**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)**

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

УТВЕРЖДАЮ
Первый проректор – проректор по учебной работе
_____ А.В. Абилов
_____ 2025 г.

Регистрационный № 11.04.25/36

СПбГУТ))) Документ подписан простой электронной подписью

Сертификат: 009b47d8b89b08d0f6
Владелец: Киричек Руслан Валентинович
Действителен с 13.02.2023 по 12.02.2028

РАБОЧАЯ ПРОГРАММА

ПМ.03. ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

(наименование профессионального модуля)

по специальности

09.02.06 Сетевое и системное администрирование
(код и наименование специальности)

квалификация
системный администратор

Санкт-Петербург
2025

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена (индекс – ПМ.03) по специальности 09.02.06 Сетевое и системное администрирование, утверждённым ректором ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 28 марта 2025 г., протокол № 3.

Составитель:
Преподаватель _____ О.М. Алексеева
(подпись)

СОГЛАСОВАНО
Главный специалист НТБ УИОР _____ Р.Х. Ахтреева
(подпись)

ОБСУЖДЕНО
на заседании предметной (цикловой) комиссии № 4 (компьютерных сетей и программно-аппаратных средств)
12 февраля 2025 г., протокол №6

Председатель предметной (цикловой) комиссии: _____ О.М. Алексеева
(подпись)

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля
19 февраля 2025 г., протокол №4

Заместитель директора по учебной работе колледжа СПб ГУТ
_____ Н.В. Калинина
(подпись)

СОГЛАСОВАНО

Директор колледжа СПб ГУТ
_____ Т.Н. Сиротская
(подпись)

СОГЛАСОВАНО

Директор департамента ОКОД
_____ С.И. Ивасишин
(подпись)

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ. 03. ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

1.1 Область применения рабочей программы

Рабочая программа профессионального модуля – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 09.02.06 Сетевое и системное администрирование.

1.2 Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности «Эксплуатация объектов сетевой инфраструктуры» и соответствующие ему общие компетенции и профессиональные компетенции:

1.2.1 Перечень общих компетенций и личностных результатов реализации программы воспитания

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
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках
ЛР1–ЛР4, ЛР9, ЛР10, ЛР13-ЛР15, ЛР20, ЛР23–ЛР28	

1.1.2 Перечень профессиональных компетенций

Код	Наименование 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 исправление нетипичных неисправностей в работе сетевой инфраструктуры

ПК 3.5	Модернизировать сетевые устройства информационно-коммуникационных систем

1.1.3. В результате освоения профессионального модуля студент должен:

владеть навыками	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; 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; обеспечивать целостность резервирования информации; обеспечивать безопасное хранение и передачу информации в глобальных и локальных сетях; фильтровать, контролировать и обеспечивать безопасность сетевого трафика; мониторинг производительности сервера и протоколирования системных и сетевых событий; создавать подсети и настраивать обмен данными; анализировать схемы потоков трафика в компьютерной сети; оценивать качество и соответствие требованиям проекта сети; оформлять техническую документацию.
уметь	– 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; – использовать многофункциональные приборы и программные средства мониторинга; – использовать программно-аппаратные средства технического контроля; – читать техническую и проектную 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.
знать	общие принципы построения сете; 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 устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование; средства тестирования и анализа; базовые протоколы и технологии локальных сетей; архитектуру сканера безопасности; принципы построения высокоскоростных локальных сетей; требования к сетевой безопасности; организацию работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей; программно-аппаратные средства технического контроля; принципы и стандарты оформления технической документации; принципы создания и оформления топологии сети; информационно-справочные системы для замены (поиска) технического оборудования.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов: **836 часов.**

Из них на освоение МДК:

МДК.03.01. Эксплуатация объектов сетевой инфраструктуры - **100 часов;**

МДК.03.02. Технологии автоматизации технологических процессов - **200 часов;**

МДК.03.03. Безопасность сетевой инфраструктуры - **212 часов.**

на практики учебную и производственную - **288 часов.**

2. СТРУКТУРА и содержание профессионального модуля

2.1. Структура профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	В т.ч. в форме практической подготовки	**Объем профессионального модуля, час.**						
				Работа обучающихся во взаимодействии с преподавателем						
				Обучение по МДК, в час.			Практики		Самостоятельная работа, часов	Промежуточная аттестация, часов
				Всего, часов	Лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Учебная, часов	Производственная		
ПК 3.1- ПК 3.5 ОК 01 – ОК 09	Раздел 1. Эксплуатация сетевой инфраструктуры	**100**	34	**78**	34	-			**20**	**2**
ПК 3.1- ПК 3.5 ОК 01 – ОК 09	Раздел 2. Технологии автоматизации технологических процессов	**200**	68	**158**	68	30			**40**	**2**
ПК 3.1- ПК 3.5 ОК 01 – ОК 09	Раздел 3. Безопасность сетевой инфраструктуры	**212**	68	**158**	68	30			**52**	**2**
Учебная практика		**144**	144							
Производственная практика		**144**	144							
Промежуточная аттестация		**36**								36
Всего:		**836**	458	**394**	170	60	**144**	**144**	**112**	**42**

2.2 Тематический план и содержание профессионального модуля

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем часов
Раздел 1. Эксплуатация объектов сетевой инфраструктуры.			
МДК.03.01. Эксплуатация объектов сетевой инфраструктуры.			100
Тема 1.1. Эксплуатация объектов сетевой инфраструктуры.	**Содержание учебного материала**		24
	1	**Занятие 1.** Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети.	
	2	**Занятие 2.** Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.	
	3	**Занятие 3.** Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб).	
	4	**Занятие 4.** Наращивание длины сегментов сети. Замена существующей аппаратуры.	
	5	**Занятие 5.** Увеличение количества узлов сети; увеличение протяженности связей между объектами сети	
	6	**Занятие 6.** Физическая карта всей сети. Логическая топология компьютерной сети. Техническая и проектная документация. Паспорт технических устройств.	
	7	**Занятие 7.** Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры. Проверка объектов сетевой инфраструктуры и профилактические работы.	
	8	**Занятие 8.** Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.	
	9	**Занятие 9.** 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.	

	10	**Занятие 10.** Аализ возможностей современного программного обеспечения мониторинга и определение эффективных подходов к использованию этих возможностей в практических задачах мониторинга компьютерных сетей и сетевых устройств.	
	11	**Занятие 11.** Протокол SNMP, его характеристики, формат сообщений, набор услуг. Анализ основных характеристик протокола SNMP, его структуры и архитектуры, формата сообщений и спецификации синтаксиса.	
	12	**Занятие 12.** Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.	
	Лабораторные работы		
	1	**Занятие 13.** Оконцовка кабеля витая пара.	
	2	**Занятие 14.** Заделка кабеля витая пара в розетку.	
	3	**Занятие 15.** Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену.	
	4	**Занятие 16.** Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы).	
	5	**Занятие 17.** Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.	20
	6	**Занятие 18.** Оформление технической документации, правила оформления документов	
	7	**Занятие 19.** Протокол управления SNMP.	
	8	**Занятие 20.** Задачи управления: анализ производительности сети, анализ надежности сети.	
	9	**Занятие 21**. Учет трафика в сети.	
	10	**Занятие 22.** Средства анализа сети с помощью команд сетевой операционной системы.	
Тема 1.2. Эксплуатация систем IP-телефонии.	**Содержание учебного материала**		
	1	**Занятие 23.** Настройка H.323. Описание H.323 и общие рекомендации. Функциональные компоненты H.323.Установка и поддержка соединения H.323.	
	2	**Занятие 24.** Соединения без и с использованием GateKeeper. Соединения с использованием нескольких GateKeeper. Многопользовательские конференции. Обеспечение отказоустойчивости.	20
	3	**Занятие 25.** Настройка SIP. Описание и общие рекомендации.	
	4	**Занятие 26.** Технология SIP и связанные с ней стандарты. Функциональные компоненты SIP.	
	5	**Занятие 27.** Сообщения SIP. Адресация SIP. Модель установления соединения. Планирование отказоустойчивости.	
	6	**Занятие 28.** Установка и инсталляция программного коммутатора. Монтажные процедуры.	

		Процедуры инсталляции. Управление аппаратными средствами и портами. Протоколы управления MGCP, H.248. Создание аналоговых абонентов. Внутристанционная маршрутизация.	
	7	**Занятие 29.** Управление программным коммутатором. Маршрутизация. Группы соединительных линий. Подключение станций с TDM (абонентский доступ TDM).	
	8	**Занятие 30.** Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP -абоненты. Группы абонентов. Дополнительные абонентские услуги.	
	9	**Занятие 31.** Организация эксплуатации систем IP-телефонии. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт.	
	10	**Занятие 32.** Восстановление работы сети после аварии. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных.	
	Лабораторные работы		
	11	**Занятие 33.** Настройка аппаратных и программных IP-телефонов, факсов.	14
	12	**Занятие 34.** Развертывание сети с использованием VLAN для IP-телефонии.	
	13	**Занятие 35.** Настройка шлюза для IP-телефонии.	
	14	**Занятие 36.** Установка и настройка программной IP-АТС.	
	15	**Занятие 37.** Мониторинг вызовов в программном коммутаторе.	
	16	**Занятие 38.** Создание резервных копий баз данных в программном коммутаторе.	
	17	**Занятие 39.** Диагностика и устранение неисправностей в системах IP-телефонии.	
	Самостоятельная работа обучающихся		
	Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Конспектирование текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа. Проектные формы работы, подготовка сообщений к выступлению на семинарах и конференциях; подготовка рефератов, докладов. Тематика домашних заданий, сообщений, рефератов: 1. Основные этапы эксплуатации сетевой инфраструктуры. 2. Технологии мониторинга и управления сетевыми ресурсами. 3. Анализ безопасности сетевой инфраструктуры и методы защиты от угроз. 4. Разработка стратегии резервного копирования данных сетевой инфраструктуры. 5. Оценка производительности и оптимизация работы сетевых устройств. 6. Разработка плана восстановления после катастрофы для сетевой инфраструктуры.		20

	7. Исследование взаимодействия сетевой инфраструктуры с системами управления и хранения данных. 8. Использование технологий виртуализации для оптимизации сетевой инфраструктуры. 9. Оценка возможностей и проблем облачных технологий в сетевой инфраструктуре. 10. Исследование применения SDN (Software-Defined Networking) в сетевой инфраструктуре. 11. Интеграция и управление сетевыми устройствами различных производителей. 12. Развитие сетевой инфраструктуры в контексте IoT (Internet of Things). 13. Оценка и управление рисками, связанными с эксплуатацией сетевой инфраструктуры. 14. Анализ влияния обновлений и изменений на работу сетевой инфраструктуры. 15. Исследование проблем масштабирования и расширения сетевой инфраструктуры.	
Промежуточная аттестация в форме дифференцированного зачета			**2**
Раздел 2. Технологии автоматизации технологических процессов.			
МДК.03.02. Технологии автоматизации технологических процессов.			**200**
Тема 2.1. Автоматизированные системы управления технологическими процессами (АСУ ТП).	**Содержание учебного материала**		30
	1	**Занятие 1.** Понятие об объекте управления. Свойства объекта управления.	
	2	**Занятие 2.** Классификация технологических объектов управления по типу, характеру технологического процесса, по характеристике параметров управления.	
	3	**Занятие 3.** Классификация систем управления технологическими объектами по способу, цели и степени централизации управления.	
	4	**Занятие 4.** Общие сведения об автоматизированных системах управления технологическими процессами (АСУТП) и системах автоматического управления (САУ).	
	5	**Занятие 5.** Основные функции АСУТП и САУ. Техническое, программное и информационное обеспечение АСУТП.	
	6	**Занятие 6.** Структура АСУТП на базе микропроцессорной техники.	
	7	**Занятие 7.** Средства измерения преобразования и регулирования в АСУТП.	
	8	**Занятие 8.** Основные понятия автоматизированной обработки информации.	
	9	**Занятие 9.** Методы и средства моделирования технологических процессов в АСУТП.	
	10	**Занятие 10.** Обзор современных технологий и тенденций развития АСУТП.	
	11	**Занятие 11.** Программирование и настройка АСУТП: языки программирования, методы и инструменты.	
	12	**Занятие 12.** Интеграция АСУТП с другими системами и оборудованием в производственном	

		процессе.	
	13	**Занятие 13.** Оценка эффективности и экономическая оценка внедрения АСУТП.	
	14	**Занятие 14.** Особенности управления производственными системами в условиях неопределенности и переменных условий работы.	
	15	**Занятие 15.** Применение систем искусственного интеллекта в АСУТП: нейронные сети, генетические алгоритмы, экспертные системы.	
	Лабораторные работы		
	1	**Занятие 16.** Определение свойств объектов управления на практике.	
	2	**Занятие 17.** Классификация технологических объектов управления на примере производственного предприятия.	
	3	**Занятие 18.** Анализ и сравнение систем управления технологическими объектами на примере различных отраслей промышленности.	
	4	**Занятие 19.** Изучение принципов работы АСУТП и САУ на примере реальных систем управления.	
	5	**Занятие 20.** Создание простой модели технологического процесса.	
	6	**Занятие 21.** Ознакомление с современными технологиями АСУТП на примере существующих проектов и исследований.	
	7	**Занятие 22.** Программирование элементов АСУТП на языках программирования на практике.	
	8	**Занятие 23.** Настройка и проверка работоспособности элементов АСУТП на примере конкретной системы управления.	28
	9	**Занятие 24.** Интеграция АСУТП с другими системами и оборудованием в производственном процессе.	
	10	**Занятие 25.** Оценка эффективности и экономическая оценка внедрения АСУТП.	
	11	**Занятие 26.** Разработка системы управления производственными процессами в условиях неопределенности и переменных условий работы.	
	12	**Занятие 27.** Применение нейронных сетей в системах управления технологическими процессами.	
	13	**Занятие 28.** Применение экспертных систем в системах управления технологическими процессами.	
	14	**Занятие 29.** Создание проекта автоматизации управления технологическим процессом на основе АСУТП.	

сетевые технологии и протоколы в АСУ ТП.	**Содержание учебного материала**		30
	1	**Занятие 30.** 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	**Занятие 31.** 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	**Занятие 32.** Протокол MODBUS. 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, типы данных, поддерживаемые протоколом. Организация работы в протоколе MODBUS контроллера (slave) и операторной панели (master).	
	4	**Занятие 33.** 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.	
	5	**Занятие 34.** 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.	
	6	**Занятие 35.** 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.	
	7	**Занятие 36.** 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.	
	8	**Занятие 37.** 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.	
	9	**Занятие 38.** 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.	
	10	**Занятие 39.** 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.	
	11	**Занятие 40.** 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.	
	12	**Занятие 41.** 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.	
	13	**Занятие 42.** 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.	
	14	**Занятие 43.** 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.	
	15	**Занятие 44.** 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.	
	Лабораторные работы		40
	15	**Занятие 45.** Разработка схемы промышленной сети и выбор средств ее реализации.	
	16	**Занятие 46.** Практическое применение протокола MODBUS для обмена данными между устройствами.	
	17	**Занятие 47.** Создание конфигурации сети с использованием протокола MODBUS.	
	18	**Занятие 48.** Организация работы контроллера (slave) и операторной панели (master) по протоколу MODBUS.	
	19	**Занятие 49.** Выравнивание адресов переменных в поле памяти протокола MODBUS.	
	20	**Занятие 50.** Настройка работы контроллера (master) с модулями ввода/вывода (slave) по протоколу MODBUS RTU.	
	21	**Занятие 51.** Практическая работа с различными устройствами по протоколу MODBUS RTU.	
	22	**Занятие 52.** Работа с протоколом MODBUS TCP.	
	23	**Занятие 53.** Работа с типовыми проводными и кабельными протоколами в промышленности.	
	24	**Занятие 54.** Изучение беспроводных локальных сетей для промышленного применения.	
	25	**Занятие 55.** Практическое применение специализированных сетевых интерфейсов для умного дома.	
	26	**Занятие 56.** Работа с преобразователями интерфейсов в промышленной сети.	
	27	**Занятие 57.** Ознакомление с современными тенденциями в развитии сетевых технологий в АСУ ТП, включая web-серверы и облачные решения.	

	28	**Занятие 58.** Особенности применения промышленных сетевых протоколов в условиях высоких нагрузок и плохой связи.	
	29	**Занятие 59.** Сравнительный анализ промышленных Ethernet-технологий: EtherNet/IP, PROFINET, Modbus TCP.	
	30	**Занятие 60.** Применение промышленных маршрутизаторов для обеспечения безопасности и надежности работы сетевой инфраструктуры.	
	31	**Занятие 61.** Практическое использование промышленных маршрутизаторов.	
	32	**Занятие 62.** Организация удаленного доступа к сетевым устройствам в промышленной сети.	
	33	**Занятие 63.** Разработка и тестирование собственного промышленного протокола для обмена данными между устройствами в сети.	
	34	**Занятие 64.** Организация кластера промышленных компьютеров для выполнения высокопроизводительных вычислений в АСУ ТП.	
	Самостоятельная работа обучающихся		
	Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Конспектирование текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа. Проектные формы работы, подготовка сообщений к выступлению на семинарах и конференциях; подготовка рефератов, докладов. Тематика домашних заданий, сообщений, рефератов: 1. Анализ промышленного объекта и выявление потребностей в автоматизации технологических процессов. 2. Разработка структурной схемы автоматизации технологического процесса на основе выбранных промышленных контроллеров и устройств. 3. Выбор и настройка датчиков и измерительных приборов для мониторинга технологических параметров. 4. Разработка программного обеспечения для автоматизации технологического процесса с использованием языков программирования, таких как Ladder, Function Block Diagram (FBD), Structured Text (ST) и т.д. 5. Разработка алгоритмов управления технологическим процессом с использованием логических операций и математических выражений. 6. Настройка промышленных сетевых устройств для обмена данными между промышленным контроллером и устройствами на производстве. 7. Оценка эффективности автоматизации технологического процесса на основе анализа		40

<table>
<tr><td></td><td colspan="2">полученных данных.
8. Разработка технического задания на автоматизацию технологических процессов для конкретного производственного объекта.
9. Определение требований к оборудованию и инструментарию для автоматизации технологического процесса.
10. Проведение инженерных изысканий и разработка технического проекта на автоматизацию технологических процессов.
11. Оценка стоимости оборудования и программного обеспечения для автоматизации технологического процесса.
12. Анализ рисков и принятие мер по обеспечению безопасности процесса автоматизации технологических процессов.
13. Изучение промышленных стандартов и нормативных документов, регулирующих автоматизацию технологических процессов.
14. Разработка методики технического обслуживания и ремонта оборудования, используемого при автоматизации технологического процесса.
15. Изучение примеров успешной реализации проектов по автоматизации технологических процессов в различных отраслях промышленности.</td><td></td></tr>
<tr><td rowspan="14">Курсовой проект (работа)</td><td colspan="2">Обязательные аудиторные учебные занятия по курсовому проекту</td><td rowspan="14">30</td></tr>
<tr><td>1</td><td>Введение. Знакомство с техническим заданием.</td></tr>
<tr><td>2</td><td>Анализ поставленной задачи.</td></tr>
<tr><td>3</td><td>Подбор теоретической информации</td></tr>
<tr><td>4</td><td>Характеристика предметной области</td></tr>
<tr><td>5</td><td>Практика применения</td></tr>
<tr><td>6</td><td>Расчет параметров объекта</td></tr>
<tr><td>7</td><td>Рассмотрение аналогов объекта</td></tr>
<tr><td>8</td><td>Сводный анализ объектов</td></tr>
<tr><td>9</td><td>Формулирование выводов по задачам</td></tr>
<tr><td>10</td><td>Обобщение работы</td></tr>
<tr><td>11</td><td>Составление заключение</td></tr>
<tr><td>12</td><td>Оформления пояснительной части</td></tr>
<tr><td>13</td><td>Оформление презентации</td></tr>
</table>

	14	Подготовка текста к защите работы	
	15	Защита работы	
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.		

Промежуточная аттестация в форме дифференцированного зачета			**2**
Раздел 3. Безопасность сетевой инфраструктуры.			
МДК.03.03. Безопасность сетевой инфраструктуры.			**212**
Тема 3.1. Безопасность компьютерных сетей.	**Содержание учебного материала**		20
	1	**Занятие 1.** Фундаментальные принципы безопасной сети. Безопасность сетевых устройств OSI. Авторизация, аутентификация и учет доступа (AAA).	
	2	**Занятие 2.** Реализация технологий брандмауэра ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах.	
	3	**Занятие 3.** Реализация технологий предотвращения вторжения. IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS.	
	4	**Занятие 4.** Безопасность локальной сети. Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN.	
	5	**Занятие 5.** Криптографические системы. Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей.	
	6	**Занятие 6.** 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.	
	7	**Занятие 7.** 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.	
	8	**Занятие 8.** 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.	
	9	**Занятие 9.** Межсетевая безопасность. Методы обеспечения безопасности взаимодействия между различными сетями. Реализация технологий маршрутизации и шлюзов, использование межсетевых экранов, технологии виртуальных локальных сетей.	
	10	**Занятие 10.** 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. Защита от социальной инженерии.	
	Лабораторные работы		28
	1	**Занятие 11.** Социальная инженерия.	
	2	**Занятие 12.** Исследование сетевых атак и инструментов проверки защиты сети.	
	3	**Занятие 13.** Настройка безопасного доступа к маршрутизатору.	
	4	**Занятие 14.** Обеспечение административного доступа AAA и сервера Radius.	
	5	**Занятие 15.** Настройка политики безопасности брандмауэров.	
	6	**Занятие 16.** Настройка системы предотвращения вторжений (IPS).	
	7	**Занятие 17.** Настройка безопасности на втором уровне на коммутаторах.	
	8	**Занятие 18.** Исследование методов шифрования.	
	9	**Занятие 19.** Настройка Site-to-SiteVPN используя интерфейс командной строки.	
	10	**Занятие 20.** Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки.	
	11	**Занятие 21.** Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM.	
	12	**Занятие 22.** Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM.	
	13	**Занятие 23.** Настройка Clientless Remote Access SSL VPNs используя ASDM.	
	14	**Занятие 24.** Настройка AnyConnect Remote Access SSL VPN используя ASDM.	
Тема 3.2. Обеспечение сетевой безопасности.	**Содержание учебного материала**		40
	1	**Занятие 25.** Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть.	
	2	**Занятие 26.** Механизмы шифрования и аутентификации для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам и сервисам.	
	3	**Занятие 27.** Использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.	
	4	**Занятие 28.** Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети.	
	5	**Занятие 29.** Методы минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.	

	6	**Занятие 30.** Введение системы обнаружения и предотвращения сетевых вторжений.	
	7	**Занятие 31.** Технологии использования виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа.	
	8	**Занятие 32.** Использование системы управления доступом для контроля доступа к корпоративной сети.	
	9	**Занятие 33.** Обеспечение безопасности Wi-Fi-сетей.	
	10	**Занятие 34.** Реализация мер по обеспечению безопасности электронной почты в корпоративной сети.	
	11	**Занятие 35.** Защита от атак типа «фишинг».	
	12	**Занятие 36.** Применение антивирусного программного обеспечения для защиты от вирусов и других вредоносных программ.	
	13	**Занятие 37.** Использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.	
	14	**Занятие 38.** Защита от DDoS-атак.	
	15	**Занятие 39.** Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети.	
	16	**Занятие 40.** Защита от внутренних угроз безопасности.	
	17	**Занятие 41.** Обеспечение безопасности облачных сервисов.	
	18	**Занятие 42.** Организация мониторинга сетевой безопасности и аудита.	
	19	**Занятие 43.** Введение системы контроля целостности файлов для защиты от изменения или внедрения вредоносных программ в файловые системы.	
	20	**Занятие 44.** Применение методов шифрования данных для защиты от несанкционированного доступа к конфиденциальной информации.	
	Лабораторные работы		40
	15	**Занятие 45.** Настройка VPN-туннелей для организации защищенных каналов передачи данных между территориально распределенными офисами.	
	16	**Занятие 46.** Работа с механизмами шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.	
	17	**Занятие 47.** Настройка и использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.	
	18	**Занятие 48.** Анализ содержимого трафика и контроль приложений и пользователей в системах	

		безопасности сети с использованием программного обеспечения для мониторинга и обнаружения угроз.	
	19	**Занятие 49.** Разработка и внедрение мер по минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.	
	20	**Занятие 50.** Настройка и работа с системами обнаружения и предотвращения сетевых вторжений для раннего обнаружения и предотвращения угроз безопасности.	
	21	**Занятие 51.** Настройка и использование виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.	
	22	**Занятие 52.** Настройка и работа с системами управления доступом для контроля доступа к корпоративной сети.	
	23	**Занятие 53.** Обеспечение безопасности Wi-Fi-сетей: настройка безопасных точек доступа, использование сетевой аутентификации, шифрования трафика и других методов.	
	24	**Занятие 54.** 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.	
	25	**Занятие 55.** Обучение пользователям основам защиты от атак типа «фишинг».	
	26	**Занятие 56.** Работа с антивирусным программным обеспечением для защиты от вирусов и других вредоносных программ: установка, настройка, обновление базы данных, сканирование и удаление вредоносных программ.	
	27	**Занятие 57.** Настройка и использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.	
	28	**Занятие 58.** Настройка и использование межсетевых экранов и фаерволов для обеспечения комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.	
	29	**Занятие 59.** Внедрение системы управления доступом для контроля доступа к корпоративной сети: настройка правил доступа, аутентификация пользователей, управление привилегиями.	
	30	**Занятие 60.** Использование технологий виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа: настройка и управление VPN-туннелями, защита данных, маршрутизация трафика.	
	31	**Занятие 61.** Обеспечение безопасности Wi-Fi-сетей: настройка и управление беспроводными точками доступа, защита сетевого трафика, аутентификация пользователей.	
	32	**Занятие 62.** Защита от DDoS-атак: использование специализированных средств защиты от	

		DDoS-атак, настройка маршрутизации трафика, мониторинг сетевой активности.	
	33	**Занятие 63.** 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.	
	34	**Занятие 64.** Обеспечение безопасности облачных сервисов: выбор надежных провайдеров облачных сервисов, настройка правил доступа и аутентификации, шифрование данных, мониторинг активности в облачных сервисах.	
	Самостоятельная работа обучающихся		
	Систематическая проработка конспектов занятий, учебной и специальной технической литературы. Конспектирование текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа. Проектные формы работы, подготовка сообщений к выступлению на семинарах и конференциях; подготовка рефератов, докладов. Тематика домашних заданий, сообщений, рефератов: 1. Сравнение и анализ различных типов защитных механизмов для сетевой инфраструктуры. 2. Разработка плана мер по минимизации рисков внедрения вредоносного ПО в корпоративную сеть через ограничение опасных коммуникаций в публичных сетях. 3. Исследование принципов работы и настройка системы управления доступом для контроля доступа к корпоративной сети. 4. Анализ принципов работы и настройка системы обнаружения и предотвращения сетевых вторжений. 5. Исследование принципов работы и настройка системы контроля целостности файлов для защиты от изменения или внедрения вредоносных программ в файловые системы. 6. Исследование принципов работы и настройка системы мониторинга сетевой безопасности и аудита. 7. Анализ основных типов DDoS-атак и разработка мер по защите от них. 8. Исследование принципов работы и настройка защиты от внутренних угроз безопасности. 9. Исследование принципов работы и настройка обеспечения безопасности Wi-Fi-сетей. 10. Исследование принципов работы и настройка системы обнаружения и предотвращения атак типа «фишинг». 11. Исследование принципов работы и настройка защиты от вредоносных программ на мобильных устройствах, используемых в корпоративной сети. 12. Анализ принципов работы и настройка системы обеспечения безопасности облачных сервисов.		52

<table>
<tr><td></td><td colspan="2">13. Исследование принципов работы и настройка систем шифрования данных для защиты от несанкционированного доступа к конфиденциальной информации.
14. Разработка и проведение сценариев тестирования безопасности сетевой инфраструктуры.
15. Анализ случаев нарушения безопасности сетевой инфраструктуры и разработка мер по их предотвращению.
16. Составление отчета о мерах по обеспечению безопасности сетевой инфраструктуры и рекомендации по улучшению.
17. Сравнение и анализ преимуществ и недостатков различных методов защиты от внешних угроз безопасности.</td><td></td></tr>
<tr><td rowspan="16">Курсовой проект (работа)</td><td colspan="2">Обязательные аудиторные учебные занятия по курсовому проекту</td><td rowspan="16">30</td></tr>
<tr><td>1</td><td>Введение. Знакомство с техническим заданием.</td></tr>
<tr><td>2</td><td>Анализ поставленной задачи.</td></tr>
<tr><td>3</td><td>Подбор теоретической информации</td></tr>
<tr><td>4</td><td>Характеристика предметной области</td></tr>
<tr><td>5</td><td>Практика применения</td></tr>
<tr><td>6</td><td>Расчет параметров объекта</td></tr>
<tr><td>7</td><td>Рассмотрение аналогов объекта</td></tr>
<tr><td>8</td><td>Сводный анализ объектов</td></tr>
<tr><td>9</td><td>Формулирование выводов по задачам</td></tr>
<tr><td>10</td><td>Обобщение работы</td></tr>
<tr><td>11</td><td>Составление заключение</td></tr>
<tr><td>12</td><td>Оформления пояснительной части</td></tr>
<tr><td>13</td><td>Оформление презентации</td></tr>
<tr><td>14</td><td>Подготовка текста к защите работы</td></tr>
<tr><td>15</td><td>Защита работы</td></tr>
<tr><td>Тематика курсовых проектов (работ)</td><td colspan="2">1. Анализ уязвимостей сетевой инфраструктуры предприятия и разработка плана обеспечения безопасности.
2. Разработка и внедрение системы обнаружения и предотвращения сетевых вторжений.
3. Исследование и анализ методов минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.
4. Проектирование и реализация защиты от DDoS-атак в корпоративной сети.</td><td></td></tr>
</table>

	5. Анализ эффективности использования межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет. 6. Разработка системы управления доступом для контроля доступа к корпоративной сети. 7. Исследование и разработка мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети. 8. Проектирование и внедрение системы мониторинга сетевой безопасности и аудита. 9. Анализ и разработка методов использования виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа. 10. Разработка и внедрение мер по обеспечению безопасности облачных сервисов. 11. Исследование и анализ методов защиты от внутренних угроз безопасности. 12. Разработка и внедрение системы контроля целостности файлов для защиты от изменения или внедрения вредоносных программ в файловые системы. 13. Проектирование и реализация системы защиты Wi-Fi-сетей. 14. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети. 15. Разработка и внедрение механизмов шифрования и аутентификации для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам и сервисам. 16. Исследование и разработка мер по защите от атак типа «фишинг». 17. Разработка и внедрение механизмов защиты от вирусов и других вредоносных программ. 18. Анализ эффективности использования системы обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.	
Промежуточная аттестация в форме дифференцированного зачета			**2**
Учебная практика (Технологии автоматизации технологических процессов)	**Виды работ**		
	1	Настройка прав доступа.	72
	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.	
Учебная практика (Безопасность сетевой инфраструктуры)	**Виды работ**		72
	1	Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети.	
	2	Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть.	
	3	Обеспечение безопасности Wi-Fi-сетей.	
	4	Реализация мер по обеспечению безопасности электронной почты в корпоративной сети.	
	5	Защита от атак типа «фишинг».	
	6	Обеспечение сетевой безопасности.	
Производственная практика (Технологии автоматизации технологических процессов)	**Виды работ**		72
	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.	
	9	Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети.	
Производственная практика (Безопасность сетевой инфраструктуры)	**Виды работ**		72
	1	Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия.	
	2	Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций.	

	3	Документирование всех произведенных действий.	
Самостоятельная работа при подготовке к экзамену по профессиональному модулю			**26**
Консультации			**2**
Промежуточная аттестация в форме экзамена по профессиональному модулю			**8**
Всего по ПМ			**836**

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Для реализации программы предусмотрены следующие специальные помещения

Лаборатория «Направляющих систем», оснащенная оборудованием: рабочее место преподавателя – ПК 1 шт., рабочие места обучающихся (25), проектор мультимедийный, экран, доска школьная, электрические кабели связи разных марок, комплекты инструмента для разделки электрических кабелей связи, материалы и инструмент компании 3М, кабели связи разных марок, набор инструментов НИМ-25, муфты оптические, катушки нормализующие, кабельный фен, автоматический сварочный аппарат оптического волокна, источник лазерный, измеритель на меди, учебно-методические и демонстрационные пособия в электронном/печатном виде.

Лаборатория «Информационных технологий», оснащенная оборудованием: рабочее место преподавателя – ноутбук 1 шт., рабочие места обучающихся - ноутбуки 25 шт., проектор, колонки, экран, доска маркерная, локальная сеть с выходом в Интернет, стенды систем технической безопасности объектов безопасности Перко, стойка с видеорегистратором, учебно-методические и демонстрационные пособия в электронном/печатном виде.

Мастерская «Монтажа и настройки объектов сетевой инфраструктуры», оснащенная оборудованием: рабочее место преподавателя – ПК 3 шт., рабочие места обучающихся (80), ПК - 29 шт., мультимедийный проектор, экран, учебная доска, локальная сеть с выходом в Интернет, гипервизор учебной сети, наборы инструмента для монтажа, настройки и диагностики сети, расходные материалы, серверная стойка, коммутаторы, маршрутизаторы, беспроводные маршрутизаторы, программно-аппаратный шлюз безопасности, IP телефоны, учебно-методические и демонстрационные пособия в электронном/печатном виде.

Мастерская «Ремонта и обслуживания устройств инфокоммуникационных систем», оснащенная оборудованием: рабочее место преподавателя – ноутбук 1 шт., рабочие места обучающихся - ноутбуки 13 шт., мобильное демонстрационное оборудование (ноутбук, мультимедиапроектор), доска школьная, стенды Связьстройдеталь, стенды для монтажа абонентского оптического доступа; участок распределительной сети GPON, стенд оптического доступа GPON на 3 абонента, макет «Изучение передатчиков и приёмников DTMFсигналов», макет «Изучения электронных телефонных аппаратов»; системные телефонные аппараты, кросс высокой плотности, стойки телекоммуникационные, шкаф, сервер Asterisk, сервер Middleware Stalker, кросс ШКОС-Л, кросс ШКОН-КПВ, кросс ШКОН-П, кросс ШКОН-ПА, коммутатор 2-го уровня D-Link DES, коммутатор 3-го уровня D-Link DGS, IP-телефоны, шлюзы D-Link, оптический тестер, оптический источник излучения, оптический сетевой терминал ONT HUAWEI, приставка телевизионная, набор монтажного инструмента для медного кабеля, терминал LLX, NEC УПАТС NEAX, ALCATEL-4100, радиотелефоны стандарта DECT различной модификации, антенные системы, эмуляторы сетевого оборудования, учебно-методические и демонстрационные пособия в электронном/печатном виде.

МДК 03.01 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

3.2 Информационное обеспечение реализации программы

3.2.1. Основные электронные издания:

1. Демидов Л.Н. Основы эксплуатации компьютерных сетей: учебник / Л.Н. Демидов. - Москва: Прометей, 2019. - 798 с. - ISBN 978-5-907100-01-5. - URL: https://ibooks.ru/bookshelf/365802/reading (дата обращения: 22.01.2024).

2. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры: учебник для среднего профессионального образования / А.В. Назаров, А.Н. Енгалычев, В.П. Мельников. — Москва: КУРС: ИНФРА-М, 2023. — 360 с. — ISBN 978-5-906923-06-6. - URL: https://znanium.ru/catalog/product/1999922 (дата обращения: 22.01.2024).
3. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы / В.Олифер, Н.Олифер. - Санкт-Петербург: Питер, 2021. - 1008 с. - ISBN 978-5-4461-1426-9. - URL: https://ibooks.ru/bookshelf/387241/ (дата обращения: 22.01.2024).

3.2.2. Дополнительные источники:

1. Борисов, С. П. Компьютерные сети. Анализ и диагностика. Ч.1: учебное пособие / С. П. Борисов. — Москва: РТУ МИРЭА, 2021. — 67 с. — URL: https://e.lanbook.com/book/176562 (дата обращения: 22.01.2024).
2. Гольдштейн Б. С. IP-Телефония / Б.С. Гольдштейн, А.В. Пинчук, А.Л. Суховицкий. - Санкт-Петербург: БХВ-Петербург, 2014. - 336 с. - ISBN 978-5-9775-3341-6. - URL: https://ibooks.ru/bookshelf/340669/reading (дата обращения: 22.01.2024).
3. Кенин, А. М. Самоучитель системного администратора/ А.М. Кенин, Д.Н. Колисниченко. - 6-е изд., перераб. и доп. - Санкт-Петербург: БХВ-Петербург, 2021. - 608 с. - ISBN 978-5-9775-6703-9. - URL: https://ibooks.ru/bookshelf/380054/ (дата обращения: 22.01.2024).
4. Москалев, А. А. Основы проектирования и документирования вычислительной сети: учебное пособие для вузов / А. А. Москалев. — Санкт-Петербург: Лань, 2024. — 120 с. — ISBN 978-5-507-49625-9. — URL: https://e.lanbook.com/book/424583 (дата обращения: 22.01.2024).
5. Передача речи в IP-сетях: учебное пособие / В. А. Александров, А. В. Глушко, В. А. Гриднев [и др.]. — Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2023. — 129 с. — URL: https://e.lanbook.com/book/426017 (дата обращения: 19.01.2024).

МДК.03.02. ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

3.2.1 Основные электронные издания:

1. Страшун, Ю. П. Технические средства автоматизации и управления на основе IIoT/IoT: учебное пособие / Ю. П. Страшун. — Санкт-Петербург: Лань, 2020. — 76 с. — ISBN 978-5-8114-5018-3. — URL: https://e.lanbook.com/book/143701(дата обращения: 22.01.2024).
2. Шишов, О. В. Технические средства автоматизации и управления: учебное пособие для среднего профессионального образования/ О.В. Шишов. — Москва: ИНФРА-М, 2024. — 396 с.— ISBN 978-5-16-015283-7. - URL: https://znanium.ru/catalog/product/2126820 (дата обращения: 18.02.2024).
1. Шишов, О. В. Современные средства АСУ ТП: учебник / О. В. Шишов. - Москва; Вологда: Инфра-Инженерия, 2021. - 532 с. - ISBN 978-5-9729-0622-2. - URL: https://znanium.ru/catalog/product/1831992 (дата обращения: 18.02.2024).

3.2.2 Дополнительные источники:

1. Страшун, Ю. П. Технические средства автоматизации и управления на основе IIoT/IoT: учебное пособие / Ю. П. Страшун. — Санкт-Петербург: Лань, 2020. — 76 с. — ISBN 978-5-8114-5018-3. — URL: https://e.lanbook.com/book/143701(дата обращения: 22.01.2024).
2. Трофимов, В. Б. Экспертные системы в АСУ ТП: учебник / В. Б. Трофимов, И. О. Темкин. - Москва; Вологда: Инфра-Инженерия, 2020. - 284 с. - ISBN 978-5-9729-

0480-8. - URL: https://znanium.com/catalog/product/1168648 (дата обращения: 18.02.2024).
3. Червинский, В. В. Средства специализированных телекоммуникационных шин и сетей систем управления: учебное пособие / В. В. Червинский, О. С. Волуева, В. В. Турупалов; под ред. В. В. Турупалова. - Москва; Вологда: Инфра-Инженерия, 2022. - 164 с. - ISBN 978-5-9729-0976-6. - URL: https://znanium.com/catalog/product/1902696 (дата обращения: 18.02.2024).
4. Шишов, О. В. Программируемые контроллеры в системах промышленной автоматизации: учебник для среднего профессионального образования/ О.В. Шишов. — Москва: ИНФРА-М, 2023. — 365 с.— ISBN 978-5-16-015321-6. - URL: https://znanium.ru/catalog/product/1900931 (дата обращения: 18.02.2024).
5. Юсупов, Р. Х. Основы автоматизированных систем управления технологическими процессами: учебное пособие / Юсупов Р.Х. - Москва: Инфра-Инженерия, 2018. - 132 с. ISBN 978-5-9729-0229-3. - URL: https://znanium.com/catalog/product/989081 (дата обращения: 18.02.2024).

МДК.03.03. БЕЗОПАСНОСТЬ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

3.2 Информационное обеспечение реализации программы

3.2.1. Основные электронные издания:

1. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры: учебник для среднего профессионального образования / А.В. Назаров, А.Н. Енгалычев, В.П. Мельников. — Москва: КУРС: ИНФРА-М, 2023. — 360 с. — ISBN 978-5-906923-06-6. - URL: https://znanium.ru/catalog/product/1999922 (дата обращения: 22.01.2024).
2. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы / В.Олифер, Н.Олифер. - Санкт-Петербург: Питер, 2021. - 1008 с. - ISBN 978-5-4461-1426-9. - URL: https://ibooks.ru/bookshelf/387241/ (дата обращения: 22.01.2024).
3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для среднего профессионального образования / В.Ф. Шаньгин. — Москва: ФОРУМ: ИНФРА-М, 2023. — 416 с. — ISBN 978-5-8199-0754-2. - URL: https://znanium.ru/catalog/product/1910870 (дата обращения: 22.01.2024).

3.2.2. Дополнительные источники:

6. Введение в криптографическую защиту информации объектов: учебник для среднего профессионального образования/ С. Н. Ильиных, С. Г. Алюшина, Т. И. Калинкина [и др.]. — Москва: МТУСИ, 2021. — 276 с. — URL: https://e.lanbook.com/book/215231 (дата обращения: 22.01.2024).
7. Елисеев, А. И. Технологии виртуальных частных сетей: учебное пособие / А. И. Елисеев, Ю. В. Минин. — Тамбов: ТГТУ, 2019. — 96 с. — ISBN 978-5-8265-2091-8. — URL: https://e.lanbook.com/book/320063 (дата обращения: 22.01.2024).
8. Маршаков, Д. В. Программно-аппаратные средства защиты информации: учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону: Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — URL: https://e.lanbook.com/book/237770 (дата обращения: 22.01.2024).
9. Кенин, А. М. Самоучитель системного администратора / А.М. Кенин, Д.Н. Колисниченко. - 6-е изд., перераб. и доп. - Санкт-Петербург: БХВ-Петербург, 2021. - 608 с. - ISBN 978-5-9775-6703-9. - URL: https://ibooks.ru/bookshelf/380054/reading (дата обращения: 22.01.2024).
10. Таненбаум, Э. Компьютерные сети/ Э. Таненбаум, Д. Уэзеролл. - Санкт-Петербург: Питер, 2023. - 6-е изд. - 992 с. - ISBN 978-5-4461-1766-6. - URL: https://ibooks.ru/bookshelf/390207 (дата обращения: 22.01.2024).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование ПК и ОК, формируемых в рамках модуля	Критерии оценки	Методы оценки
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	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 лабораторных занятиях, при выполнении работ по учебной и производственной практикам Защита отчетов по лабораторным работам Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различными контекстам	Подбор вариантов решения конкретной профессиональной задачи или проблемы	Оценка полноты перечня подобранных вариантов
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	Демонстрация навыков использования информационных порталов в сети Интернет, включая официальные информационно-правовые порталы	Оценка полноты перечня подобранных вариантов
ОК 03. Планировать и реализовывать собственное профессиональное и	Демонстрация интереса к выбранной специальности, к	Участие в мероприятиях (олимпиады, конкурсы профессионального

личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	инновационным технологиям в области профессиональной деятельности	мастерства, стажировки и др.), проводимых как образовательным заведением, так и ведущими предприятиями отрасли
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	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. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	Демонстрация навыков грамотной устной и письменной речи	Экспертное наблюдение навыков устного и письменного общения в ходе обучения
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	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. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы	Формирование бережного отношения к природе и окружающей среде	Экспертное наблюдение демонстрации навыков соблюдения правил экологической безопасности в ведении

бережливого производства, эффективно действовать в чрезвычайных ситуациях		профессиональной деятельности; формирование навыков эффективных действий в чрезвычайных ситуациях
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	Формирование бережного отношения к здоровью	Участие в спортивных мероприятиях, проводимых образовательным учреждением; ведение здорового образа жизни
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	Демонстрация умения составлять тексты документов, относящихся к профессиональной деятельности, на государственном и иностранном языках	Экспертная оценка соблюдения правил составления документов