Государственное бюджетное профессиональное образовательное
учреждение Республики Хакасия
Техникум коммунального хозяйства и сервиса

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

основной образовательной программы

09.02.06 Сетевое и системное администрирование

Абакан, 2025

СОДЕРЖАНИЕ ПРОГРАММЫ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«ПМ.03 Эксплуатация объектов сетевой инфраструктуры»
код и наименование модуля

1.1. Цель и место профессионального модуля в структуре образовательной программы

Цель модуля: освоение вида деятельности «Эксплуатация объектов сетевой инфраструктуры».

Профессиональный модуль включен в обязательную часть образовательной программы по выбору.

1.2. Планируемые результаты освоения профессионального модуля

Результаты освоения профессионального модуля соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника (п. 4.3.3 ПОП-П).

В результате освоения профессионального модуля обучающийся должен[1]:

Код *ОК, ПК*	**Уметь**	**Знать**	**Владеть навыками**
ОК.01	распознавать задачу и/или проблему в профессиональном и/или социальном контексте, анализировать и выделять её составные части; определять этапы решения задачи, составлять план действия, реализовывать составленный план, определять необходимые ресурсы; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; владеть актуальными методами работы в профессиональной и смежных сферах; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; структура плана для решения задач, алгоритмы выполнения работ в профессиональной и смежных областях; основные источники информации и ресурсы для решения задач и/или проблем в профессиональном и/или социальном контексте; методы работы в профессиональной и смежных сферах; порядок оценки результатов решения задач профессиональной деятельности;	

[1] *Берутся сведения, указанные по данному виду деятельности в п. 4.2.*

ОК.02	определять задачи для поиска информации, планировать процесс поиска, выбирать необходимые источники информации; выделять наиболее значимое в перечне информации, структурировать получаемую информацию, оформлять результаты поиска; оценивать практическую значимость результатов поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение в профессиональной деятельности; использовать различные цифровые средства для решения профессиональных задач;	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации, порядок их применения и программное обеспечение в профессиональной деятельности, в том числе цифровые средства;	
ОК.03	определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования; выявлять достоинства и недостатки коммерческой идеи; определять инвестиционную привлекательность	содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; основы предпринимательской деятельности, правовой и финансовой грамотности; правила разработки презентации; основные этапы разработки и реализации проекта;	

	коммерческих идей в рамках профессиональной деятельности, выявлять источники финансирования; презентовать идеи открытия собственного дела в профессиональной деятельности; определять источники достоверной правовой информации; составлять различные правовые документы; находить интересные проектные идеи, грамотно их формулировать и документировать; оценивать жизнеспособность проектной идеи, составлять план проекта;		
ОК.04	организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности;	психологические основы деятельности коллектива; психологические особенности личности;	
ОК.05	грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке; проявлять толерантность в рабочем коллективе;	правила оформления документов; правила построения устных сообщений; особенности социального и культурного контекста;	
ОК.06	проявлять гражданско-патриотическую позицию; демонстрировать осознанное поведение; описывать значимость своей специальности; применять стандарты антикоррупционного поведения;	сущность гражданско-патриотической позиции; традиционных общечеловеческих ценностей, в том числе с учетом гармонизации; межнациональных и межрелигиозных отношений; значимость	

		профессиональной деятельности по специальности; стандарты антикоррупционного поведения и последствия его нарушения;	
ОК.07	соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности; организовывать профессиональную деятельность с соблюдением принципов бережливого производства; организовывать профессиональную деятельность с учетом знаний об изменении климатических условий региона; эффективно действовать в чрезвычайных ситуациях;	правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения; принципы бережливого производства; основные направления изменения климатических условий региона; правила поведения в чрезвычайных ситуациях;	
ОК.08	использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения, характерными для данной специальности;	роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения;	
ОК.09	понимать общий смысл четко произнесенных высказываний на	правила построения простых и сложных предложений на	

	известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснять свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы;	профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности;	
ПК.3.1	проектировать локальную сеть; выбирать сетевые топологии; рассчитывать основные параметры локальной сети; применять алгоритмы поиска кратчайшего пути; планировать структуру сети с помощью графа с оптимальным расположением узлов; использовать математический аппарат теории графов; настраивать стек протоколов TCP/IP и использовать встроенные утилиты операционной системы для диагностики работоспособности сети	общие принципы построения сетей; сетевые топологии; многослойную модель OSI; требования к компьютерным сетям; архитектуру протоколов; стандартизацию сетей; этапы проектирования сетевой инфраструктуры; элементы теории массового обслуживания; основные понятия теории графов; алгоритмы поиска кратчайшего пути; основные проблемы синтеза графов атак; системы топологического анализа защищенности компьютерной сети; основы проектирования локальных сетей, беспроводные локальные сети; стандарты кабелей, основные виды коммуникационных	проектировать архитектуру локальной сети в соответствии с поставленной задачей; использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей; настраивать протоколы динамической маршрутизации; определять влияния приложений на проект сети; анализировать, проектировать и настраивать схемы потоков трафика в компьютерной сети

		устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование; средства тестирования и анализа; базовые протоколы и технологии локальных сетей	
ПК.3.2	выбирать сетевые топологии; рассчитывать основные параметры локальной сети; применять алгоритмы поиска кратчайшего пути; планировать структуру сети с помощью графа с оптимальным расположением узлов; использовать математический аппарат теории графов; использовать многофункциональные приборы и программные средства мониторинга; использовать программно-аппаратные средства технического контроля	общие принципы построения сетей; сетевые топологии; стандартизацию сетей; этапы проектирования сетевой инфраструктуры; элементы теории массового обслуживания; основные понятия теории графов; основные проблемы синтеза графов атак; системы топологического анализа защищенности компьютерной сети; архитектуру сканера безопасности; принципы построения высокоскоростных локальных сетей	устанавливать и настраивать сетевые протоколы и сетевое оборудование в соответствии с конкретной задачей; выбирать технологии, инструментальные средства при организации процесса исследования объектов сетевой инфраструктуры; создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть; выполнять поиск и устранение проблем в компьютерных сетях; отслеживать пакеты в сети и настраивать программно-аппаратные межсетевые экраны; настраивать коммутацию в корпоративной сети
ПК.3.3	использовать программно-аппаратные средства технического контроля	требования к компьютерным сетям; требования к сетевой безопасности; элементы теории массового обслуживания; основные понятия теории графов; основные проблемы синтеза графов атак; системы топологического анализа	обеспечивать целостность резервирования информации; обеспечивать безопасное хранение и передачу информации в глобальных и локальных сетях; создавать и настраивать одноранговую сеть, компьютерную сеть с помощью

		защищенности компьютерной сети; архитектуру сканера безопасности	маршрутизатора, беспроводную сеть; выполнять поиск и устранение проблем в компьютерных сетях; отслеживать пакеты в сети и настраивать программно-аппаратные межсетевые экраны; фильтровать, контролировать и обеспечивать безопасность сетевого трафика; определять влияние приложений на проект сети
ПК.3.4	читать техническую и проектную документацию по организации сегментов сети; контролировать соответствие разрабатываемого проекта нормативно-технической документации; использовать программно-аппаратные средства технического контроля; использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования	требования к компьютерным сетям; архитектуру протоколов; стандартизацию сетей; этапы проектирования сетевой инфраструктуры; организацию работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей; стандарты кабелей, основные виды коммуникационных устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы (монтаж, тестирование); средства тестирования и анализа; программно-аппаратные средства технического контроля	мониторинг производительности сервера и протоколирования системных и сетевых событий; использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей; создавать и настраивать одноранговую сеть, компьютерную сеть с помощью маршрутизатора, беспроводную сеть; создавать подсети и настраивать обмен данными; выполнять поиск и устранение проблем в компьютерных сетях; анализировать схемы потоков трафика в компьютерной сети; оценивать качество и соответствие требованиям проекта сети
ПК 3.5.	читать техническую и проектную	принципы и стандарты оформления технической	оформлять техническую документацию;

	документацию по организации сегментов сети; контролировать соответствие разрабатываемого проекта нормативно-технической документации; использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования	документации принципы создания и оформления топологии сети; информационно-справочные системы для замены (поиска) технического оборудования	определять влияние приложений на проект сети; анализировать схемы потоков трафика в компьютерной сети; оценивать качество и соответствие требованиям проекта сети

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Трудоемкость освоения модуля

Наименование составных частей модуля	**Объем в часах**
Учебные занятия	208
Курсовая работа (проект)	60
Самостоятельная работа	
Практика, в т.ч.:	252
учебная	144
производственная	108
Промежуточная аттестация	18
Всего	**520**

2.2. Структура профессионального модуля

Код ОК, ПК	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Обучение по МДК, в т.ч.:	Учебные занятия	Курсовая работа (проект)	Самостоятельная работа[2]	Учебная практика	Производственная практика
1	2	3	4	5	6	7	8	9	10
ОК.01 – ОК.09 ПК3.1 - ПК3.4	Раздел 1. Технологии автоматизации технологических процессов	**64**	**34**						
ОК.01 – ОК.09 ПК3.1 - ПК3.4	Раздел 2. Безопасность сетевой инфраструктуры	**102+64**	**36**						
ОК.01 – ОК.09 ПК3.1 - ПК3.4	Раздел 3. Эксплуатация сетевой инфраструктуры	**102+36**	**36**						
ОК.01 – ОК.09 ПК3.1 - ПК3.4	Учебная практика	**102**	**102**					**102**	
ОК.01 – ОК.09 ПК3.1 - ПК3.4	Производственная практика	**252**	**252**						**252**
	Промежуточная аттестация	**18**							
	Всего:	***750***	**358**					**102**	**252**

[2] *Самостоятельная работа в рамках образовательной программы планируется образовательной организацией.*

2.3. Содержание профессионального модуля

Наименование разделов и тем	Содержание учебного материала, практических и лабораторных занятия, *курсовой проект (работа)*
Раздел 1. Эксплуатация сетевой инфраструктуры 64 час.	
МДК.03.01. Эксплуатация сетевой инфраструктуры	
Тема 1.1 Эксплуатация объектов сетевой инфраструктуры	**Содержание**
	1. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.
	2. Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб).
	3. Наращивание длины сегментов сети Замена существующей аппаратуры. Увеличение количества узлов сети; увеличение протяженности связей между объектами сети
	4. Физическая карта всей сети Логическая топология компьютерной сети. Техническая и проектная документация. Паспорт технических устройств.
	5. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры. Проверка объектов сетевой инфраструктуры и профилактические работы.
	6. Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.
	7. Программное обеспечение мониторинга компьютерных сетей и сетевых устройств. Анализ функциональных особенностей программного обеспечения мониторинга, определение методов и алгоритмов, используемых в процессе мониторинга, изучение основных принципов выбора программного обеспечения мониторинга для конкретной сети или устройства на основе учета их параметров и особенностей работы, анализ возможностей современного программного обеспечения мониторинга и определение эффективных подходов к использованию этих возможностей в практических задачах мониторинга компьютерных сетей и сетевых устройств.
	8. Протокол SNMP, его характеристики, формат сообщений, набор услуг. Анализ основных характеристик протокола SNMP, его структуры и архитектуры, формата сообщений и спецификации синтаксиса
	9. Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.
	В том числе практических занятий и лабораторных работ

	Практическое занятие 1. Оконцовка кабеля витая пара
	Практическое занятие 2. Заделка кабеля витая пара в розетку
	Практическое занятие 3. Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену
	Практическое занятие 4. Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы)
	Практическое занятие 5. Выполнение действий по устранению неисправностей. Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.
	Практическое занятие 6. Оформление технической документации, правила оформления документов
	Практическое занятие 7. Протокол управления SNMP. Основные характеристики протокола SNMP. Набор услуг (PDU) протокола SNMP. Формат сообщений SNMP.
	Практическое занятие 8.Задачи управления: анализ производительности сети, анализ надежности сети
	Практическое занятие 9. Управление безопасностью в сети. Учет трафика в сети
	Практическое занятие 10. Средства мониторинга компьютерных сетей. Средства анализа сети с помощью команд сетевой операционной системы
Тема 1.2 Эксплуатация систем IP-телефонии	**Содержание**
	1. Настройка H.323. Описание H.323 и общие рекомендации. Функциональные компоненты H.323.Установка и поддержка соединения H.323. Соединения без и с использованием GateKeeper. Соединения с использованием нескольких GateKeeper. Многопользовательские конференции. Обеспечение отказоустойчивости.
	2. 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.
	3. Установка и инсталляция программного коммутатора. Монтажные процедуры. Процедуры инсталляции. Управление аппаратными средствами и портами. Протоколы управления MGCP, H.248. Создание аналоговых абонентов. Внутристанционная маршрутизация.
	4. 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.
	5. Организация эксплуатации систем IP-телефонии. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт
	6. Восстановление работы сети после аварии. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы рабоы хранилищ данных;

	В том числе практических занятий и лабораторных работ
	Практическое занятие 1. Настройка аппаратных и программных IP-телефонов, факсов
	Практическое занятие 2. Развертывание сети с использованием VLAN для IP-телефонии. Настройка шлюза
	Практическое занятие 3. Установка, подключение и первоначальные настройки голосового маршрутизатора. Настройка таблицы пользователей, настройка групп, настройка голосовых сообщений в голосовом маршрутизаторе.
	Практическое занятие 4. Настройка программно-аппаратной IP-АТС. Установка и настройка программной IP-АТС (например, Asterisk).
	Практическое занятие 5. Мониторинг и анализ соединений по различным протоколам. Мониторинг вызовов в программном коммутаторе
	Практическое занятие 6. Создание резервных копий баз данных
	Практическое занятие 7. Диагностика и устранение неисправностей в системах IP-телефонии
Раздел 2. Технологии автоматизации технологических процессов 72 часа	
МДК.03.02. Технологии автоматизации технологических процессов	
Тема 2.1. Автоматизированные системы управления технологическими процессами (АСУ ТП)	**Содержание**
	1. Понятие об объекте управления. Свойства объекта управления.
	2. Классификация технологических объектов управления по типу, характеру технологического процесса, по характеристике параметров управления
	3. Классификация систем управления технологическими объектами по способу, цели и степени централизации управления.
	4. Общие сведения об автоматизированных системах управления технологическими процессами (АСУТП) и системах автоматического управления (САУ)
	5. Основные функции АСУТП и САУ. Техническое, программное и информационное обеспечение АСУТП
	6. Структура АСУТП на базе микропроцессорной техники.
	7. Средства измерения преобразования и регулирования в АСУТП
	8. Основные понятия автоматизированной обработки информации
	9. Методы и средства моделирования технологических процессов в АСУТП
	10. Обзор современных технологий и тенденций развития АСУТП
	11. Программирование и настройка АСУТП: языки программирования, методы и инструменты
	12. Интеграция АСУТП с другими системами и оборудованием в производственном процессе
	13. Оценка эффективности и экономическая оценка внедрения АСУТП
	14. Особенности управления производственными системами в

	условиях неопределенности и переменных условий работы
	15. Применение систем искусственного интеллекта в АСУТП: нейронные сети, генетические алгоритмы, экспертные системы
	В том числе практических занятий и лабораторных работ
	Практическое занятие 1. Определение свойств объектов управления на практике
	Практическое занятие 2. Классификация технологических объектов управления на примере производственного предприятия
	Практическое занятие 3. Анализ и сравнение систем управления технологическими объектами на примере различных отраслей промышленности
	Практическое занятие 4. Изучение принципов работы АСУТП и САУ на примере реальных систем управления
	Практическое занятие 5. Создание простой модели технологического процесса
	Практическое занятие 6. Ознакомление с современными технологиями АСУТП на примере существующих проектов и исследований
	Практическое занятие 7. Программирование элементов АСУТП на языках программирования на практике
	Практическое занятие 8. Настройка и проверка работоспособности элементов АСУТП на примере конкретной системы управления
	Практическое занятие 9. Интеграция АСУТП с другими системами и оборудованием в производственном процессе
	Практическое занятие 10. Оценка эффективности и экономическая оценка внедрения АСУТП
	Практическое занятие 11. Разработка системы управления производственными процессами в условиях неопределенности и переменных условий работы
	Практическое занятие 12. Применение нейронных сетей в системах управления технологическими процессами
	Практическое занятие 13. Применение экспертных систем в системах управления технологическими процессами
	Практическое занятие 14. Создание проекта автоматизации управления технологическим процессом на основе АСУТП
Тема 2.2. Промышленные сетевые технологии и протоколы в АСУ ТП	**Содержание**
	1. Роль и место сетевых технологий в промышленной автоматизации Обзор сетевых технологий, их роль в промышленной автоматизации, а также их преимущества и недостатки. Основные типы промышленных сетей, их характеристики и особенности, а также методы их реализации. Протоколы связи, используемые в промышленной автоматизации, их особенности и применение.
	2. Требования к промышленным сетям. Базовые подходы к их реализации Описание основных требований к сетям промышленной автоматизации, в том числе по надежности, пропускной способности и управляемости, а также базовых подходов к проектированию и реализации промышленных сетей, включая выбор типа сети, топологию, средства передачи данных, сетевые

	протоколы и системы безопасности.
	3. Протокол MODBUS Описание основных характеристик и принципов работы промышленного протокола связи MODBUS, включая формат кадра, адресацию, коды функций, методы передачи данных и возможности расширения. Также рассматриваются типовые применения и устройства, работающие по протоколу MODBUS.
	4. Общие принципы организации работы различных устройств при использовании протокола MODBUS Принципы взаимодействия устройств, работающих на протоколе MODBUS, включая правила обмена данными, формат адресации, типы запросов и ответов, а также типы данных, поддерживаемые протоколом.
	5. Организация работы в протоколе MODBUS контроллера (slave) и операторной панели (master) Основные принципы работы в режимах slave и master, а также процедуры обмена данными между ними с использованием протокола MODBUS.
	6. Выравнивание адресов переменных в поле памяти протокола Принципы работы с адресацией переменных в протоколе MODBUS. 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.
	7. Работа контроллера (master) в сети с модулями ввода/вывода (slave) Основные принципы взаимодействия контроллера и устройств ввода-вывода посредством сетевых протоколов. Протоколы MODBUS RTU и MODBUS TCP, их особенности и правила использования при работе контроллера как в режиме master, так и в режиме slave. Порядок настройки параметров соединения и обмена данными между контроллером и устройствами ввода-вывода, анализируются возможные проблемы при работе в сети и способы их устранения.
	8. Работа в сети по протоколу MODBUS RTU с различными устройствами Основные аспекты протокола MODBUS RTU, включая формат кадра, адресацию, функции, а также изучение работы различных устройств (контроллеров и модулей ввода-вывода) в сети, используя этот протокол. Настройка и конфигурация устройств, анализ протокола обмена и методы диагностики проблем, возникающих в работе сети MODBUS RTU.
	9. Работа в сети по протоколу MODBUS TCP Основы протокола MODBUS TCP, включая форматы сообщений, структуру транзакций, способы обмена данными между устройствами, а также настройку и конфигурацию сети MODBUS TCP и ее устройств. Современные технологии и инструменты для мониторинга и управления сетью MODBUS TCP, такие как SCADA-системы и ПО для сетевого анализа.

	10. 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). Особенности и принципы работы каждого протокола, его преимущества и недостатки, а также способы настройки и конфигурирования сетей с использованием этих протоколов.
	11. Беспроводные локальные сети для промышленного применения Технологии беспроводной связи, используемых в промышленности, таких как Wi-Fi, Bluetooth, Zigbee, LoRa, NB-IoT и др. 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.
	12. 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.
	13. 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.
	14. 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.
	15. 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.
	16. 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.
	17. 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.
	18. 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.
	В том числе практических занятий и лабораторных работ
	Практическое занятие 1. Работа с основными сетевыми технологиями в промышленной автоматизации
	Практическое занятие 2. Разработка схемы промышленной сети и выбор средств ее реализации
	Практическое занятие 3. Практическое применение протокола MODBUS для обмена данными между устройствами
	Практическое занятие 4. Создание конфигурации сети с использованием протокола MODBUS
	Практическое занятие 5. Организация работы контроллера (slave) и операторной панели (master) по протоколу MODBUS
	Практическое занятие 6. Выравнивание адресов переменных в поле памяти протокола MODBUS
	Практическое занятие 7. Настройка работы контроллера (master) с модулями ввода/вывода (slave) по протоколу MODBUS RTU
	Практическое занятие 8. Практическая работа с различными устройствами по протоколу MODBUS RTU
	Практическое занятие 9. Работа с протоколом MODBUS TCP
	Практическое занятие 10. Работа с типовыми проводными и кабельными протоколами в промышленности
	Практическое занятие 11. Изучение беспроводных локальных сетей для промышленного применения
	Практическое занятие 12. Практическое применение специализированных сетевых интерфейсов для умного дома
	Практическое занятие 13. Работа с преобразователями интерфейсов в промышленной сети
	Практическое занятие 14. Ознакомление с современными тенденциями в развитии сетевых технологий в АСУ ТП, включая web-серверы и облачные решения
	Практическое занятие 15. Особенности применения промышленных сетевых протоколов в условиях высоких нагрузок и плохой связи
	Практическое занятие 16. Сравнительный анализ промышленных Ethernet-технологий: EtherNet/IP, PROFINET, Modbus TCP

	Практическое занятие 17. Применение промышленных маршрутизаторов для обеспечения безопасности и надежности работы сетевой инфраструктуры
	Практическое занятие 18. Практическое использование промышленных маршрутизаторов
	Практическое занятие 19. Организация удаленного доступа к сетевым устройствам в промышленной сети
	Практическое занятие 20. Разработка и тестирование собственного промышленного протокола для обмена данными между устройствами в сети
	Практическое занятие 21. Организация кластера промышленных компьютеров для выполнения высокопроизводительных вычислений в АСУ ТП
Раздел 3. Безопасность сетевой инфраструктуры 72 часа	
МДКн.03.03. Безопасность сетевой инфраструктуры	
Тема 3.1. Безопасность компьютерных сетей	**Содержание**
	1. **Фундаментальные принципы безопасной сети** Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.
	2. **Безопасность сетевых устройств OSI** Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.
	3. **Авторизация, аутентификация и учет доступа (AAA)** Свойства AAA. Локальная AAA аутентификация. Server-based AAA
	4. **Реализация технологий брандмауэра ACL.** Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах.
	5. **Реализация технологий предотвращения вторжения** IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS
	6. **Безопасность локальной сети** Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN
	7. **Криптографические системы** Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей
	8. **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 CCP. Реализация Remote-access VPN
	9. **Управление безопасной сетью** 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.
	10. **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.
	11. Межсетевая безопасность Методы обеспечения безопасности взаимодействия между различными сетями. Реализация технологий маршрутизации и шлюзов, использование межсетевых экранов, технологии виртуальных локальных сетей.
	12. 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.
	13. Защита от социальной инженерии Методы социальной инженерии, опасности, связанные с подделкой и манипулированием данными, а также методы защиты и обучения персонала.
	В том числе практических занятий и лабораторных работ
	Практическое занятие 1. Социальная инженерия
	Практическое занятие 2. Исследование сетевых атак и инструментов проверки защиты сети
	Практическое занятие 3. Настройка безопасного доступа к маршрутизатору
	Практическое занятие 4. Обеспечение административного доступа AAA и сервера Radius
	Практическое занятие 5. Настройка политики безопасности брандмауэров
	Практическое занятие 6. Настройка системы предотвращения вторжений (IPS)
	Практическое занятие 7. Настройка безопасности на втором уровне на коммутаторах
	Практическое занятие 8. Исследование методов шифрования
	Практическое занятие 9. Настройка Site-to-SiteVPN используя интерфейс командной строки
	Практическое занятие 10. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки
	Практическое занятие 11. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM
	Практическое занятие 12. Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM
	Практическое занятие 13. НастройкаClientless Remote Access SSL VPNs используя ASDM

	Практическое занятие 14. Настройка AnyConnect Remote Access SSL VPN используя ASDM
	Практическое занятие 15. Комплексная лабораторная работа по безопасности
Тема 3.2. Обеспечение сетевой безопасности	**Содержание**
	1. Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть.
	2. Механизмы шифрования и аутентификации для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам и сервисам.
	3. Использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.
	4. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети.
	5. Методы минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.
	6. Введение системы обнаружения и предотвращения сетевых вторжений.
	7. Технологии использования виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа.
	8. Использование системы управления доступом для контроля доступа к корпоративной сети.
	9. Обеспечение безопасности Wi-Fi-сетей.
	10. Реализация мер по обеспечению безопасности электронной почты в корпоративной сети.
	11. Защита от атак типа "фишинг".
	12. Применение антивирусного программного обеспечения для защиты от вирусов и других вредоносных программ.
	13. Использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.
	14. Защита от DDoS-атак.
	15. Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети.
	16. Защита от внутренних угроз безопасности.
	17. Обеспечение безопасности облачных сервисов.
	18. Организация мониторинга сетевой безопасности и аудита.
	19. Введение системы контроля целостности файлов для защиты от изменения или внедрения вредоносных программ в файловые системы.
	20. Применение методов шифрования данных для защиты от несанкционированного доступа к конфиденциальной информации.
	В том числе практических занятий и лабораторных работ
	Практическое занятие 1. Настройка VPN-туннелей для организации защищенных каналов передачи данных между территориально распределенными офисами.
	Практическое занятие 2. Работа с механизмами шифрования и аутентификации для обеспечения безопасного удаленного доступа

	к корпоративным информационным ресурсам и сервисам.
	Практическое занятие 3. Настройка и использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.
	Практическое занятие 4. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети с использованием программного обеспечения для мониторинга и обнаружения угроз.
	Практическое занятие 5. Разработка и внедрение мер по минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.
	Практическое занятие 6. Настройка и работа с системами обнаружения и предотвращения сетевых вторжений для раннего обнаружения и предотвращения угроз безопасности.
	Практическое занятие 7. Настройка и использование виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.
	Практическое занятие 8. Настройка и работа с системами управления доступом для контроля доступа к корпоративной сети.
	Практическое занятие 9. Обеспечение безопасности Wi-Fi-сетей: настройка безопасных точек доступа, использование сетевой аутентификации, шифрования трафика и других методов.
	Практическое занятие 10. 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 11. Обучение пользователям основам защиты от атак типа "фишинг".
	Практическое занятие 12. 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 13. Настройка и использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.
	Практическое занятие 14. Настройка и использование межсетевых экранов и фаерволов для обеспечения комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.
	Практическое занятие 15. Внедрение системы управления доступом для контроля доступа к корпоративной сети: настройка правил доступа, аутентификация пользователей, управление привилегиями.
	Практическое занятие 16. Использование технологий виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа: настройка и управление VPN-туннелями, защита данных, маршрутизация трафика.
	Практическое занятие 17. Обеспечение безопасности Wi-Fi-сетей: настройка и управление беспроводными точками доступа, защита сетевого трафика, аутентификация пользователей.

	Практическое занятие 18. Защита от DDoS-атак: использование специализированных средств защиты от DDoS-атак, настройка маршрутизации трафика, мониторинг сетевой активности.
	Практическое занятие 19. Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети: настройка политик безопасности для мобильных устройств, управление устройствами и приложениями, защита данных на устройствах.
	Практическое занятие 20. Обеспечение безопасности облачных сервисов: выбор надежных провайдеров облачных сервисов, настройка правил доступа и аутентификации, шифрование данных, мониторинг активности в облачных сервисах.

Курсовой проект (работа) (60 час.)

Учебная практика

Виды работ

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

Производственная практика

Виды работ

1. Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение.
2. Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях.
3. Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций.
4. Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли.
5. Установка прав доступа и контроль использования сетевых ресурсов.
6. Обеспечение своевременного копирования, архивирования и резервирования данных.
7. Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования.
8. Выявление ошибок пользователей и программного обеспечения и принятие мер по их

исправлению. Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети. 9. Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия. 10. Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций. 11. Документирование всех произведенных действий.
Промежуточная аттестация
Всего: часов

2.4. Курсовой работа (проект)

Примерная тематика курсовых проектов (работ)

1. Разработка системы автоматизации процесса производства на базе промышленного контроллера.
2. Создание системы автоматического управления технологическими процессами на основе методов искусственного интеллекта.
3. Разработка программного обеспечения для автоматизации процесса сборки изделий на промышленном производстве.
4. Исследование и внедрение технологии RFID (Radio Frequency Identification) для автоматизации учета и контроля процессов на производстве.
5. Создание системы мониторинга технологических процессов с использованием датчиков и IoT-технологий.
6. Разработка системы автоматического управления энергопотреблением на производстве для повышения эффективности и экономии затрат.
7. Исследование и внедрение технологии 3D-печати в производственный процесс с целью автоматизации и оптимизации процессов.
8. Разработка системы автоматического контроля и управления качеством продукции на производстве.
9. Исследование и анализ существующих технологий автоматизации технологических процессов с целью выбора наиболее эффективной и оптимальной.
10. Создание системы автоматизации управления складскими процессами с использованием технологий IoT и искусственного интеллекта.
11. Разработка программного обеспечения для автоматизации технологических процессов на малых предприятиях.
12. Исследование и внедрение системы автоматизации управления производственным циклом на основе принципов LEAN-производства.
13. Создание системы автоматизированного управления и контроля технологических процессов в сельском хозяйстве.
14. Разработка системы автоматизации процесса транспортировки грузов на складах и производстве с использованием робототехники.
15. Исследование и анализ существующих технологий автоматизации процессов в машиностроительной отрасли с целью выбора оптимальной для конкретного производства
16. Анализ уязвимостей сетевой инфраструктуры предприятия и разработка плана обеспечения безопасности.
17. Разработка и внедрение системы обнаружения и предотвращения сетевых вторжений.
18. Исследование и анализ методов минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.
19. Проектирование и реализация защиты от DDoS-атак в корпоративной сети.

20. Анализ эффективности использования межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.
21. Разработка системы управления доступом для контроля доступа к корпоративной сети.
22. Исследование и разработка мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети.
23. Проектирование и внедрение системы мониторинга сетевой безопасности и аудита.
24. Анализ и разработка методов использования виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа.
25. Разработка и внедрение мер по обеспечению безопасности облачных сервисов.
26. Исследование и анализ методов защиты от внутренних угроз безопасности.
27. Разработка и внедрение системы контроля целостности файлов для защиты от изменения или внедрения вредоносных программ в файловые системы.
28. Проектирование и реализация системы защиты Wi-Fi-сетей.
29. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети.
30. Разработка и внедрение механизмов шифрования и аутентификации для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам и сервисам.
31. Исследование и разработка мер по защите от атак типа "фишинг".
32. Разработка и внедрение механизмов защиты от вирусов и других вредоносных программ.
33. Анализ эффективности использования системы обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Кабинеты «Общепрофессиональных дисциплин и профессиональных модулей» оснащенные в соответствии с приложением 3 ПОП-П.

Лаборатории «Информационных технологий», «Направляющих систем». Лаборатории «Информационных технологий», «Направляющих систем» оснащенные в соответствии с приложением 3 ПОП-П.

Оснащенные базы практики, оснащенная в соответствии с приложением 3 ПОП-П.

3.2. Учебно-методическое обеспечение

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

3.2.1. Основные печатные издания

1. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры: учебник / А.В. Назаров, А.Н. Енгалычев, В.П. Мельников. — Москва: КУРС: ИНФРА-М, 2023. — 360 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-06-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/1999922.

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие/ В.Ф. Шаньгин. – М.: ИД «ФОРУМ» - ИНФРА-М, 2023. – 416 с.

3.2.2. Основные электронные издания

1. Куль, Т. П. Операционные системы. Программное обеспечение учебник для СПО / Т. П. Куль. — 3-е изд., стер. — Санкт-Петербург: Лань, 2023. — 248 с. — ISBN 978-5-507-46005 2. Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/2929943.2.2. Основные электронные издания

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код ПК, ОК	Критерии оценки результата (показатели освоенности компетенций)	Формы контроля и методы оценки[3]
ПК 3.1	Определение профессиональной задачи и этапов ее выполнения Эффективный поиск информации для решения профессиональной задачи Определение ресурсов для решения профессиональной задачи Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «хорошо» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Защита отчетов по практическим и лабораторным работам Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ПК 3.2.		
ПК 3.3.		
ПК 3.4.		
ПК 3.5.		
ПК 3.6.		
ОК 01.	Подбор вариантов решения конкретной профессиональной задачи или проблемы	Оценка полноты перечня подобранных вариантов
ОК 02.	Демонстрация навыков использования информационных порталов в сети Интернет, включая официальные информационно-правовые порталы	Оценка полноты перечня подобранных вариантов
ОК 03.	Демонстрация интереса к выбранной специальности, к инновационным технологиям в области профессиональной деятельности	Участие в мероприятиях (олимпиады, конкурсы профессионального мастерства, стажировки и др.), проводимых как образовательным заведением, так и ведущими предприятиями отрасли

[3] Примеры оформления формы контроля: контрольные работы, зачеты, квалификационные испытания, защита курсовых и дипломных проектов (работ), экзамены. Примеры оформления методов оценки: интерпретация результатов выполнения практических и лабораторных заданий, оценка решения ситуационных задач, оценка тестового контроля.

ОК 04.	Демонстрировать навыки межличностного общения с соблюдением общепринятых правил со сверстниками в образовательной группе, с преподавателями во время обучения, с руководителями производственной практики	Экспертное наблюдение поведенческих навыков в ходе обучения
ОК 05.	Демонстрация навыков грамотной устной и письменной речи	Экспертное наблюдение навыков устного и письменного общения в ходе обучения
ОК 06.	Формирование чувства патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку, человеку труда и старшему поколению; взаимного уважения, бережного отношения к культурному наследию и традициям многонационального народа Российской Федерации; нетерпимости к коррупционным проявлениям	Участие в мероприятиях патриотической направленности, в проведении военно-спортивных игр; участие в программах антикоррупционной направленности
ОК 07.	Формирование бережного отношения к природе и окружающей среде	Экспертное наблюдение демонстрации навыков соблюдения правил экологической безопасности в ведении профессиональной деятельности; формирование навыков эффективных действий в чрезвычайных ситуациях
ОК 08.	Формирование бережного отношения к здоровью	Участие в спортивных мероприятиях, проводимых образовательным учреждением; ведение здорового образа жизни