ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

ВЫСШИЙ КОЛЛЕДЖ «ПОЛИТЕХНИК»

УТВЕРЖДАЮ
Заместитель директора по УМР
_____ Е.Ю. Кузнецов
«05» апреля 2024 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

по специальности 09.02.06 Сетевое и системное администрирование

2024

РАССМОТРЕНА И ОДОБРЕНА

Предметно-цикловой комиссией
Протокол № 7
«04» апреля 2024 г.
Председатель ПЦК_____/Л.И. Логинова/

Рабочая программа профессионального модуля ПМ.03 Эксплуатация объектов сетевой инфраструктуры разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование.

Разработчик:

Морохин Д.В., преподаватель с ученой степенью кандидата технических наук, доцент, заведующий кафедрой информационно-вычислительных систем ФГБОУ ВО «Поволжский государственный технологический университет»

Рецензент (внутренний)

Кузнецов Е.Ю., преподаватель с ученой степенью кандидата технических наук, заместитель директора по УМР Высшего колледжа ПГТУ «Политехник»

Рецензент (внешний)

Савинов А.Н., преподаватель с ученой степенью кандидата технических наук, доцент кафедры информационно-вычислительных систем ФГБОУ ВО «Поволжский государственный технологический университет»

Рецензент (представитель работодателя)

Лоханов М.А., заместитель начальника отдела информационных технологий локальной вычислительной сети и компьютерной техники – начальник бюро АО «Марийский машиностроительный завод»

©Морохин Д.В., 2024

СОДЕРЖАНИЕ

1. АННОТАЦИЯ
2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1. АННОТАЦИЯ

Профессиональный модуль ПМ.03 Эксплуатация объектов сетевой инфраструктуры относится к профессиональному циклу профессиональной подготовки по программе подготовки специалистов среднего звена (далее ППССЗ) специальности 09.02.06 Сетевое и системное администрирование.

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

иметь практический опыт:

– обслуживания сетевой инфраструктуры, восстановлении работоспособности сети после сбоя;

– удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;

– поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры.

Общий объем учебной нагрузки по профессиональному модулю составляет 618 часов, нагрузка во взаимодействии с преподавателем составляет 355 часов, часов самостоятельной работы – 63 часа.

Содержание профессионального модуля включает изучение следующих разделов:

МДК.03.01 Эксплуатация сетевой инфраструктуры.

Тема 1. Эксплуатация технических средств сетевой инфраструктуры.

Тема 2. Эксплуатация систем IP-телефонии.

МДК.03.02 Технологии автоматизации технологических процессов.

Тема 1. Автоматизированные системы управления технологическими процессами (АСУ ТП).

Тема 2. Промышленные сетевые технологии и протоколы в АСУ ТП

МДК.03.03 Безопасность сетевой инфраструктуры.

Тема 1. Безопасность компьютерных сетей

Тема 2. Обеспечение сетевой безопасности

Текущий контроль проводится в форме оценки тестирования, решения ситуационных задач и выполнения практических работ.

Форма промежуточной аттестации – дифференцированный зачет, экзамен, квалификационный экзамен.

2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Место профессионального модуля в структуре программы подготовки специалистов среднего звена: профессиональный модуль ПМ.03 Эксплуатация объектов сетевой инфраструктуры относится к профессиональному учебному циклу профессиональной подготовки программы подготовки специалистов среднего звена по специальности среднего профессионального образования 09.02.06 Сетевое и системное администрирование.

2.2. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен освоить вид деятельности: Эксплуатация объектов сетевой инфраструктуры и соответствующие ему профессиональные компетенции:

Код	Наименование результата обучения
ВД.	Эксплуатация объектов сетевой инфраструктуры.
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.

Освоение профессионального модуля направлено на развитие общих компетенций:

Код	Наименование результата обучения
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.

Результаты обучения (знания, умения, практический опыт)

В результате освоения профессионального модуля обучающийся 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. – 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. – Фильтровать, контролировать и обеспечивать безопасность сетевого трафика. – Определять влияние приложений на проект сети. – 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. – Оформлять техническую документацию. – Определять влияние приложений на проект сети. – Анализировать схемы потоков трафика в компьютерной сети. – Оценивать качество и соответствие требованиям проекта сети –
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. –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 –Использовать программно-аппаратные средства технического контроля. –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. –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 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 устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование. – Средства тестирования и анализа. – Базовые протоколы и технологии локальных сетей. – 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. – Требования к компьютерным сетям. – Требования к сетевой безопасности. – Элементы теории массового обслуживания. – Основные понятия теории графов. – Основные проблемы синтеза графов атак. – Системы топологического анализа защищенности компьютерной сети. – Архитектуру сканера безопасности. – 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. – Принципы и стандарты оформления технической документации – Принципы создания и оформления топологии сети. – Информационно-справочные системы для замены (поиска) технического оборудования –

2.3. Количество часов, отводимое на освоение профессионального модуля:

Всего часов – 684 часа, в том числе:

на освоение МДК - 378 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося–308 часов;

самостоятельной работы обучающегося– 48 часов;

на практики:

учебную – 144 часа;

производственную –144 часа.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЭКСПЛУАТАЦИЯ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

3.1. Тематический план профессионального модуля

Код профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)									Практика	
			Обязательная аудиторная учебная нагрузка обучающегося						Самостоятельная работа обучающегося, часов	консультации часов	Промежуточная аттестация	Учебная, часов	Производственная часов
			Всего, часов	теоретическое	практические занятия, часов	лабораторные занятия, часов	Семинар. занятия	в т.ч., курсовая работа (проект), часов					
1	*2*	*3*	*4*	*5*	*6*	*7*		*8*	*9*	*10*	*11*	*12*	*13*
ПК 3.1 - ПК 3.5 ОК.01-ОК.09	МДК.03.01 Эксплуатация сетевой инфраструктуры	**90**	**64**	**30**	**34**	**-**	**-**	**-**	**6**	**2**	**-**	**144 (4 нед)**	**144 (4 нед)**
ПК 3.1 - ПК 3.6 ОК.01-ОК.11	МДК.03.02 Технологии автоматизации технологических процессов	**117**	**102**	**50**	**52**	**-**	**-**	**-**	**15**	**-**	**-**		
ПК 3.1 - ПК 3.6 ОК.01-ОК.11	МДК.03.02 Безопасность сетевой инфраструктуры	**171**	**142**	**56**	**56**	**-**	**-**	**30**	**27**	**2**	**-**		
ПК 3.1 - ПК 3.6 ОК.01-ОК.11	Учебная практика	**144**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**		
ПК 3.1 - ПК 3.6 ОК.01-ОК.11	Производственная практика	**144**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**		
	Экзамен (квалификационный)	**18**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**18**		
	Всего:	**684**	**308**	**136**	**142**	**-**	**-**	**30**	**48**	**4**	**18**	**144**	**144**

3.2. Тематический план и содержание профессионального модуля ПМ.03 Эксплуатация объектов сетевой инфраструктуры

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)		Объем часов	Коды компетенций, формированию которых способствует элемент учебной дисциплины
1	*2*		*3*	*4*
ПМ.03 Эксплуатация объектов сетевой инфраструктуры.				
МДК.03.01 Эксплуатация сетевой инфраструктуры.			**70**	
Тема 1. Эксплуатация объектов сетевой инфраструктуры.	**Содержание учебного материала**		**18**	ПК 3.1 - ПК 3.5 ОК.01-ОК.09
	1	Физическое вмешательство в инфраструктуру сети. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.	2	
	2	Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб).	2	
	3	Замена существующей аппаратуры. Увеличение количества узлов сети; увеличение протяженности связей между объектами сети	2	
	4	Логическая топология компьютерной сети. Техническая и проектная документация. Паспорт технических устройств.	2	
	5	Проверка объектов сетевой инфраструктуры и профилактические работы.	2	
	6	Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.	2	
	7	Техническая и проектная документация. Паспорт технических устройств.	2	
	8	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.	2	
	9	Анализ основных характеристик протокола SNMP, его структуры и архитектуры, формата сообщений и спецификации синтаксиса Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.	2	
	Практические занятия		**20**	

	1	Оконцовка кабеля витая пара	2	
	2	Заделка кабеля витая пара в розетку	2	
	3	Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену	2	
	4	Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы)	2	
	5	Выполнение действий по устранению неисправностей. Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.	2	
	6	Оформление технической документации, правила оформления документов	2	
	7	Протокол управления SNMP. Основные характеристики протокола SNMP. Набор услуг (PDU) протокола SNMP. Формат сообщений SNMP.	2	
	8	Задачи управления: анализ производительности сети, анализ надежности сети	2	
	9	Управление безопасностью в сети. Учет трафика в сети	2	
	10	Средства мониторинга компьютерных сетей. Средства анализа сети с помощью команд сетевой операционной системы	2	
Тема 2. Эксплуатация систем IP-телефонии.	**Содержание учебного материала**		**12**	ПК 3.1 - ПК 3.5 ОК.01-ОК.09
	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	
	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.	2	
	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.	2	
	4	Управление программным коммутатором. Маршрутизация. Группы соединительных линий. Подключение станций с TDM (абонентский доступ TDM).	2	
	5	Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP-абоненты. Группы абонентов. Дополнительные абонентские услуги. Организация эксплуатации систем IP-телефонии. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт.	2	

	6	Восстановление работы сети после аварии. Схемы послеаварийного восстановления работоспособности сети. Техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных.	2	
	Практические занятия		**14**	
	1	Настройка аппаратных IP-телефонов.	2	
	2	Настройка программных IP-телефонов, факсов.	2	
	3	Развертывание сети с использованием VLAN для IP-телефонии. Настройка шлюза.	2	
	4	Установка, подключение и первоначальные настройки голосового маршрутизатора. Настройка таблицы пользователей в голосовом маршрутизаторе. Настройка групп в голосовом маршрутизаторе.	2	
	5	Настройка программно-аппаратной IP-АТС. Установка и настройка программной IP-АТС (например, Asterisk).	2	
	6	Мониторинг и анализ соединений по различным протоколам. Мониторинг вызовов в программном коммутаторе.	2	
	7	Создание резервных копий баз данных. Диагностика и устранение неисправностей в системах IP-телефонии	2	
	Самостоятельная работа обучающихся		6	

	Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление лабораторных работ, отчетов и подготовка к их защите. **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. 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.			
	Консультации		**2**	
	Промежуточная аттестация		**18**	
МДК.03.02 Технологии автоматизации технологических процессов.			**117**	
Тема 1. Автоматизированные системы управления технологическими процессами (АСУ ТП)	**Содержание учебного материала**		**10**	ПК 3.1 - ПК 3.5 ОК.01-ОК.09
	1	Понятие об объекте управления. Свойства объекта управления.ассификация технологических объектов управления по типу, характеру технологического процесса, по характеристике параметров управления Классификация систем управления технологическими объектами по способу, цели и степени централизации управления. Общие сведения об автоматизированных системах управления технологическими процессами (АСУТП) и системах автоматического управления (САУ)	2	
	2	Основные функции АСУТП и САУ. Техническое, программное и информационное обеспечение АСУТП Структура АСУТП на базе микропроцессорной техники. Средства измерения преобразования и регулирования в АСУТП	2	

	3	Основные понятия автоматизированной обработки информации Методы и средства моделирования технологических процессов в АСУТП Обзор современных технологий и тенденций развития АСУТП	2	
	4	Программирование и настройка АСУТП: языки программирования, методы и инструменты Интеграция АСУТП с другими системами и оборудованием в производственном процессе Оценка эффективности и экономическая оценка внедрения АСУТ	2	
	5	Особенности управления производственными системами в условиях неопределенности и переменных условий работы Применение систем искусственного интеллекта в АСУТП: нейронные сети, генетические алгоритмы, экспертные системы	2	
	Практические занятия		**24**	
	1	Определение свойств объектов управления на практике	4	
		Классификация технологических объектов управления на примере производственного предприятия		
	2	Анализ и сравнение систем управления технологическими объектами на примере различных отраслей промышленности	2	
	3	Изучение принципов работы АСУТП и САУ на примере реальных систем управления	2	
		Создание простой модели технологического процесса		
	4	Ознакомление с современными технологиями АСУТП на примере существующих проектов и исследований	2	
		Программирование элементов АСУТП на языках программирования на практике		
	5	Настройка и проверка работоспособности элементов АСУТП на примере конкретной системы управления	2	
	6	Интеграция АСУТП с другими системами и оборудованием в производственном процессе	4	
		Оценка эффективности и экономическая оценка внедрения АСУТП		
	7	Разработка системы управления производственными процессами в условиях неопределенности и переменных условий работы	2	
	8	Применение нейронных сетей в системах управления технологическими процессами	2	
		Применение экспертных систем в системах управления технологическими процессами		
	9	Создание проекта автоматизации управления технологическим процессом на основе АСУТП	2	
		Определение свойств объектов управления на практике	2	
		Классификация технологических объектов управления на примере производственного предприятия		
Тема 2. Промышленные	**Содержание учебного материала**		**40**	

сетевые технологии и протоколы в АСУ ТП	1	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	ПК 3.1 - ПК 3.5 ОК.01-ОК.09
	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.	2	
	3	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.	2	
	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.	2	
	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.	2	
	6	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.	2	
	7	Основные принципы работы в режимах slave и master, а также процедуры обмена данными между ними с использованием протокола MODBUS.	2	
	8	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.	2	
	9	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.	2	
	10	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.	2	

	11	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.	2	
	12	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.	2	
	13	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.	2	
	14	Различные протоколы и технологии, используемые в системах умного дома (ZigBee, Z-Wave, Thread, Bluetooth, Wi-Fi и другие). Особенности их применения в системах автоматизации умного дома. Аспекты безопасности и защиты данных в системах умного дома, возможности интеграции различных устройств и систем в одну сеть.	2	
	15	Преобразователи интерфейсов для различных стандартов связи (RS-232, RS-485, Ethernet, USB). Выбор и настройка преобразователей интерфейсов в соответствии с требованиями конкретной задачи.	2	
	16	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.	2	
	17	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.	2	
	18	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.	2	
	19	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.	2	

	20	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.	2	
	Практические работы		**28**	
	1	Работа с основными сетевыми технологиями в промышленной автоматизации	2	
		Разработка схемы промышленной сети и выбор средств ее реализации		
	2	Практическое применение протокола MODBUS для обмена данными между устройствами	2	
	3	Создание конфигурации сети с использованием протокола MODBUS	2	
		Организация работы контроллера (slave) и операторной панели (master) по протоколу MODBUS		
	4	Выравнивание адресов переменных в поле памяти протокола MODBUS	2	
		Настройка работы контроллера (master) с модулями ввода/вывода (slave) по протоколу MODBUS RTU		
	5	Практическая работа с различными устройствами по протоколу MODBUS RTU	2	
		Работа с протоколом MODBUS TCP		
	6	Работа с типовыми проводными и кабельными протоколами в промышленности	2	
		Изучение беспроводных локальных сетей для промышленного применения		
	7	Практическое применение специализированных сетевых интерфейсов для умного дома	2	
		Работа с преобразователями интерфейсов в промышленной сети		
	8	Ознакомление с современными тенденциями в развитии сетевых технологий в АСУ ТП, включая web-серверы и облачные решения	2	
	9	Особенности применения промышленных сетевых протоколов в условиях высоких нагрузок и плохой связи	2	
	10	Сравнительный анализ промышленных Ethernet-технологий: EtherNet/IP, PROFINET, Modbus TCP	2	
	11	Применение промышленных маршрутизаторов для обеспечения безопасности и надежности работы сетевой инфраструктуры	2	
	12	Практическое использование промышленных маршрутизаторов	2	
		Организация удаленного доступа к сетевым устройствам в промышленной сети		
	13	Разработка и тестирование собственного промышленного протокола для обмена данными между устройствами в сети	2	
	14	Организация кластера промышленных компьютеров для выполнения высокопроизводительных вычислений в АСУ ТП	2	

Самостоятельная работа обучающихся			**15**	
Примерная тематика самостоятельной учебной работы при изучении раздела 2. Технологии автоматизации технологических процессов Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление лабораторных работ, отчетов и подготовка к их защите. 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 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.				
МДК 03.03 Безопасность сетевой инфраструктуры			**171**	ПК 3.1 - ПК 3.5 ОК.01-ОК.09
Тема 3 Безопасность компьютерных сетей	**Содержание учебного материала**		**26**	
	1	**Фундаментальные принципы безопасной сети** Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.	2	
	2	**Безопасность сетевых устройств OSI** Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.	2	
	3	**Авторизация, аутентификация и учет доступа (AAA)** Свойства AAA. Локальная AAA аутентификация. Server-based AAA	2	

	4	**Реализация технологий брандмауэра ACL.** Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах.	2	
	5	**Реализация технологий предотвращения вторжения** IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS	2	
	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	2	
	7	**Криптографические системы** Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей	2	
	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	2	
	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.	2	
	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.	2	
	11	**Межсетевая безопасность** Методы обеспечения безопасности взаимодействия между различными сетями. Реализация технологий маршрутизации и шлюзов, использование межсетевых экранов, технологии виртуальных локальных сетей.	2	
	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.	2	
	13	**Защита от социальной инженерии** Методы социальной инженерии, опасности, связанные с подделкой и манипулированием данными, а также методы защиты и обучения персонала.	2	
	Практические занятия		**14**	

	1	Социальная инженерия Исследование сетевых атак и инструментов проверки защиты сети	2	
	2	Настройка безопасного доступа к маршрутизатору Обеспечение административного доступа AAA и сервера Radius	2	
	3	Настройка политики безопасности брандмауэров Настройка системы предотвращения вторжений (IPS)	2	
	4	Настройка безопасности на втором уровне на коммутаторах Исследование методов шифрования	2	
	5	Настройка Site-to-SiteVPN используя интерфейс командной строки Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки	2	
	6	Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM	2	
	7	НастройкаClientless Remote Access SSL VPNs используя ASDM Настройка AnyConnect Remote Access SSL VPN используя ASDM	2	
Тема 2 Обеспечение сетевой безопасности	**Содержание учебного материала**		**30**	ПК 3.1 - ПК 3.5 ОК.01-ОК.09
	1	Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть. Механизмы шифрования и аутентификации для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам и сервисам.	2	
	2	Использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети.	2	
	3	Методы минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях. Введение системы обнаружения и предотвращения сетевых вторжений.	2	
	4	Технологии использования виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа. Использование системы управления доступом для контроля доступа к корпоративной сети.	2	
	5	Обеспечение безопасности Wi-Fi-сетей. Реализация мер по обеспечению безопасности электронной почты в корпоративной сети.	2	
	6	Защита от атак типа "фишинг".	2	

	7	Применение антивирусного программного обеспечения для защиты от вирусов и других вредоносных программ.	2	
	8	Использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.	2	
	9	Защита от DDoS-атак.	2	
	10	Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети.	2	
	11	Защита от внутренних угроз безопасности.	2	
	12	Обеспечение безопасности облачных сервисов.	2	
	13	Организация мониторинга сетевой безопасности и аудита.	2	
	14	Введение системы контроля целостности файлов для защиты от изменения или внедрения вредоносных программ в файловые системы.	2	
	15	Применение методов шифрования данных для защиты от несанкционированного доступа к конфиденциальной информации.	2	
	Практические занятия		**42**	
	1	Настройка VPN-туннелей для организации защищенных каналов передачи данных между территориально распределенными офисами.	2	
	2	Работа с механизмами шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.	2	
	3	Настройка и использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.	2	
	4	Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети с использованием программного обеспечения для мониторинга и обнаружения угроз.	2	
	5	Разработка и внедрение мер по минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.	2	
	6	Настройка и работа с системами обнаружения и предотвращения сетевых вторжений для раннего обнаружения и предотвращения угроз безопасности.	2	
	7	Настройка и использование виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.	2	
	8	Настройка и работа с системами управления доступом для контроля доступа к корпоративной сети.	2	
	9	Обеспечение безопасности Wi-Fi-сетей: настройка безопасных точек доступа, использование сетевой аутентификации, шифрования трафика и других методов.	2	
	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.	2	
	11	Обучение пользователям основам защиты от атак типа "фишинг".	2	

	12	Работа с антивирусным программным обеспечением для защиты от вирусов и других вредоносных программ: установка, настройка, обновление базы данных, сканирование и удаление вредоносных программ.	2	
	13	Настройка и использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.	2	
	14	Настройка и использование межсетевых экранов и фаерволов для обеспечения комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.	2	
	15	Внедрение системы управления доступом для контроля доступа к корпоративной сети: настройка правил доступа, аутентификация пользователей, управление привилегиями.	2	
	16	Использование технологий виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа: настройка и управление VPN-туннелями, защита данных, маршрутизация трафика.	2	
	17	Обеспечение безопасности Wi-Fi-сетей: настройка и управление беспроводными точками доступа, защита сетевого трафика, аутентификация пользователей.	2	
	18	Защита от DDoS-атак: использование специализированных средств защиты от DDoS-атак, настройка маршрутизации трафика, мониторинг сетевой активности.	2	
	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.	2	
	20-21	Обеспечение безопасности облачных сервисов: выбор надежных провайдеров облачных сервисов, настройка правил доступа и аутентификации, шифрование данных, мониторинг активности в облачных сервисах.	4	
	Самостоятельная работа		27	
	Примерная тематика самостоятельной учебной работы при изучении раздела 3. Безопасность сетевой			

	инфраструктуры Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторным работам с использованием методических рекомендаций преподавателя, оформление лабораторных работ, отчетов и подготовка к их защите. 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. 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.		

Тематика курсовых проектов (работ) 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. 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.	30	ПК 3.1 - ПК 3.5 ОК.01-ОК.09
Учебная практика		
Виды работ 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	**144**	
Производственная практика		
Виды работ 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.	**144**	
Консультации	**2**	
Экзамен (квалификационный)	**18**	
Всего	**684**	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Материально-техническое обеспечение профессионального модуля ПМ.03 Эксплуатация объектов сетевой инфраструктуры

Лаборатория информационных технологий

Комплект мебели для учебного процесса.

Мультимедийное оборудование: персональные компьютеры – 14 шт., подключенные к локальной вычислительной сети и сети «Интернет»; ноутбуки – 4 шт., проектор мультимедийный, экран.

Программное обеспечение: Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); Mathcad University Classroom Perpetual – 40 (лицензия №296133); комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); комплект ПО для решения основных пользовательских задач (свободно распр. ПО); Справочная правовая система «Консультант Плюс» (контракт №2025_СВ_2 от 04.12.2024г); эмулятор активного сетевого оборудования (Cisco Packet Tracer (свободно-распространяемое для студентов)); программное обеспечение сетевого оборудования (точки доступа CISCO CAP 26021-R-K9, ПО коммутатора CiscoCatalyst 2960, ПО коммутатора Cisco Catalyst WS-C2960); 7-Zip (свободно распр. ПО); Internet Explorer, Yandex Browser(свободно распр. ПО); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); PDF24 (свободно распр. ПО); КОМПАС-3D V19 (лицензия №Вг-20-00154); Cisco Packet Tracer 6.2sv(свободно распр. ПО); Hyper-V, Oracle VirtualBox (свободно распр. ПО); Облачная платформа Yandex Cloud.

Средства обучения: интерактивная доска, медиатека (мультимедиа разработки и презентации к занятиям), раздаточный материал: учебные карточки с заданиями, дидактический материал для выполнения практических работ, гигабитный управляемый коммутатор на 16 портов; структурированная кабельная система; стойки для серверов – 2шт, сервер AQS-QEE-E50D202*11410F225D01; сервер AquariusSrv PX 102; ОСЦИЛЛОГРАФ С1-75; коммутатор NETGEAR ^FC728TSEU; коммутатор SWtch SS101 TX DEV8x10; эмулятор ATICE200, источник беспереб. питания Smart-UPS 1000i USB - 2 шт.; стенды сетей передачи данных (коммутатор CiscoCatalyst 2960, коммутатор TrendNetN-WaySwitchTEGS160TX, коммутатор WS-C2960-48TT с конвертором, коммутатор ЛВС, коммутатор Cisco Catalyst WS-C2960; программно-технический комплекс WS-C2960-48TS с установлен. программным обеспечением), точка доступа CISCO CAP 26021-R-K9, IP- видеокамера Nikvision, анализатор спектра NS-30A, антенна M102 в компл. с кабелем ВЧ TNCm-SMAm, блок питания лаборат. HY 3003 D-3, внешний HDD WD 2TB 3.0 , 3.5"USB, внешний накопитель 1 Seagate Original USB 3.0 4 Tb, универсальная приёмо-передающая платформа для проектирования СВЧ-систем компл.mgx 92, усилитель LZY-22, усилитель ZHL-3A-S, измеритель CN -801 HP, источник бесперебойного питания APC Smart-UPS 1000VA, многофункциональный измерительный прибор, МФУ – 2 шт., набор

ВЧпереходников, паяльная станция AOYUE 968, переключатель ZX80-DR230, преобразователь SP-200-24-AC-DC, приемо-передающая программно-конфигурируемая радиоплатформа G32, принтер, станок сверлильный 350 вт.

Лаборатория направляющих систем
Комплект мебели для учебного процесса.
Мультимедийное оборудование: интерактивная доска -1 шт, компьютеры - 15 шт.: ПК H404,2 420W/Intel Core i3 540/клав., мышь,монит. 21,5" VA2248-LED; ПК RAY S902.4(клав.,мышь оптич.,пачкорд,ИДТО ,монитор 21,5 " View Sonic VA2248-LED; монитор 17" LCD PROVIEW VA-796KN; принтер струйный рулон. HP500 120*600, проектор.
Программное обеспечение: «Адепт: Управление строительством» (контракт № А-859); Autodesk AutoCAD (регистрация на сайте производителя); Autodesk ReCap (регистрация на сайте производителя); CREDO DAT 5.2 (лицензия №1249.28749.28.08-13); MapInfo Professional (лицензионный договор №32/2014-У); Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); комплект ПО для решения основных пользовательских задач (свободно распр. ПО); Справочная правовая система «Консультант Плюс» (контракт №2025_СВ_2 от 04.12.2024г); Renga (лицензия №ДЛ-19-00224); SCAD Office s64 (лицензия № 15417); STARK ES 2019 (лицензия №066700); ГИС "Карта 2011" (сетевой USB-ключ); КОМПАС-3D V19 (лицензия №Вг-20-00154); ЛИРА-САПР 2018 PRO (сублицензионный контракт № 3641/ЙО от 21.09.2018 г.); Смета-Багира 4.0 (лицензия №4475); 7-Zip (свободно распр. ПО); Internet Explorer, Yandex Browser(свободно распр. ПО); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); PDF24 (свободно распр. ПО); КОМПАС-3D V19 (лицензия №Вг-20-00154); Cisco Packet Tracer 6.2sv(свободно распр. ПО); Hyper-V, Oracle VirtualBox (свободно распр. ПО); Облачная платформа Yandex Cloud.
Средства обучения: электрические кабели, волокнооптические кабели, комплекты инструментов, лабораторный копмлекс «Теоретические основы специальных электронных систем» источник бесп.питания APC Smart UPS 1000VA USB 2U 230V; коммутатор Cisco Catalyst WS C2960-24 PC-L; коммутатор Cisco Catalyst WS - C2960-48 TC-L; коммутатор WS-C2960-48TT с конвертором.

Лаборатория настройки сетевой инфраструктуры
Комплект мебели для учебного процесса.
Мультимедийное оборудование: компьютеры- 15 шт: RAMEC STORM Custom i7-3770K/8ГБ/ монитор LCD 21.5", клавиат., мышь, 15 шт.; ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATA II/INWIN ATX-450, монитор BenQ G2450HM, клав, мышь, 3 шт.; ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb

SATAIII/INWIN EAR003, монитор 24" BenQ G2450HM,клав, мышь, 2 шт.; ПК P212,4 675W/Intel Core i7-2600/кл, мышь, мон. Ben Q EW2430, 2 шт.
Программное обеспечение: Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); комплект ПО для решения основных пользовательских задач (свободно распр. ПО); Справочная правовая система «Консультант Плюс» (контракт №2025_СВ_2 от 04.12.2024г); 1С:Предприятие 8. Комплект для обучения. (лицензия №8922961); Программный комплекс "Компьютерная деловая игра "БИЗНЕС-КУРС: Максимум. версия 1" (лицензия №БК-М1-СЕТ-1169); Смета-Багира 5.0 (лицензия №5451); 7-Zip (свободно распр. ПО); Internet Explorer, Yandex Browser(свободно распр. ПО); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); PDF24 (свободно распр. ПО); КОМПАС-3D V19 (лицензия №Вг-20-00154); Cisco Packet Tracer 6.2sv(свободно распр. ПО); Hyper-V, Oracle VirtualBox (свободно распр. ПО); Облачная платформа Yandex Cloud.
Средства обучения: шкаф телекоммуникационный- 2 шт., Сервер – 1шт, Серверный SSD накопитель – 10 щт., KMV- переключатель ATEN – 1 шт, анализатор линейных коммуникаций УЛАН-2; доска маркерная 100*200см; ИБП UPS 1100VA, 7 шт.; коммутатор D-Link DES-3200-28, 8 шт.; коммутатор D-Link DES-3810-28, 2 шт.; коммутатор; комплекс защиты информации Secret Disk 4.0; Комплекс защиты информации Secret Net 5.0, 2 шт.; нелинейный локатор SEL SP-61/M "Катран"; проектор мультимедийный Hitachi CP-X1250+разветвитель видеосигнала; система виброакустической защиты "Соната-АВ"; система виброакустической.защиты "Соната-РС2"; сплит-система (напольно-потолочный кондиционер) GeneralClimate CF24HRN1/GU24HRN1; средства ограничения доступа к компьютеру АПМДЗ "КРИПТОН-ЗАМОК/Е", 3 шт.; экран настенный 200*200см Braun Roll Vision;

Мастерская монтажа и настройки объектов сетевой инфраструктуры
Комплект мебели для учебного процесса.
Мультимедийное оборудование: интерактивная доска, компьютеры в комплекте (системный блок, монитор, клавиатура, манипулятор «мышь») – 7 шт., локальная сеть с выходом в ИНТЕРНЕТ, проектор мультимедийный HITACHICP-X2514WN 1шт. компьютер P4-3.0/2*256Mb/HDD 200Gb/128 6600GT/DVD-RW/KM/FDD/ MBi945P/ UPS; монитор 19" Samsung 940N (KSB) TFT Silver. Round Simple, 3 шт.; монитор 19"Samsung 940N (LKSB) TFT; монитор LG LCD 19" L1919S-SF; Систем.блок Athlon 64 3500/512Mb*2/ 160Gb/FDD/DVD-RW клав. мышь. ковр., 2 шт.; систем. блок Core 2Duo E6320/2Гб/320Гб/512Мб клав. мышь, 2 шт.; систем.блок АМД3000+ (512*2)/160Gb/DVD+RWrkfd/+мышь+коврик+клвав.; системный блок AMD*2 4000/2*512 MB/160Gb/512 MB.
Программное обеспечение: Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project

Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); Mathcad University Classroom Perpetual - 40 (лицензия №296133); комплект ПО для решения основных пользовательских задач (свободно распр. ПО); Справочная правовая система «Консультант Плюс» (контракт №2025_СВ_2 от 04.12.2024г); Mathcad University Classroom Perpetual - 40 (лицензия №296133); 7-Zip (свободно распр. ПО); Internet Explorer, Yandex Browser(свободно распр. ПО); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); PDF24 (свободно распр. ПО); КОМПАС-3D V19 (лицензия №Вг-20-00154); Cisco Packet Tracer 6.2sv(свободно распр. ПО); Hyper-V, Oracle VirtualBox (свободно распр. ПО); Облачная платформа Yandex Cloud.
Средства обучения: маршрутизатор – 2шт., коммутатор – 2 шт, точка доступа Wi-Fi – 1шт.,межсетевой экран, набор для монтажа и наладки компьютерной сети – 2 шт., GPS приемник в составе; аппаратно-программный комплекс (адаптер+ПО); вольтметр В7-37, 2 шт.; генератор Г2-57, 4 шт.; генератор шумовых сигналов; измеритель помех LMZ-4, 2 шт.; измеритель XG-5; измерительный прибор SNT LITE PSTN; лабораторный стенд "Цифровая электроника " 1060x256x654, 2 шт.; осцилограф GDS-820C; прибор Д/ИС КОР Х6-5; прибор Д/ИС КОР Х6-8, 2 шт.; прибор ИКХ-Х6-5; /; учебная лабораторная установка "Изучение КМ-кодека"; учебная лабораторная установка "Изучение принципов временного разделения каналов"; аппаратно-программный комплекс для изучения стандартных процедур и мониторинга сетей WiFi - 1 шт., антенны AMZ-3A/50 - 3 шт., измерители LMZ-4/50 - 4 шт., измеритель SMZ-6/50 - 1 шт., канерEpson - 1 шт., измеритель радиопомех - 1шт., радиостанция «Карат» - 2 шт., вольтметр В7-37 - 2 шт., стенд «Цифровая электроника» - 2 шт., экран настенный 200*200см Braun Roll Vision.

Мастерская ремонта и обслуживания устройств инфокоммуникационных систем
Комплект мебели для учебного процесса.
Мультимедийное оборудование: интерактивная доска – 1 шт, ноутбук ASUS K72DR 17.3" N830/4 GB/640 GB/; ноутбук IdeaPad U260 12,5" Lenovo; ноутбук Lenovo IdeaPad510S-13IKBwhite 13,3" FHD i5-7200U/4Gb/256GbSSD/R5 V430 2G/W10 сумка,мышь; ПК RAMEC GALE/i5-3470/B75M2x4DDR3/GT630/500SATA3/монит.LCD PHILIPS 23,6"клав.,мышь; планшет Apple iPad 2; планшет AppleiPad 4 32 Gb., проектор.
Программное обеспечение: Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); Комплект ПО для решения основных пользовательских задач (свободно распространяемое ПО); Справочная правовая система «Консультант Плюс» (контракт №2025_СВ_2 от 04.12.2024г); 7-Zip (свободно распр. ПО); Internet Explorer, Yandex Browser(свободно распр. ПО); Агент Dr.Web

(лицензия № QS34-HC7C-SD53-K5L2); PDF24 (свободно распр. ПО); КОМПАС-3D V19 (лицензия №Вг-20-00154); Cisco Packet Tracer 6.2sv(свободно распр. ПО); Hyper-V, Oracle VirtualBox (свободно распр. ПО); Облачная платформа Yandex Cloud.

Средства обучения: электроизмериетльные приборы – 6 шт, коммутатор – 2 шт, маршрутизатор – 2шт., источник бесперебойного питания – 2 шт.,комплекты инструментов для выполнения электромонтажных работ – 3 шт., аккумулятор гелевый Minn Kota МК-31; аппаратно-программный комплекс беспроводной регистрации и интерпретации биопотенциалов на активных электродах; генератор бензиновый "Штурм" PG8708 700Вт; зарядное устройство Minn Kota МК-110Р; инвертор - трансформатор "Фубаг" IN 160-230В 160А; комплект мобильный базовый экономичный (видеооборудование); корпус квадрокоптера DJI Phantom с двигателем и лопастями+Блок управле-ния DJI Phantom-4 (Квадрокоптер Phantom-4); навигатор CARMIN eTrex Touch 25 GPS/GLONASS; навигатор Garmin Oregon 550 GPS; проекционный комплекс на базе системы EIKI LC-XB43 с лазерным сведением изображений; система видеонаблюдения и слежения (на базе матрицы Sony Super HAD CCD); система виртуальной реальности (Шлем виртуальной реальности HTC Vive Pro с базовыми станциями и контроллерами Steam VR Tracking 2.0 + Системный блок i7-6700/16 Gb/2Gb/120Gb,клав. мышь + мани; спутниковый телефон Thuraya XT; цифровая видеокамера Экшн-камера GOPRO HEROS Black UHD 4K; цифровая фотокамера Sony Alpha A 7 kit FE 28-70/3.5-5.6 OSS; шлем виртуальной реальности HTC Vive; электромотор Minn Kota Traxxis 55; электроэнцефалограф-регистратор компьютеризированный портативный "Энцефалан-ЭЭГР -19/26".

Договоры о практической подготовке:

- АО «Марийский машиностроительный завод» Договор № 1/2021 от 01.02.2021 – бессрочный.
- Филиал ПАО «Ростелеком» в Республике Марий Эл Договор № 83/2021 от 27.01.2021 – бессрочный.

4.2. Информационное обеспечение профессионального модуля ПМ.03 Эксплуатация объектов сетевой инфраструктуры

Основная и дополнительная литература

№ п/п	Список используемой литературы (*печатные издания, электронные издания за последние 5 лет*)	Количество экземпляров, имеющихся в библиотеке, или ссылка на ЭБС
ОСНОВНАЯ ЛИТЕРАТУРА		
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/1860128 Режим доступа: для авториз. пользователей	Электронный ресурс
2	**Сергеев, А. Н.** Основы локальных компьютерных сетей / А. Н. Сергеев. - 3-е изд., стер. - Санкт-Петербург: Лань, 2023. - 184 с. - ISBN 978-5-507-46832-4. - Текст : электронный // Лань : электронно-библиотечная система.-URL: https://e.lanbook.com/book/321215 Режим доступа: для авториз. пользователей	Электронный ресурс
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА		
1	**Кутузов, О. И.** Инфокоммуникационные системы и сети : учебник для спо / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 244 с. — ISBN 978-5-8114-8488-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176902 Режим доступа: для авториз. пользователей	Электронный ресурс
2	**Журавлев, А. Е.** Инфокоммуникационные системы. Аппаратное обеспечение / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 396 с. — ISBN 978-5-507-44963-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/322610 Режим доступа: для авториз. пользователей	Электронный ресурс

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в форме текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация имеет целью определить степень достижения запланированных результатов обучения по профессиональному модулю за период обучения. Форма промежуточной аттестации - дифференцированный зачет, экзамен (квалификационный).

Текущий контроль успеваемости осуществляется в процессе проведения практических занятий и лабораторных работ, обеспечивает оценивание хода освоения модуля.

Формы текущего контроля успеваемости: тестирование, устный опрос, доклады, выполнение практических и лабораторных работ.

№	Наименование темы	Код формируемой компетенции	Результаты обучения по профессиональному модулю		Формы контроля
			уметь	знать	
МДК.03.01 Эксплуатация объектов сетевой инфраструктуры.					
1.	Тема 1. Эксплуатация объектов сетевой инфраструктуры.	ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.4 ПК 3.5 ОК.01-ОК.09	– 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. – Выбирать сетевые топологии. – Рассчитывать основные параметры локальной сети. – Применять алгоритмы поиска кратчайшего пути. – Планировать структуру сети с помощью графа с оптимальным расположением узлов. – Использовать	– 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 устройств, термины, понятия, стандарты и типовые элементы структурированной кабельной системы: монтаж, тестирование. – Средства тестирования и анализа. – Базовые протоколы и технологии	Текущий контроль педагога в форме оценки решения задач, защиты лабораторных работ.
2.	Тема 2. Эксплуатация систем IP-телефонии.	ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.4 ПК 3.5 ОК.01-ОК.09			

			математический аппарат теории графов. – Использовать многофункциональные приборы и программные средства мониторинга. – Использовать программно-аппаратные средства технического контроля – Использовать программно-аппаратные средства технического контроля. – 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. – Читать техническую и проектную документацию по организации сегментов сети. – Контролировать соответствие разрабатываемого проекта нормативно-технической документации.	локальных сетей. – 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. – Требования к компьютерным сетям. – Требования к сетевой безопасности. – Элементы теории массового обслуживания. – Основные понятия теории графов. – Основные проблемы синтеза графов атак. – Системы топологического анализа защищенности компьютерной сети. – Архитектуру сканера безопасности. – Требования к компьютерным сетям.	

			– Использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования. – – администрировать локальные вычислительные сети; – принимать меры по устранению возможных сбоев; – обеспечивать защиту при подключении к информационно-телекоммуникационной сети "Интернет".	– 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. – Принципы и стандарты оформления технической документации – Принципы создания и оформления топологии сети. – Информационно-справочные системы для замены (поиска) технического оборудования	
МДК.03.02 Безопасность компьютерных сетей.					
3.	Тема 1. Автоматизированные системы управления технологическими процессами (АСУ ТП)	ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.4 ПК 3.5 ОК.01-ОК.09	– Проектировать локальную сеть. – Выбирать сетевые топологии. – Рассчитывать основные параметры локальной сети. – Применять алгоритмы поиска кратчайшего пути.	– Общие принципы построения сетей. – Сетевые топологии. – Многослойную модель OSI. – Требования к компьютерным сетям. – Архитектуру протоколов.	Текущий контроль педагога в форме оценки решения задач, защиты лабораторных работ. Итоговый контроль в форме экзамена (квалификационного).

4.	Тема 2. Промышленные сетевые технологии и протоколы в АСУ ТП	ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.4 ПК 3.5 ОК.01-ОК.09	– 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. – 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 – Использовать программно-аппаратные средства	– 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. – Общие принципы построения сетей. – Сетевые топологии. – Стандартизацию сетей. – Этапы проектирования сетевой инфраструктуры. – Элементы теории массового обслуживания. – Основные понятия теории графов.	

			технического контроля. – 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. – 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. – – администрировать локальные вычислительные сети; – принимать меры по устранению возможных сбоев; обеспечивать защиту при	– Основные проблемы синтеза графов атак. – Системы топологического анализа защищенности компьютерной сети. – Архитектуру сканера безопасности. – Принципы построения высокоскоростных локальных сетей. – Требования к компьютерным сетям. – Требования к сетевой безопасности. – Элементы теории массового обслуживания. – Основные понятия теории графов. – Основные проблемы синтеза графов атак. – Системы топологического анализа защищенности компьютерной сети. – Архитектуру сканера безопасности. – 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	

			подключении к информационно-телекоммуникационной сети "Интернет".	типовые элементы структурированной кабельной системы: монтаж, тестирование. – Средства тестирования и анализа. – 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	
МДК.03.02 Безопасность сетевой инфраструктуры.					
5.	Безопасность компьютерных сетей	ПК 3.1 ПК 3.2 ПК 3.3 ПК 3.4 ПК 3.5 ОК.01-ОК.09	– 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	– 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	
6.	Обеспечение сетевой безопасности				

			операционной системы для диагностики работоспособности сети. – 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 – Использовать программно-аппаратные средства технического контроля. – Читать техническую и проектную документацию по организации сегментов сети. – Контролировать соответствие разрабатываемого проекта нормативно-технической документации. – Использовать программно-аппаратные средства	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. – 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. – Требования к компьютерным	

			технического контроля. – Использовать техническую литературу и информационно-справочные системы для замены (поиска аналогов) устаревшего оборудования. – 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. – – администрировать локальные вычислительные сети; – принимать меры по устранению возможных сбоев; обеспечивать защиту при подключении к информационно-телекоммуникационной сети "Интернет".	сетям. – Требования к сетевой безопасности. – Элементы теории массового обслуживания. – Основные понятия теории графов. – Основные проблемы синтеза графов атак. – Системы топологического анализа защищенности компьютерной сети. – Архитектуру сканера безопасности. – 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. – Принципы и стандарты оформления технической документации	

				– Принципы создания и оформления топологии сети. – Информационно-справочные системы для замены (поиска) технического оборудования	

Критерии оценивания результатов обучения по профессиональному модулю, шкала оценивания

Критерии оценивания:

- усвоение программного теоретического материала (объем знаний, глубина усвоения);
- умение излагать программный материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания на практике.

Шкала оценивания:

Результаты сдачи дифференцированного зачета, экзамена (квалификационного) оцениваются по шкале «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется обучающемуся, который глубоко и прочно усвоил программный материал, проявляет знание основной и дополнительной литературы, грамотно, логически стройно и аргументировано излагает материал, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с практическими заданиями.

Оценка «хорошо» выставляется обучающемуся, твердо знающему программный материал, который излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, не испытывает затруднений с ответами на вопросы.

Оценка «удовлетворительно» выставляется обучающемуся, который имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, испытывает затруднения при выполнении практических работ.

Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

Дополнения и изменения к рабочей программе на учебный год

Дополнения и изменения к рабочей программе на 2025-2026 учебный год по профессиональному модулю ПМ.03 Эксплуатация объектов сетевой инфраструктуры: в раздел Условия реализации профессионального модуля (пункт Информационное обеспечение профессионального модуля) внесены изменения в список основной и дополнительной литературы.

Дополнения и изменения в рабочей программе обсуждены на заседании ПЦК информационных технологии.

«30» августа 2025г. (протокол № 1)

Председатель ПЦК _____ /Л.И.Логинова/