**СОЧИНСКИЙ ИНСТИТУТ (ФИЛИАЛ)**
**федерального государственного автономного образовательного**
**учреждения высшего образования**
**«РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ ПАТРИСА ЛУМУМБЫ»**

Отделение среднего профессионального образования

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Петенко Александр Тимофеевич
Должность: Директор
Дата подписания: 24.04.2026
Уникальный программный ключ:
28acbc88a6d3ce11b5b992501f9a43df0be7b81d

# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

"Безопасность сетевой инфраструктуры"

(наименование дисциплины)

**Освоение учебной дисциплины ведется в рамках реализации основной образовательной программы среднего профессионального образования (ОП СПО):**

09.02.06 Сетевое и системное администрирование

(код и наименование специальности/профессии ОП СПО)

**Квалификация:**

системный администратор

(наименование квалификации)

Сочи,
2026 г.

# 1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
## ПМ.03.02 Безопасность сетевой инфраструктуры

*название дисциплины*

### 1.1. Область применения программы

Программа учебной дисциплины ПМ.03.02 Безопасность сетевой инфраструктуры является частью программы подготовки специалистов среднего звена в соответствии с ФГОС "Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ (приказ Минпросвещения России от 10.07.2023 г. № 519)"

### 1.2. Место учебной дисциплины в структуре программы подготовки специалистов среднего звена.

Учебная дисциплина ПМ.03.02 Безопасность сетевой инфраструктуры входит в Профессиональный цикл Профессиональной подготовки.

### 1.3. Цели и задачи – требования к результатам освоения учебной дисциплины.

Основная цель – способствовать формированию общих и профессиональных компетенций посредством приобретения знаний, умений и навыков.

**В результате освоения учебной дисциплины студент должен знать:**

- архитектуру и функции систем управления сетями, стандарты систем управления;
- средства мониторинга и анализа локальных сетей;
- методы устранения неисправностей в технических средствах.

**В результате освоения учебной дисциплины студент должен уметь:**

- выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
- осуществлять диагностику и поиск неисправностей всех компонентов сети;
- выполнять действия по устранению неисправностей.

**В результате освоения учебной дисциплины студент должен иметь навыки и (или) опыт деятельности:**

- обслуживании сетевой инфраструктуры, восстановлении работоспособности сети после сбоя;
- удаленном администрировании и восстановлении работоспособности сетевой инфраструктуры;
- поддержке пользователей сети, настройке аппаратного и программного обеспечения сетевой инфраструктуры.

### 1.4. Рекомендуемое количество часов на освоение программы учебной дисциплины:

Объем программы 72 часов, в том числе:
аудиторной учебной нагрузки обучающегося 60 часов;
самостоятельной работы обучающегося 12 часов.

# 2. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ
### 2.1. Объем учебной дисциплины и виды учебной работы

*Таблица 1. Виды учебной работы по периодам освоения ООП СПО для формы обучения - очная.*

| Вид учебной работы | Всего, ак. ч. | Семестр(-ы) | | | | | |
|---|---|---|---|---|---|---|---|
| | | 8 | | | | | |
| **Контактная (аудиторная) работа (всего)** | 60 | 60 | | | | | |
| в том числе: | - | - | - | - | - | - | - |
| лекции (если предусмотрено) | 24 | 24 | | | | | |
| в том числе в форме практической подготовки (если предусмотрено) | - | - | | | | | |
| лабораторные занятия (если предусмотрено) | - | - | | | | | |
| в том числе в форме практической подготовки (если предусмотрено) | - | - | | | | | |
| практические занятия (если предусмотрено) | 36 | 36 | | | | | |
| в том числе в форме практической подготовки (если предусмотрено) | 12 | 12 | | | | | |
| **Самостоятельная работа обучающегося (всего)** | 12 | 12 | | | | | |
| в том числе: | - | - | - | - | - | - | - |
| в форме практической подготовки (если предусмотрено) | - | - | | | | | |
| Часов на контроль: | - | - | | | | | |
| Промежуточная аттестация в форме: (зачет/дифзачет/ экзамен) | - | Др | | | | | |
| Общая трудоемкость час | 72 | 72 | | | | | |

## 2.2. Тематический план и содержание учебной дисциплины ПМ.03.02 Безопасность сетевой инфраструктуры

*Таблица 2. Содержание дисциплины/МДК по видам учебной работы*

| НАИМЕНОВАНИЕ РАЗДЕЛА ДИСЦИПЛИНЫ<br>Содержание раздела (темы) | Вид учебной работы* | Кол-во часов |
|---|---|---|
| **Тема 1. Безопасность компьютерных сетей.** | **32** | |
| Фундаментальные принципы безопасной сети | Лек | 2 |
| Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак. | | |
| Безопасность сетевых устройств OSI | Лек | 2 |
| Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности. | | |
| Авторизация, аутентификация и учет доступа (AAA) | Лек | 2 |
| Свойства AAA. Локальная AAA аутентификация. Server-based AAA | | |
| Реализация технологий предотвращения вторжения | Лек | 2 |
| IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS | | |
| Безопасность локальной сети | Лек | 2 |
| Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN | | |
| Криптографические системы | Лек | 2 |
| Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей. | | |
| Реализация технологий VPN | Лек | 2 |
| VPN. GRE VPN. Компоненты и функционирование IPSec VPN. Реализация Site-to-site. IPSec VPN с использованием CLI. Реализация Site-to-site IPSec VPN с использованием CCP. Реализация Remote-access VPN | | |

| | | |
|---|---|---|
| Управление безопасной сетью | Лек | 2 |
| Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности. | | |
| Межсетевая безопасность | Лек | 2 |
| Методы обеспечения безопасности взаимодействия между различными сетями. Реализация технологий маршрутизации и шлюзов, использование межсетевых экранов, технологии виртуальных локальных сетей. | | |
| Защита от социальной инженерии | Пр | 2 |
| Методы социальной инженерии, опасности, связанные с подделкой и манипулированием данными, а также методы защиты и обучения персонала. | | |
| Социальная инженерия | Пр | 2 |
| Исследование сетевых атак и инструментов проверки защиты сети | Пр | 2 |
| Настройка безопасного доступа к маршрутизатору | Пр | 2 |
| Обеспечение административного доступа AAA и сервера Radius | Пр | 2 |
| Настройка политики безопасности брандмауэров | Пр | 2 |
| Настройка системы предотвращения вторжений (IPS) | Пр | 2 |
| **Тема 2. Обеспечение сетевой безопасности.** | **38** | |
| Организация защищенных каналов передачи данных | Лек | 2 |
| Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть. | | |
| Механизмы шифрования и аутентификации для обеспечения защищенного удаленного доступа | Лек | 2 |
| Механизмы шифрования и аутентификации для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам и сервисам. | | |
| Использование фаерволов и межсетевых экранов | Лек | 2 |
| Использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет. | | |
| Настройка VPN-туннелей | Пр | 2 |
| Настройка VPN-туннелей для организации защищенных каналов передачи данных между территориально распределенными офисами. | | |
| Работа с механизмами шифрования и аутентификации | Пр | 2 |
| Работа с механизмами шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам. | | |
| Настройка и использование фаерволов и межсетевых экранов | Пр | 2 |
| Настройка и использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет. | | |
| Анализ содержимого трафик | Пр | 2 |
| Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети с использованием программного обеспечения для мониторинга и обнаружения угроз | | |
| Разработка и внедрение мер по минимизации рисков внедрения вредоносного ПО | Пр | 2 |
| Разработка и внедрение мер по минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях. | | |
| Настройка и работа с системами обнаружения и предотвращения сетевых вторжений | Пр | 2 |
| Настройка и работа с системами обнаружения и предотвращения сетевых вторжений для раннего обнаружения и предотвращения угроз безопасности. | | |

| | | |
|---|---|---|
| Настройка и использование виртуальных частных сетей (VPN) | Пр | 2 |
| Настройка и использование виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам. | | |
| Настройка и работа с системами управления доступом для контроля доступа к корпоративной сети. | Пр | 2 |
| Обеспечение безопасности Wi-Fi-сетей | Пр | 2 |
| Настройка безопасных точек доступа, использование сетевой аутентификации, шифрования трафика и других методов. | | |
| Работа с антивирусным программным обеспечением | Пр | 2 |
| Работа с антивирусным программным обеспечением для защиты от вирусов и других вредоносных программ: установка, настройка, обновление базы данных, сканирование и удаление вредоносных программ. | | |
| Защита от DDoS-атак | СР | 4 |
| Использование специализированных средств защиты от DDoS-атак, настройка маршрутизации трафика, мониторинг сетевой активности. | | |
| Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети | СР | 4 |
| Настройка политик безопасности для мобильных устройств, управление устройствами и приложениями, защита данных на устройствах. | | |
| Обеспечение безопасности облачных сервисов | СР | 4 |
| Выбор надежных провайдеров облачных сервисов, настройка правил доступа и аутентификации, шифрование данных, мониторинг активности в облачных сервисах. | | |
| **Дифференцированный зачет** | **2** | |
| Зачет | ЗаО | 2 |

** - Лек – лекции; Пр – практические занятия; СР – самостоятельная работа; ЛР – лабораторные работы.*

## 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

### 3.1. Требования к минимальному материально-техническому обеспечению

Для реализации программы учебной дисциплины предусмотрены специальные помещения, приведенным в п 6.3 основной образовательной программы специальности.

*Таблица 3. Материально-техническое обеспечение дисциплины*

| **Тип аудитории** | **Оснащение аудитории**<br>**Специализированное учебное оборудование, ПО и материалы для освоения дисциплины (при необходимости)** |
|---|---|

| | |
|---|---|
| Учебная аудитория для проведения занятий лекционного типа, практических занятий, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации | Комплект специализированной мебели, маркерная доска; кафедра; автоматизированное рабочее место преподавателя: компьютер AMD Ryzen, монитор LCD 24" Philips, интерактивная панель 86", имеется выход в интернет<br>Программное обеспечение: Операционная система Windows 10 Pro; Office Professional 2007, Kaspersky Endpoint security для бизнеса - Стандартный |
| Учебная аудитория для проведения занятий лекционного типа, практических занятий, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации (Компьютерный класс) | Комплект специализированной мебели; доска аудиторная меловая, автоматизированные рабочие места (процессор не ниже Intel Core i5, оперативная память объемом не менее 16Gb;(SSD 500 GB HDD 1 TB); проектор EPSON, проекционный экран, имеется выход в интернет<br>Программное обеспечение: Операционная система Windows 10 Pro; Office Professional 2007, Kaspersky Endpoint security для бизнеса - Стандартный |
| Аудитория для самостоятельной работы обучающихся | Комплект специализированной мебели; Телевизор LED LG 42" автоматизированные рабочие места (процессор не ниже AMD Ryzen, оперативная память объемом не менее 8 Гб; SDD 500 GB, моноблок Lenovo Intel i3), имеется выход в интернет<br>Программное обеспечение: Операционная система Windows 10 Pro; Office Professional 2007, Kaspersky Endpoint security для бизнеса - Стандартный |

**3.2. Информационное обеспечение обучения**
**Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы**

*Основные источники:*

1. Васильков А.В., Васильков И. А. Безопасность и управление доступом в информационных системах : Учебное пособие. - Москва: Издательство "ФОРУМ", 2022. - 368 с. - Текст : электронный. - URL: https://znanium.com/catalog/document?id=399436

2. Щербак А. В. Информационная безопасность : учебник для спо. - Москва: Юрайт, 2024. - 259 с - Текст : электронный. - URL: https://urait.ru/bcode/543873

*Дополнительные источники:*

3. Ниматулаев М.М. Информационные технологии в профессиональной деятельности : Учебник. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2023. - 250 с. - Текст : электронный. - URL: https://znanium.com/catalog/document?id=417518

4. Самуйлов К. Е., Василевский В. В., Васин Н. Н., Королькова А. В., Шалимов И. А., Кулябов Д. С. Сети и телекоммуникации : учебник и практикум для спо. - Москва: Юрайт, 2023. - 363 с - Текст : электронный. - URL: https://urait.ru/bcode/517817

*Ресурсы информационно-телекоммуникационной сети «Интернет»:*

1. ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров:

- Образовательная платформа Юрайт https://urait.ru

- ЭБС «Университетская библиотека онлайн» http://biblioclub.ru
- ЭБС Znanium https://znanium.ru
- Электронно-библиотечная система РУДН – ЭБС РУДН http://mega.rudn.ru/MegaPro/Web

2. Базы данных и поисковые системы:

- Учебный портал института https://portal.rudn-sochi.ru/

*Методические материалы для обучающихся*

Самостоятельная работа студента является ключевой составляющей учебного процесса, которая определяет формирование навыков, умений и знаний, приемов познавательной деятельности и обеспечивает интерес к творческой работе.
Правильно спланированная и организованная самостоятельная работа студентов позволяет:
-сделать образовательный процесс более качественным и интенсивным;
-способствует созданию интереса к избранной профессии и овладению ее особенностями;
-приобщить студента к творческой деятельности;
-проводить в жизнь дифференцированный подход к обучению.
При организации самостоятельной работы студентов в качестве методологической основы должен применяться деятельный подход, когда обучение ориентировано на формирование умений решать не только типовые, но и нетиповые задачи, когда студент должен проявить творческую активность, инициативу, знания, умения и навыки, полученные при изучении конкретной дисциплины.
Учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины на Учебном портале.

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

*Таблица 4. Контроль и оценка результатов освоения дисциплины*

| **Результаты обучения (освоенные умения, усвоенные знания)** | **Формы и методы контроля и оценки результатов обучения** |
|---|---|
| Знания:<br>- архитектуру и функции систем управления сетями, стандарты систем управления;<br>- средства мониторинга и анализа локальных сетей;<br>- методы устранения неисправностей в технических средствах. | Анализ и оценка выполнения индивидуальных заданий, расчетных работ, опрос, тематический диктант, контрольная работа, практические занятия, домашние работы, компьютерное тестирование, Взаимоконтроль и самоконтроль студентов. Полнота и грамотность подготовленных докладов, сообщений, презентаций. |
| Умения:<br>- выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;<br>- осуществлять диагностику и поиск неисправностей всех компонентов сети;<br>- выполнять действия по устранению неисправностей. | Наблюдение, контроль преподавателя за деятельностью обучающихся, анализ и оценка оптимальности метода решения задач, беседа, опрос, практические занятия, домашние работы, компьютерное тестирование |
| Практический опыт:<br>- обслуживании сетевой инфраструктуры, восстановлении работоспособности сети после сбоя;<br>- удаленном администрировании и восстановлении работоспособности сетевой инфраструктуры;<br>- поддержке пользователей сети, настройке аппаратного и программного обеспечения сетевой инфраструктуры. | Наблюдение, контроль преподавателя за деятельностью обучающихся, анализ и оценка оптимальности метода решения задач, выполнение и защита индивидуальных заданий. |

## 5. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

*Таблица 5. Перечень компетенций*

| **Шифр** | **Результаты (компетенции)**<br>**Основные показатели результатов подготовки** |
|---|---|
| **ПК 3.1.** | **Осуществлять проектирование сетевой инфраструктуры.** |

| | |
|---|---|
| Знать:<br>этапы проектирования сетевой инфраструктуры;<br>активное и пассивное оборудование сетей;<br>виды кабелей и технические особенности их монтажа;<br>специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей;<br>технологии обеспечения масштабируемости, надежности и отказоустойчивости сети;<br>элементы теории массового обслуживания;<br>основы проектирования беспроводных сетей;<br>принципы построения высокоскоростных компьютерных сетей. | |
| Уметь:<br>выбирать и применять сетевые топологии и технологии передачи данных для обеспечения масштабируемой надежной отказоустойчивой сетевой инфраструктуры;<br>использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей;<br>анализировать, проектировать и настраивать схемы потоков трафика в компьютерной сети. | |
| Владеть:<br>проектирования архитектуры масштабируемой отказоустойчивой сетевой инфраструктуры. | |
| **ПК 3.2.** | **Обслуживать сетевые конфигурации программно-аппаратных средств.** |
| Знать:<br>особенности построения гибридных многоуровневых сетей;<br>способы добавления, замены, удаления отдельных элементов сети;<br>технологию QinQ (IEEE 802.1QinQ);<br>технологии многопротокольной коммутации по меткам (mpls);<br>особенности протоколов is-is, bgp, ospf;<br>понятие о качестве обслуживания(qos). | |
| Уметь:<br>выполнять добавление, замену, удаление отдельных элементов сети;<br>применять технологии построения ip фабрик;<br>устанавливать и настраивать беспроводные сети;<br>применять технологии тегирования и многопротокольной коммутации по меткам;<br>настраивать протоколы is-is, bgp, ospf;<br>устанавливать и настраивать системы ip-телефонии. | |
| Владеть:<br>установки и настройки сетевых протоколов и сетевого оборудования гибридных многоуровневых сетей;<br>установки систем качества обслуживания. | |
| **ПК 3.3.** | **Осуществлять защиту информации в сети с использованием программно-аппаратных средств.** |
| Знать:<br>требования к сетевой безопасности;<br>системы управления доступом для контроля доступа к корпоративной сети;<br>системы обнаружения и предотвращения сетевых вторжений;<br>технологии организации частных сетей;<br>методы безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам;<br>межсетевые экраны;<br>механизмы шифрования и аутентификации. | |

| | |
|---|---|
| Уметь:<br>внедрять системы управления доступом для контроля доступа к корпоративной сети;<br>применять технологии организации частных сетей;<br>выполнять работы по обеспечению безопасности электронной почты;<br>использовать системы обнаружения и предотвращения сетевых вторжений;<br>применять механизмы шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам;<br>устанавливать и настраивать антивирусное программное обеспечение;<br>выполнять установку и настройку межсетевых экранов для комплексной защиты корпоративной сети. | |
| Владеть:<br>внедрения систем безопасного хранения и передачи информации в глобальных и локальных сетях. | |
| **ПК 3.4.** | **Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.** |
| Знать:<br>проектную документацию по организации сегментов сети;<br>технологии, инструментальные средства организации процесса исследования объектов сетевой инфраструктуры;<br>нетипичные неисправности в работе сетевой инфраструктуры. | |
| Уметь:<br>контролировать соответствие разрабатываемого проекта нормативно-технической документации;<br>применять технологии, инструментальные средства при организации процесса исследования объектов сетевой инфраструктуры;<br>устранять выявленные неисправности в работе сетевой инфраструктуры. | |
| Владеть:<br>организации мониторинга производительности сервера и протоколирования системных и сетевых событий в целях выявления нетипичных неисправностей;<br>устранения нетипичных неисправностей в работе сетевой инфраструктуры. | |
| **ПК 3.5.** | **Модернизировать сетевые устройства информационно-коммуникационных систем.** |

| |
|---|
| Знать:<br>требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы;<br>основы архитектуры, устройства и функционирования вычислительных систем;<br>общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы;<br>стандарты информационного взаимодействия систем;<br>конструкции типичных элементов линий передачи;<br>архитектуру аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы;<br>технические характеристики основного оборудования, комплектующих и материалов информационно-коммуникационной системы;<br>типовые варианты взаимозаменяемости;<br>принципы установки и настройки программного обеспечения;<br>принципы организации, состав и схемы работы операционных систем;<br>инструкции по установке администрируемого периферийного оборудования;<br>инструкции по эксплуатации администрируемого периферийного оборудования;<br>регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе;<br>лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения;<br>принципы организации информационных систем управления ремонтом и обслуживанием;<br>типовые сроки проведения профилактического ремонта;<br>правила и процедуры проведения инвентаризации;<br>программные средства инвентаризации;<br>правила маркировки устройств и элементов информационно-коммуникационной системы;<br>основы делопроизводства;<br>процедуры списания технических средств;<br>отраслевые нормативные правовые акты;<br>типовые сроки заключения и действия договоров на обслуживание информационно-коммуникационной системы;<br>английский язык на уровне чтения технической документации в области информационных и компьютерных технологий. |
| Уметь:<br>вести техническую документацию по объектам информационно-коммуникационной системы;<br>контролировать наличие и движение аппаратных, программно-аппаратных и программных средств;<br>пользоваться нормативно-технической документацией в области инфокоммуникационных технологий;<br>пользоваться нормативно-технической документацией на информационно-коммуникационную систему, в том числе на английском языке;<br>работать с информационной системой управления запасами и ремонтом;<br>оформлять заявки на материалы и комплектующие информационно-коммуникационной системы;<br>работать с договорной и отчетной документацией на обслуживаемую информационно-коммуникационную систему;<br>вести деловую переписку;<br>идентифицировать типичные инциденты;<br>регистрировать инцидент в информационной системе управления инцидентами;<br>проводить диагностику инцидента согласно инструкции;<br>оценивать степень критичности инцидентов при работе. |

| | |
|---|---|
| Владеть:<br>конфигурирования периферийных устройства;<br>применения методов управления сетевыми устройствами;<br>применения методов задания базовых параметров и параметров защиты от несанкционированного доступа к операционным системам;<br>применения методов статической и динамической конфигурации параметров операционных систем;<br>установки базовых параметров, в том числе параметров защиты от несанкционированного доступа к операционным системам. | |
| **ПК 3.1.** | **Осуществлять поиск и устранение нетипичных неисправностей, возникающих в серверных операционных системах.** |
| Знать:<br>этапы проектирования сетевой инфраструктуры;<br>активное и пассивное оборудование сетей;<br>виды кабелей и технические особенности их монтажа;<br>специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей;<br>технологии обеспечения масштабируемости, надежности и отказоустойчивости сети;<br>элементы теории массового обслуживания;<br>основы проектирования беспроводных сетей;<br>принципы построения высокоскоростных компьютерных сетей. | |
| Уметь:<br>выбирать и применять сетевые топологии и технологии передачи данных для обеспечения масштабируемой надежной отказоустойчивой сетевой инфраструктуры;<br>использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей;<br>анализировать, проектировать и настраивать схемы потоков трафика в компьютерной сети. | |
| Владеть:<br>проектирования архитектуры масштабируемой отказоустойчивой сетевой инфраструктуры. | |
| **ПК 3.2.** | **Обновлять программное обеспечение серверных операционных систем и серверного программного обеспечения.** |
| Знать:<br>особенности построения гибридных многоуровневых сетей;<br>способы добавления, замены, удаления отдельных элементов сети;<br>технологию QinQ (IEEE 802.1QinQ);<br>технологии многопротокольной коммутации по меткам (mpls);<br>особенности протоколов is-is, bgp, ospf;<br>понятие о качестве обслуживания(qos). | |
| Уметь:<br>выполнять добавление, замену, удаление отдельных элементов сети;<br>применять технологии построения ip фабрик;<br>устанавливать и настраивать беспроводные сети;<br>применять технологии тегирования и многопротокольной коммутации по меткам;<br>настраивать протоколы is-is, bgp, ospf;<br>устанавливать и настраивать системы ip-телефонии. | |
| Владеть:<br>установки и настройки сетевых протоколов и сетевого оборудования гибридных многоуровневых сетей;<br>установки систем качества обслуживания. | |
| **ПК 3.3.** | **Выполнять послеаварийное восстановление серверных операционных систем.** |

| | |
|---|---|
| Знать:<br>требования к сетевой безопасности;<br>системы управления доступом для контроля доступа к корпоративной сети;<br>системы обнаружения и предотвращения сетевых вторжений;<br>технологии организации частных сетей;<br>методы безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам;<br>межсетевые экраны;<br>механизмы шифрования и аутентификации. | |
| Уметь:<br>внедрять системы управления доступом для контроля доступа к корпоративной сети;<br>применять технологии организации частных сетей;<br>выполнять работы по обеспечению безопасности электронной почты;<br>использовать системы обнаружения и предотвращения сетевых вторжений;<br>применять механизмы шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам;<br>устанавливать и настраивать антивирусное программное обеспечение;<br>выполнять установку и настройку межсетевых экранов для комплексной защиты корпоративной сети. | |
| Владеть:<br>внедрения систем безопасного хранения и передачи информации в глобальных и локальных сетях. | |
| **ПК 3.4.** | **Администрировать серверные операционные системы.** |
| Знать:<br>проектную документацию по организации сегментов сети;<br>технологии, инструментальные средства организации процесса исследования объектов сетевой инфраструктуры;<br>нетипичные неисправности в работе сетевой инфраструктуры. | |
| Уметь:<br>контролировать соответствие разрабатываемого проекта нормативно-технической документации;<br>применять технологии, инструментальные средства при организации процесса исследования объектов сетевой инфраструктуры;<br>устранять выявленные неисправности в работе сетевой инфраструктуры. | |
| Владеть:<br>организации мониторинга производительности сервера и протоколирования системных и сетевых событий в целях выявления нетипичных неисправностей;<br>устранения нетипичных неисправностей в работе сетевой инфраструктуры. | |
| **ПК 3.1.** | **Осуществлять развертывание облачной инфраструктуры.** |
| Знать:<br>этапы проектирования сетевой инфраструктуры;<br>активное и пассивное оборудование сетей;<br>виды кабелей и технические особенности их монтажа;<br>специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей;<br>технологии обеспечения масштабируемости, надежности и отказоустойчивости сети;<br>элементы теории массового обслуживания;<br>основы проектирования беспроводных сетей;<br>принципы построения высокоскоростных компьютерных сетей. | |
| Уметь:<br>выбирать и применять сетевые топологии и технологии передачи данных для обеспечения масштабируемой надежной отказоустойчивой сетевой инфраструктуры;<br>использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей;<br>анализировать, проектировать и настраивать схемы потоков трафика в компьютерной сети. | |
| Владеть:<br>проектирования архитектуры масштабируемой отказоустойчивой сетевой инфраструктуры. | |

| ПК 3.2. | **Проводить документирование требований и технических возможностей облачных инфраструктур.** |
|---|---|
| Знать:<br>особенности построения гибридных многоуровневых сетей;<br>способы добавления, замены, удаления отдельных элементов сети;<br>технологию QinQ (IEEE 802.1QinQ);<br>технологии многопротокольной коммутации по меткам (mpls);<br>особенности протоколов is-is, bgp, ospf;<br>понятие о качестве обслуживания(qos). | |
| Уметь:<br>выполнять добавление, замену, удаление отдельных элементов сети;<br>применять технологии построения ip фабрик;<br>устанавливать и настраивать беспроводные сети;<br>применять технологии тегирования и многопротокольной коммутации по меткам;<br>настраивать протоколы is-is, bgp, ospf;<br>устанавливать и настраивать системы ip-телефонии. | |
| Владеть:<br>установки и настройки сетевых протоколов и сетевого оборудования гибридных многоуровневых сетей;<br>установки систем качества обслуживания. | |
| **ПК 3.3.** | **Проводить настройку виртуальных машин с использованием механизмов автоматического масштабирования и распределения нагрузки.** |
| Знать:<br>требования к сетевой безопасности;<br>системы управления доступом для контроля доступа к корпоративной сети;<br>системы обнаружения и предотвращения сетевых вторжений;<br>технологии организации частных сетей;<br>методы безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам;<br>межсетевые экраны;<br>механизмы шифрования и аутентификации. | |
| Уметь:<br>внедрять системы управления доступом для контроля доступа к корпоративной сети;<br>применять технологии организации частных сетей;<br>выполнять работы по обеспечению безопасности электронной почты;<br>использовать системы обнаружения и предотвращения сетевых вторжений;<br>применять механизмы шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам;<br>устанавливать и настраивать антивирусное программное обеспечение;<br>выполнять установку и настройку межсетевых экранов для комплексной защиты корпоративной сети. | |
| Владеть:<br>внедрения систем безопасного хранения и передачи информации в глобальных и локальных сетях. | |
| **ПК 3.4.** | **Производить хранение и анализ данных.** |
| Знать:<br>проектную документацию по организации сегментов сети;<br>технологии, инструментальные средства организации процесса исследования объектов сетевой инфраструктуры;<br>нетипичные неисправности в работе сетевой инфраструктуры. | |
| Уметь:<br>контролировать соответствие разрабатываемого проекта нормативно-технической документации;<br>применять технологии, инструментальные средства при организации процесса исследования объектов сетевой инфраструктуры;<br>устранять выявленные неисправности в работе сетевой инфраструктуры. | |

Владеть:
организации мониторинга производительности сервера и протоколирования системных и сетевых событий в целях выявления нетипичных неисправностей;
устранения нетипичных неисправностей в работе сетевой инфраструктуры.

| | |
|---|---|
| **ПК 3.5.** | **Обеспечивать информационную безопасность в облачной инфраструктуре с помощью различных инструментов.** |

Знать:
требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы;
основы архитектуры, устройства и функционирования вычислительных систем;
общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы;
стандарты информационного взаимодействия систем;
конструкции типичных элементов линий передачи;
архитектуру аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы;
технические характеристики основного оборудования, комплектующих и материалов информационно-коммуникационной системы;
типовые варианты взаимозаменяемости;
принципы установки и настройки программного обеспечения;
принципы организации, состав и схемы работы операционных систем;
инструкции по установке администрируемого периферийного оборудования;
инструкции по эксплуатации администрируемого периферийного оборудования;
регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе;
лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения;
принципы организации информационных систем управления ремонтом и обслуживанием;
типовые сроки проведения профилактического ремонта;
правила и процедуры проведения инвентаризации;
программные средства инвентаризации;
правила маркировки устройств и элементов информационно-коммуникационной системы;
основы делопроизводства;
процедуры списания технических средств;
отраслевые нормативные правовые акты;
типовые сроки заключения и действия договоров на обслуживание информационно-коммуникационной системы;
английский язык на уровне чтения технической документации в области информационных и компьютерных технологий.

Уметь:
вести техническую документацию по объектам информационно-коммуникационной системы;
контролировать наличие и движение аппаратных, программно-аппаратных и программных средств;
пользоваться нормативно-технической документацией в области инфокоммуникационных технологий;
пользоваться нормативно-технической документацией на информационно-коммуникационную систему, в том числе на английском языке;
работать с информационной системой управления запасами и ремонтом;
оформлять заявки на материалы и комплектующие информационно-коммуникационной системы;
работать с договорной и отчетной документацией на обслуживаемую информационно-коммуникационную систему;
вести деловую переписку;
идентифицировать типичные инциденты;
регистрировать инцидент в информационной системе управления инцидентами;
проводить диагностику инцидента согласно инструкции;
оценивать степень критичности инцидентов при работе.

| |
|---|
| Владеть:<br>конфигурирования периферийных устройства;<br>применения методов управления сетевыми устройствами;<br>применения методов задания базовых параметров и параметров защиты от несанкционированного доступа к операционным системам;<br>применения методов статической и динамической конфигурации параметров операционных систем;<br>установки базовых параметров, в том числе параметров защиты от несанкционированного доступа к операционным системам. |

## 6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

### 6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Безопасность сетевой инфраструктуры»

Перечень вопросов для подготовки к занятиям и промежуточной аттестации, контрольных работ, содержание заданий для выполнения практических и самостоятельных работ, рекомендации по выполнению и критерии оценивания представлены в фонде оценочных средств по дисциплине «Безопасность сетевой инфраструктуры» в Приложении к настоящей Рабочей программе дисциплины.

Оценочные средства позволяют провести текущий контроль по дисциплине. По каждому средству оценивается полнота и глубина освоения, характеризующиеся показателями и критериями оценивания

*Таблица 6. Показатели и критерии оценивания*

| Показатель | Критерий |
|---|---|
| Пороговый (узнавание) «3» | Знает: базовые общие знания;<br>Умеет: основные умения, требуемые для выполнения простых задач;<br>Владеет: работает при прямом наблюдении. |
| Базовый (воспроизведение) «4» | Знает: факты, принципы, процессы, общие понятия в пределах области исследования;<br>Умеет: диапазон практических умений, требуемых для решения определенных проблем в области исследования;<br>Владеет: берет ответственность за завершение задач в исследовании, приспосабливает свое поведение к обстоятельствам в решении проблем |
| Высокий (компетентность) «5» max балл | Знает: фактическое и теоретическое знание в пределах области исследования с пониманием границ применимости;<br>Умеет: диапазон практических умений, требуемых для развития творческих решений, абстрагирования проблем;<br>Владеет: контролирует работу, проводит оценку, совершенствует действия работы |

Максимальное количество баллов по каждому оценочному средству соответствует вербальному критерию «высокий».

## 7. ИНЫЕ СВЕДЕНИЯ И (ИЛИ) МАТЕРИАЛЫ

### 7.1 Перечень образовательных технологий, используемых при осуществлении образовательного процесса по дисциплине

В процессе обучения используются активные и интерактивные образовательные технологии (формы проведения занятий):

-лекции, фронтальные опросы, презентации и защита мини-проектов;

-кейс-стади (разбор конкретных ситуаций),

-имитационные компьютерные модели;

-организации самостоятельной учебно-познавательной деятельности (индивидуальные домашние задания).