннельный режимы IPsec и когда каждый применяется?
3. Каков порядок действий при компрометации ключей в системе криптографической защиты (СКЗИ)?
4. Какие методы резервного копирования конфигураций сетевых устройств существуют и какой протокол предпочтителен для безопасного копирования?
5. Для чего служат протоколы VRRP и HSRP и как они повышают отказоустойчивость сети?

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
6. Что такое агрегация каналов (LACP) и как она влияет на пропускную способность и надёжность?
7. В чём разница между системами IDS и IPS, и как они настраиваются для обнаружения атак?
8. Какие типовые сигнатуры используются для обнаружения сетевых сканирований и DoS-атак?

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
9. Назовите основные шаги по изоляции заражённого хоста в сети без отключения остальных узлов.
10. Какие артефакты необходимо сохранять при реагировании на сетевой инцидент и с какой целью?

КОНТРОЛЬНАЯ РАБОТА (8 СЕМЕСТР)

Индикатор ЗНАТЬ

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

1. Установите правильную последовательность действий администратора при внедрении нового серверного оборудования (ОС Windows Server) в защищённую сеть.
А) Назначение статического IP-адреса и настройка DNS-клиента.
Б) Проверка сетевой связности и маршрутов с помощью встроенных утилит.
В) Установка серверной операционной системы с проверкой системных требований.

Г) Настройка локальных политик безопасности и создание учетных записей администраторов.
2. Установите правильную последовательность действий при диагностике отсутствия доступа к удалённому ресурсу по модели OSI «снизу-вверх».
А) Проверка доступности порта и состояния кабеля (физический уровень).
Б) Проверка IP-адресации и таблиц маршрутизации (сетевой уровень).
В) Проверка корректности разрешения доменного имени через DNS (прикладной уровень).
Г) Проверка MAC-адресов и таблиц коммутации (канальный уровень).
3. Установите правильную последовательность этапов планово-предупредительного технического обслуживания (ТО) сетевого оборудования.
А) Внешний осмотр оборудования и проверка световой индикации на предмет ошибок.
Б) Резервирование текущих конфигураций на внешний репозиторий.
В) Обесточивание устройства, чистка внутренних компонентов и замена термопасты (при необходимости).
Г) Проверка источников бесперебойного питания и обновление прошивок.
4. Установите соответствие между топологией компьютерной сети и её ключевой характеристикой.
А) Топология «Шина»
Б) Топология «Кольцо»
В) Топология «Звезда»
Г) Топология «Mesh» (полносвязная)
1. Высокая отказоустойчивость за счёт множества резервных путей.
2. Выход из строя одного устройства не влияет на остальные, но требует концентратора.
3. Наличие маркера для передачи данных и последовательный обход узлов.
4. Все компьютеры подключены к одному общему кабелю, разрыв которого останавливает всю сеть.
5. Используется исключительно для беспроводных соединений.
5. Установите соответствие между протоколом стека TCP/IP и его основной функцией.
А) ARP
Б) ICMP
В) UDP
Г) TCP
1. Установление логического соединения с гарантией доставки и контролем потока.
2. Определение MAC-адреса узла по его известному IP-адресу в локальной сети.
3. Передача сообщений об ошибках маршрутизации и диагностика связности (ping).
4. Обеспечение высокоскоростной передачи данных без установки соединения.
5. Защита передаваемых данных с помощью алгоритмов шифрования.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
6. Установите правильную последовательность административных мер при организации защищённого VPN-соединения на базе IPsec.
А) Генерация ключей и настройка политик аутентификации (IKE).
Б) Проверка работоспособности туннеля и анализ журналов аудита.
В) Выбор режима работы (транспортный или туннельный) и параметров шифрования.
Г) Настройка межсетевого экрана для разрешения прохождения ESP/AH трафика.
7. Установите правильную последовательность процедуры реагирования на инцидент (обнаружение сетевой атаки) в корпоративной сети.
А) Сбор артефактов (журналы, pcap-файлы) и изоляция заражённого хоста.
Б) Оповещение руководства и отдела информационной безопасности об инциденте.
В) Отключение порта коммутатора или блокировка IP-адреса злоумышленника.
Г) Восстановление работоспособности сервисов и анализ уязвимостей.
8. Установите соответствие между видом технического обслуживания (ТО) и перечнем выполняемых работ.
А) Ежедневное ТО
Б) Еженедельное ТО
В) Планово-предупредительное ТО
Г) Аварийное восстановление
1. Чистка вентиляционных отверстий, проверка уровня шума и резервирование конфигураций.
2. Замена термопасты, обновление прошивок и тестирование ИБП.
3. Внешний осмотр индикации и проверка физической целостности кабелей.
4. Оперативная замена модуля или восстановление из резервной копии после сбоя.
5. Установка нового программного обеспечения без отключения пользователей.
9. Установите соответствие между сетевым протоколом/службой и стандартным портом.
А) DHCP
Б) DNS
В) HTTPS
Г) SMB (CIFS)
1. 67 (UDP)
2. 53 (UDP/TCP)
3. 445 (TCP)
4. 443 (TCP)
5. 22 (TCP)

10. Установите соответствие между протоколом маршрутизации/резервирования и его назначением.
А) VRRP
Б) LACP
В) ECMP
Г) OSPF
1. Объединение физических портов в логический канал для увеличения пропускной способности.
2. Распределение трафика между несколькими маршрутами с одинаковой стоимостью.
3. Обеспечение автоматического переключения на резервный шлюз по умолчанию.
4. Динамический обмен информацией о маршрутах внутри автономной системы.
5. Настройка статической маршрутизации между филиалами.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
11. Установите правильную последовательность замены отказавшего коммутатора в защищённой автоматизированной системе с сохранением контура безопасности.
А) Перенос конфигурации и криптографических ключей/сертификатов на новый коммутатор.
Б) Сверка контрольных сумм и проверка целостности сетевых настроек после включения.
В) Оформление наряда-допуска и согласование времени замены с пользователями.
Г) Физическая замена модуля и синхронизация системного времени устройства.
12. Установите правильную последовательность действий при комплексной проверке АИС (сеть + СЗИ) по годовому регламенту.
А) Инструментальный контроль физических параметров среды передачи (тестером кабеля).
Б) Анализ итоговых актов и формирование рекомендаций по устранению отклонений.
В) Тестирование сквозной доступности ресурсов и проверка корректности фильтрации.
Г) Проверка целостности журналов аудита и политик авторизации пользователей.
13. Установите соответствие между средством криптографической защиты (СКЗИ) или его компонентом и описанием функции.
А) Ключевой носитель
Б) Модуль доверенной загрузки
В) Журнал аудита СКЗИ
Г) Сертификат открытого ключа
1. Устройство, содержащее закрытые ключи доступа к защищённому каналу.
2. Фиксация событий генерации, обмена и компрометации ключей.
3. Подтверждение подлинности владельца ключа и его полномочий.
4. Проверка целостности программных модулей перед началом работы системы.
5. Программа для сканирования сетевых портов на предмет уязвимостей.
14. Установите соответствие между действием злоумышленника (типом угрозы) и методом обнаружения в IDS/IPS.
А) DoS-атака (отказ в обслуживании)
Б) Сканирование портов
В) Эксплуатация уязвимости веб-приложения
Г) Атака «человек посередине» (MITM)
1. Сигнатура на большое количество SYN-пакетов с разных адресов.
2. Правило на обнаружение строки SQL-инъекции или XSS в теле запроса.
3. Аномалия в виде несоответствия SSL-сертификата ожидаемому хешу.
4. Сигнатура на последовательные подключения к закрытым портам за короткое время.
5. Фильтрация исходящего трафика по портам электронной почты.
15. Установите соответствие между архитектурным решением в защищённой АИС и его назначением.
А) Сегментация сети по уровням конфиденциальности
Б) Трансляция адресов (NAT)
В) Резервирование источников питания (ИБП)
Г) Интеграция с SIEM-системой
1. Централизованный сбор и корреляция событий безопасности со всех устройств.
2. Скрытие внутренней структуры сети и экономия публичных IP-адресов.
3. Разделение потоков трафика с разными грифами секретности.
4. Обеспечение бесперебойной работы при кратковременных скачках напряжения.
5. Увеличение скорости передачи данных за счёт сжатия пакетов.

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.  защищённой автоматизированной системе администратор обнаружил, что сетевое устройство не отвечает на ping, но при этом по журналам коммутатора порт активен, а светодиоды горят зелёным. С какой проблемы, скорее всего, начать диагностику согласно модели OSI «сверху-вниз»?
А) Обрыв физического кабеля на патч-панели.

Б) Неправильная конфигурация DNS-записей для данного устройства.
В) Блокировка ICMP-запросов на межсетевом экране или самом устройстве.
Г) Сбой в работе DHCP-сервера (аренда истекла).
2. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. При ежедневном техническом обслуживании сетевого оборудования администратор заметил, что температура внутри серверной комнаты превышает норму, а вентиляторы коммутатора работают на предельной скорости. Какое действие должно быть выполнено в первую очередь в рамках регламента?
А) Немедленно отключить оборудование для предотвращения перегрева.
Б) Проверить исправность системы кондиционирования и усилить воздухообмен.
В) Заменить термопасту на всех процессорах коммутаторов.
Г) Создать резервную копию конфигураций на внешний носитель.
3. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. При настройке защищённого VPN-соединения на базе IPsec администратор выбрал туннельный режим. Какое утверждение правильно описывает отличие этого режима от транспортного применительно к корпоративной сети?
А) Туннельный режим инкапсулирует весь исходный IP-пакет, включая заголовки, и используется для соединения «сеть-сеть».
Б) Туннельный режим шифрует только полезную нагрузку, оставляя заголовки открытыми, что быстрее для шлюзов.
В) Туннельный режим требует обязательного использования протокола L2TP, а транспортный – только ESP.
Г) Туннельный режим не поддерживает аутентификацию через IKE, в отличие от транспортного.

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. В корпоративной сети внедрены протоколы VRRP и LACP. Как распределяются их функции при обеспечении отказоустойчивости?
А) VRRP резервирует каналы связи путём агрегации портов, а LACP обеспечивает резервный шлюз.
Б) Оба протокола служат для балансировки нагрузки между разными маршрутизаторами.
В) LACP объединяет физические интерфейсы в логический канал, а VRRP предоставляет виртуальный шлюз для автоматического переключения при отказе основного маршрутизатора.
Г) VRRP работает только на уровне ядра ОС, а LACP – на прикладном уровне.
5. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. При проведении планового инструментального контроля оптической линии администратор получил показания OTDR, указывающие на повышенное затухание на определённом участке. Что из перечисленного является наиболее вероятной причиной и соответствует регламенту проверки?
А) Нарушение минимального радиуса изгиба кабеля или загрязнение коннектора.
Б) Неправильно настроенный IP-адрес на оптическом трансивере.
В) Превышение допустимого количества промежуточных коммутаций (сварных соединений).
Г) Выход из строя источника бесперебойного питания на той стороне.

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. После замены отказавшего маршрутизатора в защищённой АИС администратор восстановил конфигурацию из резервной копии, но криптографические ключи на новом устройстве не совпадают с прежними. Каков алгоритм действий для сохранения контура безопасности?
А) Перегенерировать все ключи и сертификаты заново, не уведомляя пользователей.
Б) Вручную ввести старые ключи с клавиатуры, игнорируя предупреждения системы.
В) Перенести ключевую информацию с доверенного носителя (или из резервного хранилища) на новое устройство и проверить целостность модулей.
Г) Отключить криптографию до следующего планового ТО, чтобы не нарушать работу сети.
7. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор. При комплексной проверке АИС (интеграция сети и СЗИ) тестирование сквозной доступности ресурсов показало, что пользователи из одного сегмента не могут получить доступ к серверу в другом сегменте, хотя политики фильтрации настроены корректно. Журналы межсетевого экрана не фиксируют блокировок. На что администратору следует обратить внимание в первую очередь?
А) На таблицу маршрутизации и правила NAT на промежуточных шлюзах.
Б) На наличие антивирусного ПО на клиентских рабочих станциях.
В) На срок действия сертификатов у пользователей.
Г) На версию прошивки коммутаторов доступа.

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. При периодическом обрыве соединения с удалённым сервером инженер проверил кабель — целостность нарушена не была, заменил коммутатор — проблема осталась. Логи показывают рост числа ICMP-запросов с одного IP-адреса. Определите, на каком уровне модели OSI, скорее всего, находится причина, и какой протокол помогает её обнаружить. Предложите первоочередное действие.
2. Прочитайте текст и запишите ответ. Средняя загрузка канала за час составила 45 Мбит/с, пиковая — 120 Мбит/с.

Пропускная способность канала — 200 Мбит/с. Рассчитайте коэффициент использования канала в процентах (средний) и округлите до целого. 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. В корпоративной сети внезапно перестали разрешаться имена внутренних ресурсов, хотя внешние сайты открываются. При этом DHCP продолжает выдавать адреса. Опишите последовательность диагностики (не менее трёх шагов) с указанием служб и утилит, которые вы будете использовать.
4. Прочитайте текст и запишите развернутый ответ. После сбоя питания при загрузке коммутатора появилось сообщение о повреждении конфигурационного файла startup-config. Резервная копия на TFTP-сервере есть, но интерфейс управления недоступен. Опишите алгоритм восстановления работоспособности устройства с сохранением настроек VLAN и маршрутизации.
5. Прочитайте текст и запишите ответ. В отказоустойчивом кластере из трёх маршрутизаторов с протоколом VRRP приоритеты равны 100, 150 и 200. Таймеры hello = 1 с, dead = 3 с. Определите, через сколько секунд после потери мастер -устройства (с приоритетом 200) произойдёт переключение на резервный, если dead-таймер не изменён. Разрешается использовать калькулятор.

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 развернутый ответ. При плановой замене вышедшего из строя маршрутизатора в защищённой АИС новый аппарат был подключён, но VPN-туннели с соседними узлами не поднялись. Ключи СКЗИ перенесены на новый носитель, сертификаты действительны. Назовите наиболее вероятную причину и порядок действий по её устранению без нарушения контура безопасности.
7. Прочитайте текст и запишите ответ. Объём конфигурационных файлов всех сетевых устройств — 8 Мбайт. Резервное копирование выполняется ежедневно инкрементно, средний размер изменений — 2 Мбайта в день. Сколько Мбайт суммарно будет занято на диске через 7 дней (полный бэкап + 6 инкрементных), если полный бэкап делается в 1-й день? Разрешается использовать калькулятор.
8. Прочитайте текст и запишите ответ. За 5 минут передано 1500 пакетов, из них потеряно 75. Чему равен процент потерянных пакетов (PLR) с точностью до десятых? Разрешается использовать калькулятор.

ИТОГОВЫЙ ТЕСТ

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении
1. Какие из перечисленных протоколов работают на сетевом уровне модели OSI и используются для маршрутизации в стеке TCP/IP?
А) IP
Б) ICMP
В) ARP
Г) TCP
2. Какие требования предъявляются к компьютерным сетям в защищённом исполнении согласно нормативным документам?
А) Наличие сертифицированных средств защиты информации.
Б) Обязательное использование только беспроводных соединений.
В) Ведение журналов аудита и регистрация событий безопасности.
Г) Отсутствие резервного копирования для экономии ресурсов.
3. Какие из перечисленных служб используются для автоматического назначения IP-адресов и преобразования доменных имён в IP-адреса?
А) DHCP
Б) DNS
В) Active Directory
Г) NFS
4. Какие утилиты командной строки используются для проверки сетевой связности и трассировки маршрута?
А) ping
Б) tracert (traceroute)
В) nslookup
Г) ipconfig (ifconfig)

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
5. Какие протоколы относятся к транспортному уровню модели OSI и обеспечивают доставку данных?
А) TCP
Б) UDP
В) IP
Г) ICMP
6. Какие из перечисленных действий входят в ежедневное техническое обслуживание сетевого оборудования?
А) Внешний осмотр индикаторов состояния.

Б) Проверка температуры и вентиляции.
В) Замена термопасты на процессорах.
Г) Резервирование конфигураций на внешний носитель.
7. Какие протоколы используются для организации защищённых каналов VPN?
А) IPsec
Б) SSL/TLS
В) SNMP
Г) HTTP
8. Какие функции выполняет система обнаружения вторжений (IDS)?
А) Анализ трафика на наличие вредоносных сигнатур.
Б) Блокировка подозрительных соединений в реальном времени.
В) Оповещение администратора об аномалиях.
Г) Шифрование всех передаваемых данных.
9. Какие методы резервного копирования конфигураций сетевых устройств могут применяться?
А) Полное копирование.
Б) Инкрементное копирование.
В) Дифференциальное копирование.
Г) Только копирование на бумажный носитель.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении
10. Какие протоколы используются для обеспечения отказоустойчивости шлюзов (виртуальный маршрутизатор)?
А) VRRP
Б) HSRP
В) LACP
Г) STP
11. Какие действия должны быть выполнены при компрометации ключей СКЗИ?
А) Немедленная смена всех ключей и сертификатов.
Б) Запись инцидента в журнал аудита.
В) Продолжение использования старых ключей до окончания срока.
Г) Уведомление ответственных должностных лиц.
12. Какие документы относятся к эксплуатационной документации на сетевые компоненты АИС?
А) Руководство администратора.
Б) Руководство пользователя.
В) Инструкция по техническому обслуживанию.
Г) Рекламный буклет производителя.
13. Какие параметры мониторинга сети относятся к показателям качества обслуживания (QoS)?
А) Задержка (latency).
Б) Потеря пакетов (packet loss).
В) Джиттер (jitter).
Г) Количество установленных соединений.
14. Какие меры применяются для сегментации сети по уровням конфиденциальности в защищённой АИС?
А) Использование VLAN для разделения трафика.
Б) Настройка межсетевых экранов между сегментами.
В) Объединение всех устройств в одну широковещательную область.
Г) Назначение разных IP-подсетей с разными политиками доступа.
15. Какие требования предъявляются к проведению планового технического обслуживания в защищённых системах?
А) Согласование времени работ с руководством и пользователями.
Б) Оформление наряда-допуска на выполнение работ.
В) Проведение работ без отключения системы для экономии времени.
Г) Ведение протокола выполненных операций.

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

Учебным планом не предусмотрено

**Описание критериев оценивания успеваемости**

| НЕДОСТАТОЧНЫЙ УРОВЕНЬ<br>Обучающийся демонстрирует:<br>- существенные пробелы в знаниях учебного материала;<br>- принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий;<br>- непонимание сущности дополнительных вопросов в рамках заданий билета;<br>- отсутствие умения выполнять практические задания, предусмотренные программой дисциплины;<br>- отсутствие готовности (способности) к дискуссии и низкая степень контактности. | ПОРОГОВЫЙ УРОВЕНЬ<br>Обучающийся демонстрирует:<br>- знания теоретического материала;<br>- неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов;<br>- неуверенные и неточные ответы на дополнительные вопросы;<br>- недостаточное владение литературой, рекомендованной программой дисциплины;<br>- умение без грубых ошибок решать практические задания, которые следует выполнить. | ПРОДВИНУТЫЙ УРОВЕНЬ<br>Обучающийся демонстрирует:<br>- знание и понимание основных вопросов контролируемого объема программного материала;<br>- твердые знания теоретического материала;<br>- способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития;<br>- правильные и конкретные, без грубых ошибок ответы на поставленные вопросы;<br>- умение решать практические задания, которые следует выполнить;<br>- владение основной литературой, рекомендованной программой дисциплины;<br>- наличие собственной обоснованной позиции по обсуждаемым вопросам;<br>- незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы. | ВЫСОКИЙ УРОВЕНЬ<br>Обучающийся демонстрирует:<br>- глубокие, всесторонние и аргументированные знания программного материала;<br>- полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий;<br>- способность устанавливать и объяснять связь практики и теории;<br>- логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора;<br>- умение решать практические задания;<br>- 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.<br>При устной презентации уверенно и быстро отвечает на заданные вопросы, выступление сопровождается приемами визуализации.<br>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.<br><br>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.<br>При устной презентации на дополнительные вопросы выступающий отвечает с некоторым затруднением, подготовленная устная презентации выполненного задания не очень структурирована.<br>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.<br><br>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,<br>показывает явный недостаток теоретических знаний. Выводы слабые, свидетельствуют о недостаточном анализе фактов, в основе решения может иметь место интерпретация фактов или предположения, собственная точка<br>зрения на причины возникновения проблемы не обоснована или отсутствует.<br>При устной презентации на вопросы отвечает с трудом или не отвечает совсем. Подготовленная презентация выполненного задания не структурирована.<br>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.<br><br>Оценка «неудовлетворительно» – задание не выполнено, или выполнено менее чем на треть.<br>Отсутствует детализация при анализе задания, изложение устное или письменное не структурировано.<br>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 | Борисов С. П. Компьютерные сети. Анализ и диагностика. Часть 1 [Электронный ресурс]:Учебное пособие. - Москва: РТУ МИРЭА, 2021. - 67 с. – Режим доступа: https://e.lanbook.com/book/176562 |
| Л.1.2 | Солоневич А. В. Компьютерные сети [Электронный ресурс]:учебное пособие. - Минск: РИПО, 2021. - 208 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=697153 |
| Л.1.3 | Алексахин А. Н., Алексахина С. А., Батищев А. В., Буланова Т. А., Дорофеев О. В. Компьютерные сети [Электронный ресурс]:учебник. - Москва: Университет Синергия, 2023. - 313 с. – Режим доступа: https://biblioclub.ru/index.php?page=book&id=699933 |
| Л.1.4 | 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.1.5 | Акмаров П. Б. Компьютерные сети. Лабораторный практикум [Электронный ресурс]:учебное пособие для спо. - Санкт-Петербург: Лань, 2026. - 120 с. – Режим доступа: https://e.lanbook.com/book/509334 |
| Л.1.6 | Бархатова Д. А., Буторин Д. Н., Левин А. А., Пак Н. И., Панова А. М. Компьютерные сети [Электронный ресурс]:учебник для вузов. - Санкт-Петербург: Лань, 2025. - 304 с. – Режим доступа: https://e.lanbook.com/book/460616 |

### 5.2. Перечень программного обеспечения

Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition

### 5.3. Перечень информационных справочных систем

ПЛАТФОРМА ОНЛАЙН-ОБРАЗОВАНИЯ «РАЗУМ»
Электронно-библиотечная система "Лань"
Научная электронная библиотека "eLIBRARY.RU"

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1303 - 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; 11 рабочих мест обучающихся, оснащенных ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Комплект типового лабораторного оборудования на основе программируемого контроллера АПК1-С-К; Комплект типового лабораторного оборудования ОАП1-С-Р; макет автоматизированной системы «Умное кафе», образовательный набор по электронике, робототехнике и микропроцессорной технике.

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:
о Глава 1 (теоретическая) – анализ концепций, выводы.
о Глава 2 (аналитическая/практическая) – анализ объекта, расчёты, данные, выводы.
о 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 _____

==========