

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Колледж радиоэлектроники имени П.Н. Яблочкова



Рабочая программа профессионального модуля

ПМ.03 Эксплуатация объектов сетевой инфраструктуры (по выбору)

09.02.06 Сетевое и системное администрирование

Профиль подготовки
технологический

Квалификация выпускника
системный администратор
Форма обучения
очная

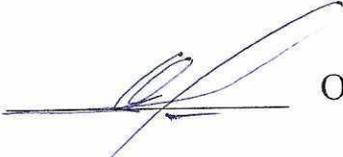
Саратов
2024

Разработчик: преподаватель В.В. Юрина 
Программа одобрена на заседании ЦК информационных систем и
программирования
от 08.04.2024 протокол № 12

Председатель ЦК информационных систем и программирования

 Е.В. Гожий

Директор
Колледжа радиоэлектроники
имени П. Н. Яблочкова


О.В. Бреус

Зам. директора по УР


Н.Н. Чернова

Рабочая программа учебной дисциплины разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование производства Приказ Минпросвещения России от 10.07.2023 № 519 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование» (Зарегистрировано в Минюсте России 15.08.2023 № 74796)).

Организация-разработчик: ФГБОУ ВО «СГУ имени Н.Г. Чернышевского» Колледж радиоэлектроники имени П.Н. Яблочкова

Разработчики: Юрина В. В. – преподаватели Колледжа радиоэлектроники имени П.Н. Яблочкова

СОДЕРЖАНИЕ

	стр.
1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	5
3 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	6
4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	23
5 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ДЕЯТЕЛЬНОСТИ)	25

1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Эксплуатация объектов сетевой инфраструктуры (по выбору)

1.1 Область применения программы

Рабочая программа профессионального модуля (далее – программа ПМ) является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование, в части освоения основного вида деятельности (ВД) Эксплуатация объектов сетевой инфраструктуры (по выбору) и соответствующих ему профессиональных компетенций:

ПК 3.1 Осуществлять проектирование сетевой инфраструктуры.

ПК 3.2 Обслуживать сетевые конфигурации программно-аппаратных средств.

ПК 3.3 Осуществлять защиту информации в сети с использованием программно-аппаратных средств.

ПК 3.4 Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.

ПК 3.5 Модернизировать сетевые устройства информационно-коммуникационных систем.

1.2 Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт в:

- обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;
- удаленном администрировании и восстановления работоспособности сетевой инфраструктуры;
- поддержке пользователей сети, настройке аппаратного и программного обеспечения сетевой инфраструктуры

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

знать:

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

1.3 Количество часов на освоение программы профессионального модуля:

всего (учебной нагрузки обучающегося) – 660 часов,

в том числе:

учебной нагрузки обучающегося во взаимодействии с преподавателем – 328 часов;

практической подготовки – 452 часа;

учебной и производственной практики – 288 часов;

самостоятельной учебной работы обучающегося – 30 часов;

промежуточная аттестация – 12 часов.

2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом деятельности Разработка модулей программного обеспечения для компьютерных систем, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 3.1	Осуществлять проектирование сетевой инфраструктуры.
ПК 3.2	Обслуживать сетевые конфигурации программно-аппаратных средств.
ПК 3.3.	Осуществлять защиту информации в сети с использованием программно-аппаратных средств.
ПК 3.4.	Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.
ПК 3.5.	Модернизировать сетевые устройства информационно-коммуникационных систем.
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.

3 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Тематический план профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Объем образовательной нагрузки	Объем времени, отведенный на освоение междисциплинарного курса (курсов), час								Практика (практическая подготовка), час	
			Учебная работа обучающегося во взаимодействии с преподавателем						самостоятельная учебная работа обучающегося		Учебная	Производственная
			Всего учебных занятий	Теоретическое обучение	в т.ч. практическая подготовка	практические занятия, час	в т.ч. практическая подготовка	Курсовое проектирование (практическая подготовка)	Всего часов	в т.ч. курсовое проектирование (практическая подготовка)		
ПК 3.1; ПК 3.4; ПК 3.5 ОК 01 – ОК 05	Раздел 1 Эксплуатация сетевой инфраструктуры	144	134	68		66	66		10			
ПК 3.2 ОК 01 – ОК 05	Раздел 2. Технологии автоматизации технологических процессов	108	92	44		46	46		10			
ПК 3.3 – ПК 3.5 ОК 01 – ОК 05	Раздел 3. Безопасность сетевой инфраструктуры	108	102	50		52	52		6			
ПК 3.1 – ПК 3.5 ОК 01 – ОК 05	Учебная практика Эксплуатация объектов сетевой инфраструктуры (по выбору), час	108									108	
ПК 3.1 – ПК 3.5 ОК 01 – ОК 05	Производственная практика Эксплуатация объектов сетевой инфраструктуры (по выбору), час	180										180
	Промежуточная аттестация	12										
	Всего:	660	328	162		164	164		26		108	180

3.2 Содержание обучения по профессиональному модулю (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов	Уровень освоения
Раздел 1 МДК. 03.01 Эксплуатация сетевой инфраструктуры		144	
Тема 1.1 Эксплуатация объектов сетевой инфраструктуры	<p>Содержание</p> <p>Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети.</p> <p>Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.</p> <p>Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб).</p> <p>Наращивание длины сегментов сети Замена существующей аппаратуры.</p> <p>Увеличение количества узлов сети; увеличение протяженности связей между объектами сети</p> <p>Физическая карта всей сети. Логическая топология компьютерной сети.</p> <p>Техническая и проектная документация. Паспорт технических устройств.</p> <p>Основные этапы эксплуатации сетевой инфраструктуры.</p> <p>Технологии мониторинга и управления сетевыми ресурсами</p> <p>Разработка стратегии резервного копирования данных сетевой инфраструктуры. Оценка производительности и оптимизация работы сетевых устройств.</p> <p>Исследование взаимодействия сетевой инфраструктуры с системами управления и хранения данных.</p> <p>Использование технологий виртуализации для оптимизации сетевой инфраструктуры.</p> <p>Интеграция и управление сетевыми устройствами различных производителей.</p> <p>Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры.</p> <p>Проверка объектов сетевой инфраструктуры и профилактические работы.</p> <p>Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.</p> <p>Программное обеспечение мониторинга компьютерных сетей и сетевых устройств. Анализ функциональных особенностей программного обеспечения мониторинга</p> <p>Протокол SNMP, его характеристики, формат сообщений, набор услуг.</p> <p>Анализ основных характеристик протокола SNMP, его структуры и архитектуры, формата сообщений и спецификации синтаксиса</p> <p>Оборудование для диагностики и сертификации кабельных систем.</p> <p>Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.</p>	<p>72</p> <p>36</p>	<p>1</p>

	Практические занятия	36	
	Практическое занятие № 1 (Практическая подготовка) Оконцовка кабеля витая пара	36	2
	Практическое занятие № 2 (Практическая подготовка) Заделка кабеля витая пара в розетку		
	Практическое занятие № 3 (Практическая подготовка) Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену		
	Практическое занятие № 4 (Практическая подготовка) Тестирование кабеля. Поддержка пользователей сети.		
	Практическое занятие № 5 (Практическая подготовка) Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы)		
	Практическое занятие № 6 (Практическая подготовка) Выполнение действий по устранению неисправностей. Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.		
	Практическое занятие № 7 (Практическая подготовка) Оформление технической документации, правила оформления документов		
	Практическое занятие № 8 (Практическая подготовка) Протокол управления SNMP. Основные характеристики протокола SNMP. Набор услуг (PDU) протокола SNMP. Формат сообщений SNMP.		
	Практическое занятие № 9 (Практическая подготовка) Задачи управления: анализ производительности сети, анализ надежности сети		
	Практическое занятие № 10 (Практическая подготовка) Управление безопасностью в сети. Учет трафика в сети		
	Практическое занятие № 11 (Практическая подготовка) Средства мониторинга компьютерных сетей. Средства анализа сети с помощью команд сетевой операционной системы		
	Практическое занятие № 12 (Практическая подготовка) Развитие сетевой инфраструктуры в контексте IoT (Internet of Things).		
	Практическое занятие № 13 (Практическая подготовка) Оценка и управление рисками, связанными с эксплуатацией сетевой инфраструктуры ²		
	Практическое занятие № 15 (Практическая подготовка) Анализ влияния обновлений и изменений на работу сетевой инфраструктуры.		
	Практическое занятие № 16 (Практическая подготовка) Исследование проблем масштабирования и расширения сетевой инфраструктуры		
Тема 1.2 Эксплуатация систем IP-телефонии	Содержание		
	Настройка H.323. Описание H.323 и общие рекомендации. Функциональные компоненты H.323. Установка и поддержка соединения H.323.	32	1
	Соединения без и с использованием GateKeeper. Соединения с использованием нескольких		

GateKeeper. Многопользовательские конференции. Обеспечение отказоустойчивости.		
Настройка SIP. Описание и общие рекомендации. Технология SIP и связанные с ней стандарты. Функциональные компоненты SIP.		
Сообщения SIP. Адресация SIP. Модель установления соединения. Планирование отказоустойчивости.		
Установка и инсталляция программного коммутатора. Монтажные процедуры. Процедуры инсталляции. Управление аппаратными средствами и портами.		
Протоколы управления MGCP, H.248. Создание аналоговых абонентов. Внутрисканционная маршрутизация.		
Управление программным коммутатором. Маршрутизация. Группы соединительных линий. Подключение станций с TDM (абонентский доступ TDM).		
Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP -абоненты. Группы абонентов. Дополнительные абонентские услуги.		
Организация эксплуатации систем IP-телефонии. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт		
Практические занятия	30	
Практическое занятие № 17 (Практическая подготовка) Настройка и устранение неполадок службы DNS	30	2
Практическое занятие № 18 (Практическая подготовка) Поддержка ADDS		
Практическое занятие № 19 (Практическая подготовка) Управление пользовательскими и служебными учетными записями		
Практическое занятие № 20 (Практическая подготовка) Внедрение инфраструктуры Групповых политик		
Практическое занятие № 21 (Практическая подготовка) Управление пользовательским рабочим столом через Групповую политику		
Практическое занятие № 22 (Практическая подготовка) Установка и настройка роли Сервер Сетевой политики		
Практическое занятие № 23 (Практическая подготовка) Применение защиты доступа к сети		
Практическое занятие № 24 (Практическая подготовка) Внедрение технологии DirectAccess с помощью мастера начальной настройки		
Практическое занятие № 25 (Практическая подготовка) Развертывание расширенной инфраструктуры DirectAccess		
Практическое занятие № 26 (Практическая подготовка) Внедрение VPN		
Практическое занятие № 27 (Практическая подготовка) Внедрение Web Application Proxy		

	Практическое занятие № 28 (Практическая подготовка) Настройка Квот и файлового экранирования в FSRM		
	Практическое занятие № 29 (Практическая подготовка) Применение DFS		
	Практическое занятие № 30 (Практическая подготовка) Настройка шифрования и расширенного аудита		
	Практическое занятие № 31 (Практическая подготовка) Использование службы развертывания Windows для развертывания WindowsServer 2012		
	Практическое занятие № 32 (Практическая подготовка) Внедрение управления обновлениями		
	Практическое занятие № 33 (Практическая подготовка) Мониторинг WindowsServer 2012		
Самостоятельная работа при изучении раздела 1		10	
Тематика самостоятельной работы: подготовка презентаций на темы: 1 Анализ безопасности сетевой инфраструктуры и методы защиты от угроз. 2 Разработка плана восстановления после катастрофы для сетевой инфраструктуры 3 Оценка возможностей и проблем облачных технологий в сетевой инфраструктуре. 4 Исследование применения SDN (Software-Defined Networking) в сетевой инфраструктуре		10	3
Промежуточная аттестация по МДК.03.01 в форме семестрового контроля			
Раздел 2 МДК.03.02 Технологии автоматизации технологических процессов		108	
Тема 2.1. Автоматизированные системы управления технологическими процессами (АСУ ТП)	Содержание	38	
	Понятие об объекте управления. Свойства объекта управления.	20	1
	Классификация технологических объектов управления по типу, характеру технологического процесса, по характеристике параметров управления		
	Классификация систем управления технологическими объектами по способу, цели и степени централизации управления.		
	Общие сведения об автоматизированных системах управления технологическими процессами (АСУТП) и системах автоматического управления (САУ)		
	Основные функции АСУТП и САУ. Техническое, программное и информационное обеспечение АСУТП		
	Структура АСУТП на базе микропроцессорной техники.		
	Средства измерения преобразования и регулирования в АСУТП		
	Основные понятия автоматизированной обработки информации		
	Методы и средства моделирования технологических процессов в АСУТП		
	Обзор современных технологий и тенденций развития АСУТП		
Оценка эффективности и экономическая оценка внедрения АСУТП			

	Особенности управления производственными системами в условиях неопределенности и переменных условий работы		
	Применение систем искусственного интеллекта в АСУТП: нейронные сети, генетические алгоритмы, экспертные системы		
	Практические занятия	18	
	Практическое занятие № 1 (Практическая подготовка) Определение свойств объектов управления на практике	18	2
	Практическое занятие № 2 (Практическая подготовка) Классификация технологических объектов управления на примере производственного предприятия		
	Практическое занятие № 3 (Практическая подготовка) Анализ и сравнение систем управления технологическими объектами на примере различных отраслей промышленности		
	Практическое занятие № 4 (Практическая подготовка) Изучение принципов работы АСУТП и САУ на примере реальных систем управления		
	Практическое занятие № 5 (Практическая подготовка) Создание простой модели технологического процесса		
	Практическое занятие № 6 (Практическая подготовка) Ознакомление с современными технологиями АСУТП на примере существующих проектов и исследований		
	Практическое занятие № 7 (Практическая подготовка) Настройка и проверка работоспособности элементов АСУТП на примере конкретной системы управления		
	Практическое занятие № 8 (Практическая подготовка) Интеграция АСУТП с другими системами и оборудованием в производственном процессе		
	Практическое занятие № 9 (Практическая подготовка) Разработка системы управления производственными процессами в условиях неопределенности и переменных условий работы		
	Практическое занятие № 10 (Практическая подготовка) Применение экспертных систем в системах управления технологическими процессами		
	Практическое занятие № 11 (Практическая подготовка) Создание проекта автоматизации управления технологическим процессом на основе АСУТП		
Тема 2.2. Промышленные сетевые технологии и протоколы в АСУ ТП	Содержание	52	
	Роль и место сетевых технологий в промышленной автоматизации. Обзор сетевых технологий, их роль в промышленной автоматизации, а также их преимущества и недостатки.	24	1
	Основные типы промышленных сетей, их характеристики и особенности, а также методы их реализации. Протоколы связи, используемые в промышленной автоматизации, их особенности и применение.		
	Требования к промышленным сетям. Базовые подходы к их реализации. Описание основных		

<p>требований к сетям промышленной автоматизации</p> <p>Протокол MODBUS. Описание основных характеристик и принципов работы промышленного протокола связи MODBUS, включая формат кадра, адресацию, коды функций, методы передачи данных и возможности расширения.</p> <p>Типовые применения и устройства, работающие по протоколу MODBUS. Общие принципы организации работы различных устройств при использовании протокола MODBUS</p> <p>Принципы взаимодействия устройств, работающих на протоколе MODBUS, включая правила обмена данными, формат адресации, типы запросов и ответов, а также типы данных, поддерживаемые протоколом.</p> <p>Организация работы в протоколе MODBUS контроллера (slave) и операторной панели (master)</p> <p>Основные принципы работы в режимах slave и master, а также процедуры обмена данными между ними с использованием протокола MODBUS.</p> <p>Выравнивание адресов переменных в поле памяти протокола. Принципы работы с адресацией переменных в протоколе MODBUS.</p> <p>Основные требования к адресации и выравниванию данных в поле памяти протокола, а также способы решения возникающих проблем. Типовые ошибки при работе с адресацией и их предотвращение.</p> <p>Работа контроллера (master) в сети с модулями ввода/вывода (slave). Основные принципы взаимодействия контроллера и устройств ввода-вывода посредством сетевых протоколов.</p> <p>Протоколы MODBUS RTU и MODBUS TCP, их особенности и правила использования при работе контроллера как в режиме master, так и в режиме slave.</p> <p>Порядок настройки параметров соединения и обмена данными между контроллером и устройствами ввода-вывода, анализируются возможные проблемы при работе в сети и способы их устранения.</p> <p>Работа в сети по протоколу MODBUS RTU с различными устройствами. Основные аспекты протокола MODBUS RTU.</p> <p>Настройка и конфигурация устройств, анализ протокола обмена и методы диагностики проблем, возникающих в работе сети MODBUS RTU.</p> <p>Работа в сети по протоколу MODBUS TCP. Основы протокола MODBUS TCP (форматы сообщений, структуру транзакций), способы обмена данными между устройствами, а также настройку и конфигурацию сети MODBUS TCP и ее устройств.</p> <p>Современные технологии и инструменты для мониторинга и управления сетью MODBUS TCP, такие как SCADA-системы и ПО для сетевого анализа.</p> <p>Типовые промышленные проводные и кабельные сетевые протоколы. Различные сетевые протоколы, используемые в промышленных сетях для обмена данными между устройствами автоматизации и управления технологическими процессами (протоколы, PROFIBUS, CAN, Ethernet/IP, DeviceNet, Modbus, Foundation Fieldbus, AS-i и другие).</p> <p>Особенности и принципы работы каждого протокола, его преимущества и недостатки, а также способы настройки и конфигурирования сетей с использованием этих протоколов.</p> <p>Беспроводные локальные сети для промышленного применения. Технологии беспроводной связи,</p>		
--	--	--

	используемых в промышленности, таких как Wi-Fi, Bluetooth, Zigbee, LoRa, NB-IoT.		
	Особенности использования беспроводных сетей в промышленном окружении, такие как требования к надежности и безопасности, особенности развертывания и конфигурирования, а также методы мониторинга и управления беспроводными сетями.		
	Преобразователи интерфейсов. Преобразователи интерфейсов для различных стандартов связи (RS-232, RS-485, Ethernet, USB).		
	Выбор и настройка преобразователей интерфейсов в соответствии с требованиями конкретной задачи.		
	Практические занятия	28	
	Практическое занятие № 12 (Практическая подготовка) Работа с основными сетевыми технологиями в промышленной автоматизации	28	2
	Практическое занятие № 13 (Практическая подготовка) Разработка схемы промышленной сети и выбор средств ее реализации		
	Практическое занятие № 14 (Практическая подготовка) Практическое применение протокола MODBUS для обмена данными между устройствами		
	Практическое занятие № 15 (Практическая подготовка) Создание конфигурации сети с использованием протокола MODBUS		
	Практическое занятие № 16 (Практическая подготовка) Организация работы контроллера (slave) и операторной панели (master) по протоколу MODBUS		
	Практическое занятие № 17 (Практическая подготовка) Выравнивание адресов переменных в поле памяти протокола MODBUS		
	Практическое занятие № 18 (Практическая подготовка) Настройка работы контроллера (master) с модулями ввода/вывода (slave) по протоколу MODBUS RTU		
	Практическое занятие № 19 (Практическая подготовка) Практическая работа с различными устройствами по протоколу MODBUS RTU		
	Практическое занятие № 20 (Практическая подготовка) Работа с протоколом MODBUS TCP		
	Практическое занятие № 21 (Практическая подготовка) Работа с типовыми проводными и кабельными протоколами в промышленности		
	Практическое занятие № 22 (Практическая подготовка) Изучение беспроводных локальных сетей для промышленного применения		
	Практическое занятие № 23 (Практическая подготовка) Работа с преобразователями интерфейсов в промышленной сети		
	Практическое занятие № 24 (Практическая подготовка) Особенности применения промышленных сетевых протоколов в условиях высоких нагрузок и плохой связи		
	Практическое занятие № 25 (Практическая подготовка) Сравнительный анализ промышленных Ethernet-технологий: EtherNet/IP, PROFINET, Modbus TCP		
Консультация		2	

Самостоятельная работа при изучении раздела 2		6	
Тематика самостоятельной работы: подготовка презентаций на темы: 1 Специализированные сетевые интерфейсы для умного дома. Различные протоколы и технологии, используемые в системах умного дома (ZigBee, Z-Wave, Thread, Bluetooth, Wi-Fi и другие). Особенности их применения в системах автоматизации умного дома. Аспекты безопасности и защиты данных в системах умного дома, возможности интеграции различных устройств и систем в одну сеть. 2 Современные тенденции развития сетевых технологий в АСУ ТП – web-серверы и облачные решения. Подходы к организации сетевых технологий в автоматизированных системах управления технологическими процессами, основанных на использовании web-серверов и облачных решений. Основные принципы построения web-серверов и их взаимодействия с устройствами АСУ ТП, возможности использования облачных решений для удаленного мониторинга и управления технологическими процессами. 3 Конфигурирование и настройка сетевых устройств для автоматизации технологических процессов. Процесс настройки и конфигурирования сетевых устройств для автоматизации технологических процессов в промышленности: изучение различных протоколов связи, настройка устройств на работу в сети, а также определение настроек безопасности и мониторинга сетевой активности. 4 Особенности применения промышленных сетевых протоколов в условиях высоких нагрузок и плохой связи. Проблемы, возникающие при передаче данных в промышленных сетях в условиях высоких нагрузок и плохой связи. Изучение методов решения этих проблем с использованием специализированных промышленных сетевых протоколов. Методы оптимизации пропускной способности сетей и уменьшения задержек передачи данных. 5 Сравнительный анализ промышленных Ethernet-технологий: EtherNet/IP, PROFINET, Modbus TCP. Обзор и анализ особенностей трех промышленных Ethernet-протоколов: EtherNet/IP, PROFINET и Modbus TCP. Различия между этими протоколами, их преимущества и недостатки, области применения в промышленных сетях и АСУ ТП. 6 Применение промышленных маршрутизаторов для обеспечения безопасности и надежности работы сетевой инфраструктуры. Роль промышленных маршрутизаторов в обеспечении безопасности и надежности работы сетевой инфраструктуры в промышленной среде. Основные функции промышленных маршрутизаторов (виртуальная частная сеть (VPN), брандмауэр, NAT-трансляция), их конфигурация и настройка. Методы защиты от внешних атак и обеспечения надежности работы сетевой инфраструктуры.			3
Самостоятельная работа (подготовка к экзамену)		4	
Промежуточная аттестация по МДК.03.02 в форме экзамена по модулю		6	
Раздел 3			
МДК 03.03. Безопасность сетевой инфраструктуры		108	
Тема 3.1. Безопасность компьютерных сетей	Содержание	30	
	Фундаментальные принципы безопасной сети. Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.	16	1
	Безопасность сетевых устройств OSI. Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.		
	Авторизация, аутентификация и учет доступа (AAA). Свойства AAA. Локальная AAA аутентификация. Server-based AAA		
	Реализация технологий брандмауэра ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах.		

Реализация технологий предотвращения вторжения. IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS		
Безопасность локальной сети. Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN		
Криптографические системы. Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей		
Реализация технологий VPN. 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 CDP. Реализация Remote-access VPN		
Управление безопасной сетью. Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасностью. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности.		
Безопасность облачных вычислений. Особенности безопасности облачных вычислений, риски и угрозы. Защита от атак в облачной среде, использование механизмов контроля доступа, мониторинга и аудита, а также методов криптографической защиты данных.		
Межсетевая безопасность. Методы обеспечения безопасности взаимодействия между различными сетями. Реализация технологий маршрутизации и шлюзов, использование межсетевых экранов, технологии виртуальных локальных сетей.		
Cisco ASA. Введение в Адаптивное устройство безопасности ASA. Конфигурация фаервола на базе ASA с использованием графического интерфейса ASDM. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM.		
Защита компьютеров предприятия от вредоносных программ и потерь данных. Обзор System Center 2012 Endpoint Protection. Настройка Endpoint Protection Client Settings и мониторинга состояния. Использование Windows Intune Endpoint Protection. Защита клиентских ОС с помощью System Center 2012 Data Protection Manager. Настройка и развертывание политик EndpointProtection. Настройка параметров клиента для поддержки Endpoint Protection. Мониторинг защиты конечных точек. Настройка и проверка защиты данных клиента		
Мониторинг производительности и работоспособности инфраструктуры клиентских ОС. Производительность и работоспособность инфраструктуры клиентских ОС. Мониторинг инфраструктуры виртуальных клиентов. Настройка Operations Manager для мониторинга виртуальных сред.		
Практические занятия	14	
Практическое занятие № 1 (Практическая подготовка) Оценка и определение параметров развертывания	14	2
Практическое занятие № 2 (Практическая подготовка) Планирование стратегии управления образами. Создание и обслуживание эталонного образа		

	Практическое занятие № 3 (Практическая подготовка) Настройка безопасности клиентских систем		
	Практическое занятие № 4 (Практическая подготовка) Настройка и управление Windows Deployment Services Планирование среды Windows Deployment Services		
	Практическое занятие № 5 (Практическая подготовка) Подготовка среды для развертывания операционной системы		
	Практическое занятие № 6 (Практическая подготовка) Использование MDT и Configuration Manager для подготовки Zero-Touch Installation		
	Практическое занятие № 7 (Практическая подготовка) Планирование и реализация инфраструктуры Remote Desktop Services. Расширение доступа к Интернет для инфраструктуры RDS		
	Практическое занятие № 8 (Практическая подготовка) Мониторинг производительности и работоспособности инфраструктуры клиентских ОС Настройка		
Тема 3.2. Обеспечение сетевой безопасности	Содержание	72	
	Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть.	34	1
	Механизмы шифрования и аутентификации для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам и сервисам.		
	Использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.		
	Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети.		
	Методы минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.		
	Введение системы обнаружения и предотвращения сетевых вторжений.		
	Технологии использования виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа.		
	Использование системы управления доступом для контроля доступа к корпоративной сети.		
	Обеспечение безопасности Wi-Fi-сетей.		
	Реализация мер по обеспечению безопасности электронной почты в корпоративной сети.		
	Защита от атак типа "фишинг".		
	Применение антивирусного программного обеспечения для защиты от вирусов и других вредоносных программ.		
	Использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.		
	Защита от DDoS-атак.		
	Защита от внутренних угроз безопасности.		
	Обеспечение безопасности облачных сервисов.		

Введение системы контроля целостности файлов для защиты от изменения или внедрения вредоносных программ в файловые системы.		
Применение методов шифрования данных для защиты от несанкционированного доступа к конфиденциальной информации.		
Практические занятия	38	
Практическое занятие № 9 (Практическая подготовка) Настройка VPN-туннелей для организации защищенных каналов передачи данных между территориально распределенными офисами.	38	2
Практическое занятие № 10 (Практическая подготовка) Работа с механизмами шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.		
Практическое занятие № 11 (Практическая подготовка) Настройка и использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.		
Практическое занятие № 12 (Практическая подготовка) Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети с использованием программного обеспечения для мониторинга и обнаружения угроз.		
Практическое занятие № 13 (Практическая подготовка) Разработка и внедрение мер по минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях		
Практическое занятие № 14 (Практическая подготовка) Настройка и работа с системами обнаружения и предотвращения сетевых вторжений для раннего обнаружения, и предотвращения угроз безопасности.		
Практическое занятие № 15 (Практическая подготовка) Настройка и использование виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.		
Практическое занятие № 16 (Практическая подготовка) Настройка и работа с системами управления доступом для контроля доступа к корпоративной сети.		
Практическое занятие № 17 (Практическая подготовка) Обеспечение безопасности Wi-Fi-сетей: настройка безопасных точек доступа, использование сетевой аутентификации, шифрования трафика и других методов.		
Практическое занятие № 18 (Практическая подготовка) Разработка и внедрение мер по обеспечению безопасности электронной почты в корпоративной сети: настройка антивирусного программного обеспечения, проверка на наличие вредоносных вложений, обучение пользователей основам безопасности электронной почты.		
Практическое занятие № 19 (Практическая подготовка) Обучение пользователям основам защиты от атак типа "фишинг".		
Практическое занятие № 20 (Практическая подготовка)		

	Работа с антивирусным программным обеспечением для защиты от вирусов и других вредоносных программ: установка, настройка, обновление базы данных, сканирование и удаление вредоносных программ.		
	Практическое занятие № 21 (Практическая подготовка) Настройка и использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.		
	Практическое занятие № 22 (Практическая подготовка) Настройка и использование межсетевых экранов и фаерволов для обеспечения комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.		
	Практическое занятие № 23 (Практическая подготовка) Внедрение системы управления доступом для контроля доступа к корпоративной сети: настройка правил доступа, аутентификация пользователей, управление привилегиями.		
	Практическое занятие № 24 (Практическая подготовка) Использование технологий виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа: настройка и управление VPN-туннелями, защита данных, маршрутизация трафика.		
	Практическое занятие № 25 (Практическая подготовка) Обеспечение безопасности Wi-Fi-сетей: настройка и управление беспроводными точками доступа, защита сетевого трафика, аутентификация пользователей		
	Практическое занятие № 26 (Практическая подготовка) Защита от DDoS-атак: использование специализированных средств защиты от DDoS-атак, настройка маршрутизации трафика, мониторинг сетевой активности		
	Практическое занятие № 27 (Практическая подготовка) Обеспечение безопасности облачных сервисов: выбор надежных провайдеров облачных сервисов, настройка правил доступа и аутентификации, шифрование данных, мониторинг активности в облачных сервисах.		
Самостоятельная работа при изучении раздела 3		6	
Тематика самостоятельной работы: подготовка презентаций на темы: 1 Безопасность веб-приложений и мобильных устройств. Особенности уязвимостей веб-приложений, методы их эксплуатации, а также средства защиты. Разработка безопасных веб-приложений, использование методов автоматического тестирования и уязвимости. Угрозы безопасности мобильных устройств, методы защиты от вредоносных программ, защита данных и коммуникаций, а также безопасное использование мобильных устройств. 2 Защита от социальной инженерии. Методы социальной инженерии, опасности, связанные с подделкой и манипулированием данными, а также методы защиты и обучения персонала.		6	3
Промежуточная аттестация по МДК.03.03 в форме семестрового контроля			
Учебная практика Эксплуатация объектов сетевой инфраструктуры (по выбору)		108	
Виды работ Настройка прав доступа. Оформление технической документации, правила оформления документов.			3

<p>Настройка аппаратного и программного обеспечения сети. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain. Программная диагностика неисправностей. Аппаратная диагностика неисправностей. Поиск неисправностей технических средств. Выполнение действий по устранению неисправностей. Использование активного, пассивного оборудования сети. Устранение паразитирующей нагрузки в сети. Построение физической карты локальной сети. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети. Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть Обеспечение безопасности Wi-Fi-сетей. Реализация мер по обеспечению безопасности электронной почты в корпоративной сети. Защита от атак типа "фишинг". Обеспечение сетевой безопасности</p>			
Вид работы 1	Содержание	2	
Настройка прав доступа.	1 Настройка прав доступа. 2 Оформление технической документации, правила оформления документов.	2	
Вид работы 2	Содержание	2	
Оформление технической документации, правила оформления документов.	1 Оформление документации 2 Правила оформления	2	
Вид работы 3	Содержание	2	
Настройка аппаратного и программного обеспечения сети.	1 Настройка аппаратного и программного обеспечения сети 2 Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain	2	
Вид работы 4	Содержание	2	
Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain.	1 Присоединение компьютера к домену 2 Присоединение сервера к домену	2	
Вид работы 5	Содержание	4	
Программная диагностика неисправностей.	1 Программная диагностика неисправностей	4	
Вид работы 6	Содержание	4	
Аппаратная диагностика неисправностей.	1 Аппаратная диагностика неисправностей	4	
Вид работы 7	Содержание	4	
Поиск неисправностей технических средств.	1 Поиск неисправностей технических средств 2 Выполнение действий по устранению неисправностей	4	

Вид работы 8 Выполнение действий по устранению неисправностей	Содержание	4	
	1 Проблема 2 Диагностика проблемы 3 Устранение проблемы	4	
Вид работы 9 Использование активного, пассивного оборудования сети	Содержание	4	
	1 Устранение паразитирующей нагрузки в сети 2 Построение физической карты локальной сети	4	
Вид работы 10 Устранение паразитирующей нагрузки в сети.	Содержание	4	
	1 Мониторинг и оповещение 2 Исследование 3 Изоляция 4 Анализ причин возникновения проблемы и ее устранение	4	
Вид работы 11 Построение физической карты локальной сети.	Содержание	4	
	1 Выполнение аудита 2 Хранение аудиторской информации 3 Создание карты сети 4 Представление сети на физическом уровне	4	
Вид работы 12 Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети	Содержание	12	
	1 Анализ сетевого трафика всей инфраструктуры 2 Комплексный подход к выявлению угроз и вторжений	12	
Вид работы 13 Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть	Содержание	12	
	1 Обеспечение защищенного удаленного доступа 2 Комплексная защита корпоративной сети	12	
Вид работы 14 Обеспечение безопасности Wi-Fi-сетей	Содержание	12	
	1 Обеспечение физической защиты сетевого устройства. 2 Запретите трансляцию ID сети. 3 Применяйте фильтрацию по MAC-адресам. 4 Использование эффективных протоколов безопасности беспроводных сетей.	12	
Вид работы 15 Реализация мер по обеспечению безопасности электронной почты в корпоративной сети.	Содержание	12	
	1 Выбор местоположения сервера, обеспечение сетевой безопасности 2 Контроль доступа к корпоративной почте 3 Использование шифрования для защиты сообщений электронной почты 4 Использование специализированных антивирусов 5 Средств защиты электронной почты для фильтрации спама	12	
Вид работы 16	Содержание	12	

Защита от атак типа "фишинг".	1 Меры защиты от фишинга 2 Основные объекты при фишинговых атаках	12	
Вид работы 17 Обеспечение сетевой безопасности	Содержание 1 Угрозы безопасности инфраструктуры 2 Основные риски информационной безопасности	12 12	
Производственная практика Эксплуатация объектов сетевой инфраструктуры (по выбору)		180	
Виды работ Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение. Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях. Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций. Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли. Установка прав доступа и контроль использования сетевых ресурсов. Обеспечение своевременного копирования, архивирования и резервирования данных. Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования. Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению. Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных) безопасность межсетевое взаимодействие Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций Документирование всех произведенных действий			3
Вид работы 1 Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение.	Содержание 1 Установка на серверы операционные системы и необходимое для работы программное обеспечение 2 Установка на рабочие станции операционные системы и необходимое для работы программное обеспечение	16 16	
Вид работы 2 Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях	Содержание 1 Осуществление конфигурирования программного обеспечения на серверах 2 Осуществление конфигурирования программного обеспечения на рабочих станциях	16 16	
Вид работы 3 Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций	Содержание 1 Поддержка в работоспособном состоянии программное обеспечение серверов 2 Поддержка в работоспособном состоянии программное обеспечение рабочих станций	16 16	
Вид работы 4 Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли.	Содержание 1 Регистрация пользователей локальной сети и почтового сервера, назначение идентификаторов 2 Регистрация пользователей локальной сети и почтового сервера, назначение паролей	16 16	
Вид работы 5 Установка прав доступа и контроль	Содержание 1 Установка прав доступа	16 16	

использования сетевых ресурсов.	2 Контроль использования сетевых ресурсов		
Вид работы 6 Обеспечение своевременного копирования, архивирования и резервирования данных.	Содержание 1 Обеспечение своевременного копирования, архивирования и резервирования данных	16 16	
Вид работы 7 Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования.	Содержание 1 Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования	16 16	
Вид работы 8 Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению.	Содержание 1 Выявление ошибок пользователей и программного обеспечения и принятие мер по их устранению	16 16	
Вид работы 9 Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных) безопасность межсетевого взаимодействия	Содержание 1 Обеспечение безопасности межсетевого взаимодействия	16 16	
Виды работ 10 Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций	Содержание 1 Осуществление антивирусной защиты локальной вычислительной сети, серверов 2 Осуществление антивирусной защиты рабочих станций	18 18	
Виды работ 11 Документирование всех произведенных действий	Содержание 1 Документирование всех произведенных действий	18 18	
Промежуточная аттестация по ПМ.01		12	
Всего		660	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

- 1 – ознакомительный (узнавание ранее изученных объектов, свойств);
- 2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
- 3 – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

4 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1 Материально-техническое обеспечение

Реализация программы профессионального модуля предполагает наличие лаборатории программно-аппаратной защиты объектов сетевой инфраструктуры.
Оборудование лаборатории и рабочих мест лаборатории: компьютерные рабочие станции для работы студентов.

Технические средства обучения:

- интерактивная доска с мультимедийным проектором,
- компьютер для преподавателя,
- компьютеры для студентов.

4.2 Информационное обеспечение обучения

Перечень используемых учебных изданий, интернет-ресурсов, дополнительной литературы

Основные источники:

- 1 **Шаньгин, В. Ф.** Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. – Москва : ФОРУМ : ИНФРА-М, 2021. – 416 с. – (Среднее профессиональное образование). – Текст : электронный. – URL: <https://znanium.ru/catalog/product/1189327> (дата обращения: 03.05.2024). – Режим доступа: по подписке.

Дополнительные источники:

- 2 **Назаров, А. В.** Эксплуатация объектов сетевой инфраструктуры : учебник / А. В. Назаров, А. Н. Енгальчев, В. П. Мельников. – Москва : КУРС ; ИНФРА-М, 2020. – 360 с. – (Среднее профессиональное образование). – Текст : электронный. – URL: <https://znanium.ru/catalog/product/1071722> (дата обращения: 03.05.2024). – Режим доступа: по подписке.

Интернет-ресурсы:

- 1 Обеспечение сетевой безопасности и защиты периметра [Электронный ресурс] : [сайт] . – URL: <https://acti.ru/resheniya-i-uslugi/informatcionnaia-bezopasnost/bezopasnost-it-infrastruktury/zashchita-perimetra-i-setevaia-bezopasnost> (дата обращения: 03.05.2024).

4.3 Общие требования к организации образовательного процесса

Реализация рабочей программы предусматривает возможность использования различных образовательных технологий, в том числе дистанционного обучения.
При реализации рабочей программы для обучающихся инвалидов и лиц с ограниченными возможностями здоровья предусмотрено информационное обеспечение обучения, включающее предоставление учебных материалов в различных формах.
В рамках освоения рабочей программы осуществляется практическая подготовка обучающихся. Практическая подготовка – форма организации образовательной деятельности при освоении образовательной программы в условиях выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью и направленных на формирование, закрепление, развитие практических навыков и компетенций.
Практическая подготовка осуществляется в колледже и в следующих структурных подразделениях СГУ:

- УЦИТ СГУ имени Н.Г. Чернышевского,
- а также на приведенных ниже предприятиях и в организациях:
- АО «НПП «Контакт»;
 - АО «КБПА»;

- АО «САЗ»;
- АО «НПП «Алмаз»;
- АО «Транспортное машиностроение»;
- ПАО «СЭЗ имени Серго Орджоникидзе»;
- ООО «СЭПО-ЗЭМ»;
- ООО «Источник»;
- ООО «Роберт Бош Саратов»;
- ООО «НПФ «Вымпел»;
- ООО «Геофизмаш»;
- ООО «КАРСАР»;
- ООО «Бош Пауэр Тулз»;
- АО «Саратовский полиграфический комбинат»;
- ООО Энгельское приборостроительное объединение «Сигнал»;
- АО Энгельское опытно-конструкторское бюро «Сигнал» им. А.И. Глухарева;
- ЗАО «СПГЭС»;
- ООО Завод «Саратовгазавтоматика»;
- АО «КБ «Электроприбор»;
- Саратовское отделение ООО внедренческая фирма «ЭЛНА»;
- ООО «ИНТЕРКАРА».

4.4 Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарным курсам:

наличие высшего профессионального образования, соответствующего профилю модуля «Осуществление интеграции программных модулей» 09.02.06 Сетевое и системное администрирование

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: наличие высшего профессионального образования, соответствующего профилю модуля выполнение установки, поддержки работоспособности системы, обеспечения безопасности и антивирусной защиты локальной вычислительной сети, серверов и рабочих станций

5 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Формы и методы контроля и оценки результатов обучения адаптированы для обучающихся инвалидов и лиц с ОВЗ с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости предусмотрено для них увеличение времени на подготовку к экзамену, а также предоставление дополнительного времени для подготовки ответа на экзамене и проведение аттестации в несколько этапов.

Результаты (освоенные общие и профессиональные компетенции)	Основные показатели оценки результата
<p>ПК 3.1 Осуществлять проектирование сетевой инфраструктуры. ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.</p>	<ul style="list-style-type: none"> – обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя; – выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; – осуществлять диагностику и поиск неисправностей всех компонентов сети; – выбор и применение методов и способов решения профессиональных задач в области разработки программного обеспечения для компьютерных систем; – оценка эффективности и качества выполнения профессиональных задач в области разработки программного обеспечения для компьютерных систем.
<p>ПК 3.2 Обслуживать сетевые конфигурации программно-аппаратных средств. ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях. ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.</p>	<ul style="list-style-type: none"> – поддержке пользователей сети, настройке аппаратного и программного обеспечения сетевой инфраструктуры; – выполнять действия по устранению неисправностей; – обоснованный анализ текущей ситуации; – аргументированный подбор средств для решения нестандартной профессиональной ситуации; – понимание и принятие ответственности за предложенные решения обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; – определение и выбор способа - поиск необходимой информации для эффективного выполнения профессиональных задач, профессионального и личностного развития; – использование различных источников, включая электронные для эффективного выполнения профессиональных задач, профессионального и личностного развития;
<p>ПК 3.3 Осуществлять защиту информации в сети с использованием программно-аппаратных средств. ОК 05. Осуществлять устную и</p>	<ul style="list-style-type: none"> – осуществлять настройку аппаратного и программного обеспечения сети; – точное выполнение отладки работы сети;

<p>письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.</p>	<ul style="list-style-type: none"> – выполнять действия по устранению неисправностей – работа с ПК и оформление результатов работы с использованием ИКТ; – разработка проектной и технической
<p>ПК 3.4 Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры. ОК 04. Эффективно взаимодействовать и работать в коллективе и команде.</p>	<ul style="list-style-type: none"> – выполнение восстановления и резервного копирования информации. – выполнение замены расходных материалов и мелкий ремонт периферийного оборудования; – определение устаревшего оборудования и программных средств сетевой инфраструктуры; – проявление интереса к будущей профессии; – аргументированность и полнота объяснения сущности и социальной значимости будущей профессии; – активность и инициативность в процессе освоения профессиональной деятельности; – наличие положительных отзывов по итогам учебной практики; – участие в студенческих конференциях, конкурсах, презентациях, олимпиадах и выставках технического творчества. – взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения на основе норм делового общения; – проявление готовности к обмену информацией; – проявление уважения к мнению и позиции членов коллектива
<p>ПК 3.5 Модернизировать сетевые устройства информационно-коммуникационных систем. ОК.05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.</p>	<ul style="list-style-type: none"> – организация инвентаризации технических средств сетевой инфраструктуры; – осуществление контроля оборудования после его ремонта; – владение механизмом планирования и организации собственной образовательной деятельности; – быть готовым к постоянному повышению профессионального мастерства, приобретению новых знаний; – организация самостоятельных занятий при изучении профессионального модуля; – планирование повышения личностного и квалификационного уровня, участие в выставках технического творчества – проявление интереса к инновациям в области профессиональной деятельности; – выбор оптимальных технологий в профессиональной деятельности, необходимых для решения профессиональных задач; – активное применение информационно-коммуникационных технологий в профессиональной деятельности.