ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А.БУНИНА

«УТВЕРЖДАЮ»
Директор института СПО
_____ / Гладышева М.С./

РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Эксплуатация объектов сетевой инфраструктуры

09.02.06 Сетевое и системное администрирование

Базовый уровень подготовки

Форма обучения: **очная**

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование», утвержденного приказом Министерства образования и науки Российской Федерации от «10» июля 2023 г. № 519

Место дисциплины в структуре ППССЗ СПО – профессиональный модуль ПМ.03 «Эксплуатация объектов сетевой инфраструктуры».

Рабочая программа разработана ПЦК по технологическому профилю

Разработчик(и) рабочей программы:

Преподаватель института СПО Попов С.Е.

СОДЕРЖАНИЕ

1. **ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

2. **РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

3. **СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ МОДУЛЯ**

4. **УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

5. **КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Эксплуатация объектов сетевой инфраструктуры (по выбору)

1.1. Область применения программы

Рабочая программа профессионального модуля является частью образовательной программы в соответствии с ФГОС по специальности СПО 09.02.06 «Сетевое и системное администрирование».

Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки) и профессиональной подготовке по смежным специальностям.

Шифр профессионального модуля: ПМ.03.

Профессиональный модуль направлен на формирование следующих общих и профессиональных компетенций: ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5.

1.2. Цели и задачи дисциплины – требования к результатам освоения содержания дисциплины

В результате освоения дисциплины обучающийся должен 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
- 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.

В результате освоения дисциплины обучающийся должен 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;
- основные понятия теории графов;
- архитектуру сканера безопасности;
- принципы построения высокоскоростных локальных сетей;
- организацию работ по вводу в эксплуатацию объектов и сегментов компьютерных сетей;
- программно-аппаратные средства технического контроля.

1.3. Рекомендуемое количество часов на освоение программы дисциплины:
максимальной учебной нагрузки обучающегося 444 часа, в том числе:
обязательной аудиторной учебной нагрузки обучающегося - 372 часа;
самостоятельная работа обучающегося – 34 часа;
промежуточная аттестация обучающегося 18 часов;
учебная и производственная практики – 144 часа.

1.4. Формы контроля и оценивания элементов ПМ

Элемент ПМ	**Форма контроля и оценивания**		
	Текущий контроль	**Промежуточная аттестация**	**Экзамен по ПМ**
1	**2**	**3**	**4**
МДК.03.01	Экзамен	да	
МДК.03.02	Дифференцированный зачет	да	
МДК.03.03	Экзамен	да	
УП.03.01	Дифференцированный зачет		
ПП.03.01	Дифференцированный зачет		
ПМ.03.Э			да

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности ПМ.03 Эксплуатация объектов сетевой инфраструктуры, в том числе профессиональными (ПК) компетенциями:

Код	Наименование видов деятельности и профессиональных компетенций
ПК 3.1.	Осуществлять проектирование сетевой инфраструктуры.
ПК 3.2.	Обслуживать сетевые конфигурации программно-аппаратных средств.
ПК 3.3.	Осуществлять защиту информации в сети с использованием программно-аппаратных средств.
ПК 3.4.	Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры.
ПК 3.5.	Модернизировать сетевые устройства информационно-коммуникационных систем.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
3.1. Тематический план профессионального модуля ПМ.03

Коды профессиональных компетенций	**Наименования разделов профессионального модуля***	**Всего часов** *(макс. учебная нагрузка и практики)*	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**	
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося**		**Учебная,** часов	**Производственная (по профилю специальности),** часов *(если предусмотрена рассредоточенная практика)*
			Всего, часов	**в т.ч. лабораторные работы и практические занятия,** часов	**в т.ч., курсовая работа (проект),** часов	**Всего,** часов	**в т.ч., курсовая работа (проект),** часов		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
ПК.3.1-3.5	**Раздел 1. Эксплуатация объектов сетевой инфраструктуры**	**208**	**132**	46		**67**			
ПК.3.1-3.5	**Раздел 2. Технологии автоматизации технологических процессов**	**61**	**40**	22		**21**			
ПК.3.1-3.5	**Раздел 3. Безопасность сетевой инфраструктуры**	**190**	**132**	46		**49**	**12**		

ПК.3.1-3.5	**ПМ.03.ЭК Экзамен по модулю**	**9**							
УП.03.01	**Учебная практика**	**72**				**12**		**72**	
ПП.03.01	**Производственная практика (по профилю специальности)**, часов *(если предусмотрена итоговая (концентрированная) практика)*	**144**							**144**
	Всего:	**684**	**228**	**114**		**149**		**72**	**144**

Ячейки в столбцах 3,4,7,9,10 заполняются жирным шрифтом, в 5,6,8 – обычным. Если какой-либо вид учебной работы не предусмотрен, необходимо в соответствующей ячейке поставить прочерк. Количество часов, указанное в ячейках столбца 3, должно быть равно сумме чисел в соответствующих ячейках столбцов 4,7,9,10 (жирный шрифт) по горизонтали. Количество часов, указанное в ячейках строки «Всего», должно быть равно сумме числе соответствующих столбцов 3,4,5,6,7,8,9,10 по вертикали. Количество часов, указанное ячейке столбца 3 строки «Всего», должно соответствовать количеству часов на освоение программы ПМ в пункте1.3 паспорта программы. Количество часов на самостоятельную работу обучающегося должно соответствовать указанному в п.1.3. паспорта программы. Сумма количества часов на учебную и производственную практики (в строке «Всего» в столбцах 9 и 10) должна соответствовать указанному в п.1.3 паспорта программы.

3.2. Содержание обучения по профессиональному модулю ПМ.03.

Наименование разделов и тем	Примерное содержание учебного материала, практических и лабораторных занятия, *курсовой проект (работа)*	Объём часов	Уровень освоения
1	**2**	**3**	**4**
Раздел 1. Эксплуатация сетевой инфраструктуры 208 час.			
МДК.03.01. Эксплуатация сетевой инфраструктуры			
Тема 1.1 Эксплуатация объектов сетевой инфраструктуры	**Содержание**		
	1. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.	4	2,3
	2. Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб).	4	2,3
	3. Наращивание длины сегментов сети Замена существующей аппаратуры. Увеличение количества узлов сети; увеличение протяженности связей между объектами сети	4	2,3
	4. Физическая карта всей сети Логическая топология компьютерной сети. Техническая и проектная документация. Паспорт технических устройств.	4	2,3
	5. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры. Проверка объектов сетевой инфраструктуры и профилактические работы.	4	2,3
	6. Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.	4	2,3
	7. Программное обеспечение мониторинга компьютерных сетей и сетевых устройств. Анализ функциональных особенностей программного обеспечения мониторинга, определение методов и алгоритмов, используемых в процессе мониторинга, изучение основных принципов выбора программного обеспечения мониторинга для конкретной сети или устройства на основе учета их параметров и особенностей работы, анализ	4	2,3

	возможностей современного программного обеспечения мониторинга и определение эффективных подходов к использованию этих возможностей в практических задачах мониторинга компьютерных сетей и сетевых устройств.		
	8. Протокол SNMP, его характеристики, формат сообщений, набор услуг. Анализ основных характеристик протокола SNMP, его структуры и архитектуры, формата сообщений и спецификации синтаксиса	4	2,3
	9. Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.	2	2,3
	В том числе практических занятий и лабораторных работ		
	Практическое занятие 1. Оконцовка кабеля витая пара	2	2,3
	Практическое занятие 2. Заделка кабеля витая пара в розетку	2	2,3
	Практическое занятие 3. Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену	2	2,3
	Практическое занятие 4. Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы)	2	2,3
	Практическое занятие 5. Выполнение действий по устранению неисправностей. Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.	4	2,3
	Практическое занятие 6. Оформление технической документации, правила оформления документов	4	2,3
	Практическое занятие 7. Протокол управления SNMP. Основные характеристики протокола SNMP. Набор услуг (PDU) протокола SNMP. Формат сообщений SNMP.	4	2,3
	Практическое занятие 8.Задачи управления: анализ производительности сети, анализ надежности сети	4	2,3
	Практическое занятие 9. Управление безопасностью в сети. Учет трафика в сети	4	2,3
	Практическое занятие 10. Средства мониторинга компьютерных сетей. Средства анализа сети с помощью команд сетевой операционной системы	4	2,3
Тема 1.2 Эксплуатация систем IP-телефонии	**Содержание**		2,3
	1. Настройка H.323. Описание H.323 и общие рекомендации. Функциональные компоненты H.323.Установка и	2	2,3

	поддержка соединения H.323. Соединения без и с использованием GateKeeper. Соединения с использованием нескольких GateKeeper. Многопользовательские конференции. Обеспечение отказоустойчивости.		
	2. Настройка SIP. Описание и общие рекомендации. Технология SIP и связанные с ней стандарты. Функциональные компоненты SIP. Сообщения SIP. Адресация SIP. Модель установления соединения. Планирование отказоустойчивости.	2	2,3
	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	2,3
	4. Управление программным коммутатором. Маршрутизация. Группы соединительных линий. Подключение станций с TDM (абонентский доступ TDM). Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP -абоненты. Группы абонентов. Дополнительные абонентские услуги.	2	2,3
	5. Организация эксплуатации систем IP-телефонии. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт	2	2,3
	6. Восстановление работы сети после аварии. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы рабоы хранилищ данных;	2	2,3
	В том числе практических занятий и лабораторных работ		2,3
	Практическое занятие 1. Настройка аппаратных и программных IP-телефонов, факсов	2	2,3
	Практическое занятие 2. Развертывание сети с использованием VLAN для IP-телефонии. Настройка шлюза	2	2,3
	Практическое занятие 3. Установка, подключение и первоначальные настройки голосового маршрутизатора. Настройка таблицы пользователей, настройка групп, настройка голосовых сообщений в голосовом маршрутизаторе.	2	2,3
	Практическое занятие 4. Настройка программно-аппаратной IP-АТС. Установка и настройка программной IP-АТС (например, Asterisk).	2	2,3

	Практическое занятие 5. Мониторинг и анализ соединений по различным протоколам. Мониторинг вызовов в программном коммутаторе	2	2,3
	Практическое занятие 6. Создание резервных копий баз данных	2	2,3
	Практическое занятие 7. Диагностика и устранение неисправностей в системах IP-телефонии	2	2,3
Раздел 2. Технологии автоматизации технологических процессов 61 час			
МДК.03.02. Технологии автоматизации технологических процессов			
Тема 2.1. Автоматизированные системы управления технологическими процессами (АСУ ТП)	**Содержание**		
	1. Понятие об объекте управления. Свойства объекта управления.	1	2,3
	2. Классификация технологических объектов управления по типу, характеру технологического процесса, по характеристике параметров управления		2,3
	3. Классификация систем управления технологическими объектами по способу, цели и степени централизации управления.	1	2,3
	4. Общие сведения об автоматизированных системах управления технологическими процессами (АСУТП) и системах автоматического управления (САУ)		2,3
	5. Основные функции АСУТП и САУ. Техническое, программное и информационное обеспечение АСУТП	1	2,3
	6. Структура АСУТП на базе микропроцессорной техники.		2,3
	7. Средства измерения преобразования и регулирования в АСУТП	1	2,3
	8. Основные понятия автоматизированной обработки информации		2,3
	9. Методы и средства моделирования технологических процессов в АСУТП	1	2,3
	10. Обзор современных технологий и тенденций развития АСУТП		2,3
	11. Программирование и настройка АСУТП: языки программирования, методы и инструменты	1	2,3
	12. Интеграция АСУТП с другими системами и оборудованием в производственном процессе		2,3
	13. Оценка эффективности и экономическая оценка внедрения АСУТП	1	2,3
	14. Особенности управления производственными системами в условиях		2,3

	неопределенности и переменных условий работы		
	15. Применение систем искусственного интеллекта в АСУТП: нейронные сети, генетические алгоритмы, экспертные системы		2,3
	В том числе практических занятий и лабораторных работ		
	Практическое занятие 1. Определение свойств объектов управления на практике	1	2,3
	Практическое занятие 2. Классификация технологических объектов управления на примере производственного предприятия	1	2,3
	Практическое занятие 3. Анализ и сравнение систем управления технологическими объектами на примере различных отраслей промышленности	1	2,3
	Практическое занятие 4. Изучение принципов работы АСУТП и САУ на примере реальных систем управления	1	2,3
	Практическое занятие 5. Создание простой модели технологического процесса	1	2,3
	Практическое занятие 6. Ознакомление с современными технологиями АСУТП на примере существующих проектов и исследований	1	2,3
	Практическое занятие 7. Программирование элементов АСУТП на языках программирования на практике	1	2,3
	Практическое занятие 8. Настройка и проверка работоспособности элементов АСУТП на примере конкретной системы управления	1	2,3
	Практическое занятие 9. Интеграция АСУТП с другими системами и оборудованием в производственном процессе	1	2,3
	Практическое занятие 10. Оценка эффективности и экономическая оценка внедрения АСУТП	1	2,3
	Практическое занятие 11. Разработка системы управления производственными процессами в условиях неопределенности и переменных условий работы	1	2,3
	Практическое занятие 12. Применение нейронных сетей в системах управления технологическими процессами	1	2,3
	Практическое занятие 13. Применение экспертных систем в системах управления технологическими процессами	1	2,3
	Практическое занятие 14. Создание проекта автоматизации управления технологическим процессом на основе АСУТП	1	2,3

Тема 2.2. Промышленные сетевые технологии и протоколы в АСУ ТП	**Содержание**		
	1. Роль и место сетевых технологий в промышленной автоматизации Обзор сетевых технологий, их роль в промышленной автоматизации, а также их преимущества и недостатки. Основные типы промышленных сетей, их характеристики и особенности, а также методы их реализации. Протоколы связи, используемые в промышленной автоматизации, их особенности и применение.	1	2,3
	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
	3. Протокол MODBUS Описание основных характеристик и принципов работы промышленного протокола связи MODBUS, включая формат кадра, адресацию, коды функций, методы передачи данных и возможности расширения. Также рассматриваются типовые применения и устройства, работающие по протоколу MODBUS.	1	2,3
	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.		2,3
	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.		2,3
	6. Выравнивание адресов переменных в поле памяти протокола Принципы работы с адресацией переменных в протоколе MODBUS. Основные требования к адресации и выравниванию данных в поле памяти протокола, а также способы решения возникающих проблем. Типовые ошибки при работе с адресацией и их предотвращение.	1	2,3
	7. Работа контроллера (master) в сети с модулями ввода/вывода (slave) Основные принципы взаимодействия контроллера и устройств ввода-вывода посредством сетевых протоколов. Протоколы MODBUS RTU и MODBUS TCP, их особенности и правила использования при работе контроллера как в режиме master, так и в режиме slave.	1	2,3

	Порядок настройки параметров соединения и обмена данными между контроллером и устройствами ввода-вывода, анализируются возможные проблемы при работе в сети и способы их устранения.		
	8. Работа в сети по протоколу MODBUS RTU с различными устройствами Основные аспекты протокола MODBUS RTU, включая формат кадра, адресацию, функции, а также изучение работы различных устройств (контроллеров и модулей ввода-вывода) в сети, используя этот протокол. Настройка и конфигурация устройств, анализ протокола обмена и методы диагностики проблем, возникающих в работе сети MODBUS RTU.	1	2,3
	9. Работа в сети по протоколу MODBUS TCP Основы протокола MODBUS TCP, включая форматы сообщений, структуру транзакций, способы обмена данными между устройствами, а также настройку и конфигурацию сети MODBUS TCP и ее устройств. Современные технологии и инструменты для мониторинга и управления сетью MODBUS TCP, такие как SCADA-системы и ПО для сетевого анализа.	1	2,3
	10. Типовые промышленные проводные и кабельные сетевые протоколы Различные сетевые протоколы, используемые в промышленных сетях для обмена данными между устройствами автоматизации и управления технологическими процессами (протоколы, PROFIBUS, CAN, Ethernet/IP, DeviceNet, Modbus, Foundation Fieldbus, AS-i и другие). Особенности и принципы работы каждого протокола, его преимущества и недостатки, а также способы настройки и конфигурирования сетей с использованием этих протоколов.	1	2,3
	11. Беспроводные локальные сети для промышленного применения Технологии беспроводной связи, используемых в промышленности, таких как Wi-Fi, Bluetooth, Zigbee, LoRa, NB-IoT и др. Особенности использования беспроводных сетей в промышленном окружении, такие как требования к надежности и безопасности, особенности развертывания и конфигурирования, а также методы мониторинга и управления беспроводными сетями.	1	2,3
	12. Специализированные сетевые интерфейсы для умного дома Различные протоколы и технологии, используемые в системах умного дома (ZigBee, Z-Wave, Thread, Bluetooth, Wi-Fi и другие). Особенности их применения в системах автоматизации умного дома. Аспекты безопасности и защиты данных в системах умного дома, возможности интеграции различных устройств и систем в одну сеть.	1	2,3
	13. Преобразователи интерфейсов Преобразователи интерфейсов для различных стандартов связи (RS-232, RS-485, Ethernet,	1	2,3

	USB). Выбор и настройка преобразователей интерфейсов в соответствии с требованиями конкретной задачи.		
	14. Современные тенденции развития сетевых технологий в АСУ ТП – web-серверы и облачные решения Подходы к организации сетевых технологий в автоматизированных системах управления технологическими процессами, основанных на использовании web-серверов и облачных решений. Основные принципы построения web-серверов и их взаимодействия с устройствами АСУ ТП, возможности использования облачных решений для удаленного мониторинга и управления технологическими процессами.	1	2,3
	15. Конфигурирование и настройка сетевых устройств для автоматизации технологических процессов Процесс настройки и конфигурирования сетевых устройств для автоматизации технологических процессов в промышленности: изучение различных протоколов связи, настройка устройств на работу в сети, а также определение настроек безопасности и мониторинга сетевой активности.	1	2,3
	16. Особенности применения промышленных сетевых протоколов в условиях высоких нагрузок и плохой связи Проблемы, возникающие при передаче данных в промышленных сетях в условиях высоких нагрузок и плохой связи. Изучение методов решения этих проблем с использованием специализированных промышленных сетевых протоколов. Методы оптимизации пропускной способности сетей и уменьшения задержек передачи данных.	1	2,3
	17. Сравнительный анализ промышленных Ethernet-технологий: EtherNet/IP, PROFINET, Modbus TCP Обзор и анализ особенностей трех промышленных Ethernet-протоколов: EtherNet/IP, PROFINET и Modbus TCP. Различия между этими протоколами, их преимущества и недостатки, области применения в промышленных сетях и АСУ ТП.	1	2,3
	18. Применение промышленных маршрутизаторов для обеспечения безопасности и надежности работы сетевой инфраструктуры. Роль промышленных маршрутизаторов в обеспечении безопасности и надежности работы сетевой инфраструктуры в промышленной среде. Основные функции промышленных маршрутизаторов (виртуальная частная сеть (VPN), брандмауэр, NAT-трансляция), их конфигурация и настройка. Методы защиты от внешних атак и обеспечения надежности работы сетевой инфраструктуры.	1	2,3

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

	Практическое занятие 17. Применение промышленных маршрутизаторов для обеспечения безопасности и надежности работы сетевой инфраструктуры		2,3
	Практическое занятие 18. Практическое использование промышленных маршрутизаторов		2,3
	Практическое занятие 19. Организация удаленного доступа к сетевым устройствам в промышленной сети	1	2,3
	Практическое занятие 20. Разработка и тестирование собственного промышленного протокола для обмена данными между устройствами в сети		2,3
	Практическое занятие 21. Организация кластера промышленных компьютеров для выполнения высокопроизводительных вычислений в АСУ ТП		2,3
Раздел 3. Безопасность сетевой инфраструктуры 190 часов			
МДКн.03.03. Безопасность сетевой инфраструктуры			
Тема 3.1. Безопасность компьютерных сетей	**Содержание**		
	1. **Фундаментальные принципы безопасной сети** Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.	1	2,3
	2. **Безопасность сетевых устройств OSI** Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.	1	2,3
	3. **Авторизация, аутентификация и учет доступа (AAA)** Свойства AAA. Локальная AAA аутентификация. Server-based AAA	1	2,3
	4. **Реализация технологий брандмауэра ACL.** Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах.	1	2,3
	5. **Реализация технологий предотвращения вторжения** IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS	1	2,3
	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	1	2,3
	7. **Криптографические системы** Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей	1	2,3

	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	1	2,3
	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.	1	2,3
	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.	1	2,3
	11. Межсетевая безопасность Методы обеспечения безопасности взаимодействия между различными сетями. Реализация технологий маршрутизации и шлюзов, использование межсетевых экранов, технологии виртуальных локальных сетей.	1	2,3
	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.	1	2,3
	13. Защита от социальной инженерии Методы социальной инженерии, опасности, связанные с подделкой и манипулированием данными, а также методы защиты и обучения персонала.	1	2,3
	В том числе практических занятий и лабораторных работ		
	Практическое занятие 1. Социальная инженерия	1	2,3
	Практическое занятие 2. Исследование сетевых атак и инструментов проверки защиты сети	1	2,3
	Практическое занятие 3. Настройка безопасного доступа к маршрутизатору	1	2,3

	Практическое занятие 4. Обеспечение административного доступа AAA и сервера Radius	1	2,3
	Практическое занятие 5. Настройка политики безопасности брандмауэров	1	2,3
	Практическое занятие 6. Настройка системы предотвращения вторжений (IPS)	1	2,3
	Практическое занятие 7. Настройка безопасности на втором уровне на коммутаторах	2	2,3
	Практическое занятие 8. Исследование методов шифрования	1	2,3
	Практическое занятие 9. Настройка Site-to-SiteVPN используя интерфейс командной строки	2	2,3
	Практическое занятие 10. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки	2	2,3
	Практическое занятие 11. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM	2	2,3
	Практическое занятие 12. Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM	2	2,3
	Практическое занятие 13. НастройкаClientless Remote Access SSL VPNs используя ASDM	1	2,3
	Практическое занятие 14. Настройка AnyConnect Remote Access SSL VPN используя ASDM	1	2,3
	Практическое занятие 15. Комплексная лабораторная работа по безопасности	1	2,3
Тема 3.2. Обеспечение сетевой безопасности	**Содержание**		
	1. Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть.	1	2,3
	2. Механизмы шифрования и аутентификации для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам и сервисам.	1	2,3
	3. Использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.	1	2,3
	4. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети.	1	2,3
	5. Методы минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.	1	2,3

	6. Введение системы обнаружения и предотвращения сетевых вторжений.	1	2,3
	7. Технологии использования виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа.	1	2,3
	8. Использование системы управления доступом для контроля доступа к корпоративной сети.	1	2,3
	9. Обеспечение безопасности Wi-Fi-сетей.	1	2,3
	10. Реализация мер по обеспечению безопасности электронной почты в корпоративной сети.	1	2,3
	11. Защита от атак типа "фишинг".	1	2,3
	12. Применение антивирусного программного обеспечения для защиты от вирусов и других вредоносных программ.	1	2,3
	13. Использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.	1	2,3
	14. Защита от DDoS-атак.	1	2,3
	15. Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети.	1	2,3
	16. Защита от внутренних угроз безопасности.	1	2,3
	17. Обеспечение безопасности облачных сервисов.	1	2,3
	18. Организация мониторинга сетевой безопасности и аудита.	1	2,3
	19. Введение системы контроля целостности файлов для защиты от изменения или внедрения вредоносных программ в файловые системы.	1	2,3
	20. Применение методов шифрования данных для защиты от несанкционированного доступа к конфиденциальной информации.	2	2,3
	В том числе практических занятий и лабораторных работ		
	Практическое занятие 1. Настройка VPN-туннелей для организации защищенных каналов передачи данных между территориально распределенными офисами.	2	2,3
	Практическое занятие 2. Работа с механизмами шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.	2	2,3

	Практическое занятие 3. Настройка и использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.	2	2,3
	Практическое занятие 4. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети с использованием программного обеспечения для мониторинга и обнаружения угроз.	2	2,3
	Практическое занятие 5. Разработка и внедрение мер по минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.	1	2,3
	Практическое занятие 6. Настройка и работа с системами обнаружения и предотвращения сетевых вторжений для раннего обнаружения и предотвращения угроз безопасности.	1	2,3
	Практическое занятие 7. Настройка и использование виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.	2	2,3
	Практическое занятие 8. Настройка и работа с системами управления доступом для контроля доступа к корпоративной сети.	1	2,3
	Практическое занятие 9. Обеспечение безопасности Wi-Fi-сетей: настройка безопасных точек доступа, использование сетевой аутентификации, шифрования трафика и других методов.	1	2,3
	Практическое занятие 10. Разработка и внедрение мер по обеспечению безопасности электронной почты в корпоративной сети: настройка антивирусного программного обеспечения, проверка на наличие вредоносных вложений, обучение пользователей основам безопасности электронной почты.	1	2,3
	Практическое занятие 11. Обучение пользователям основам защиты от атак типа "фишинг".	1	2,3
	Практическое занятие 12. Работа с антивирусным программным обеспечением для защиты от вирусов и других вредоносных программ: установка, настройка, обновление базы данных, сканирование и удаление вредоносных программ.	1	2,3
	Практическое занятие 13. Настройка и использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.	1	2,3
	Практическое занятие 14. Настройка и использование межсетевых экранов и фаерволов для обеспечения комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.	2	2,3
	Практическое занятие 15. Внедрение системы управления доступом для контроля доступа к	1	2,3

	корпоративной сети: настройка правил доступа, аутентификация пользователей, управление привилегиями.		
	Практическое занятие 16. Использование технологий виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа: настройка и управление VPN-туннелями, защита данных, маршрутизация трафика.	1	2,3
	Практическое занятие 17. Обеспечение безопасности Wi-Fi-сетей: настройка и управление беспроводными точками доступа, защита сетевого трафика, аутентификация пользователей.	1	2,3
	Практическое занятие 18. Защита от DDoS-атак: использование специализированных средств защиты от DDoS-атак, настройка маршрутизации трафика, мониторинг сетевой активности.	1	2,3
	Практическое занятие 19. Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети: настройка политик безопасности для мобильных устройств, управление устройствами и приложениями, защита данных на устройствах.	1	2,3
	Практическое занятие 20. Обеспечение безопасности облачных сервисов: выбор надежных провайдеров облачных сервисов, настройка правил доступа и аутентификации, шифрование данных, мониторинг активности в облачных сервисах.	2	2,3
Курсовой проект (работа) (12 час.)			
Учебная практика (72 часа) **Виды работ** 1. Настройка прав доступа. 2. Оформление технической документации, правила оформления документов. 3. Настройка аппаратного и программного обеспечения сети. 4. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain. 5. Программная диагностика неисправностей. 6. Аппаратная диагностика неисправностей. 7. Поиск неисправностей технических средств. 8. Выполнение действий по устранению неисправностей. 9. Использование активного, пассивного оборудования сети. 10. Устранение паразитирующей нагрузки в сети. 11. Построение физической карты локальной сети.Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети. 12. Организация защищенных каналов передачи данных для объединения территориально распределенных		**72**	2,3

офисов в одну сеть 13. Обеспечение безопасности Wi-Fi-сетей. 14. Реализация мер по обеспечению безопасности электронной почты в корпоративной сети. 15. Защита от атак типа "фишинг". 16. Обеспечение сетевой безопасности		
Производственная практика (72 часа) **Виды работ** 1. Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение. 2. Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях. 3. Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций. 4. Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли. 5. Установка прав доступа и контроль использования сетевых ресурсов. 6. Обеспечение своевременного копирования, архивирования и резервирования данных. 7. Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования. 8. Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению. Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети. 9. Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия. 10. Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций. 11. Документирование всех произведенных действий.	**144**	2,3
Промежуточная аттестация	**18**	
Всего: 684 часа		

Внутри каждого раздела указываются соответствующие темы. По каждой теме описывается содержание учебного материала (в дидактических единицах),наименования необходимых лабораторных работ и практических занятий (отдельно по каждому виду),

*контрольных работ, а также примерная тематика самостоятельной работы. Если предусмотрены курсовые работы (проекты) по дисциплине, описывается примерная тематика. Объем часов определяется по каждой позиции столбца 3 (отмечено звездочкой *). Уровень освоения проставляется напротив дидактических единиц в столбце 4 (отмечено двумя звездочками **).*

Для характеристики уровня освоения учебного материала используются следующие обозначения:

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

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требуется наличия лаборатории организации и принципов построения компьютерных систем

Оборудование:

Комплект учебной мебели (16 посадочных мест)
Персональный компьютер обучающегося (13 шт.)
Персональный компьютер преподавателя (1 шт.)
Экран для проектора напольный Projecta (ширина 160 см)
Мультимедийный проектор Epson EB-X8
Сетевое оборудование:
коммутатор D-Link DES-1228 24 порта, коммутатор COMPEX DS2216 16 портов,
шлюз IP-телефонии Cisco SPA8000 8 портов,
6 медиаконвертеров D-Link DMC-920R

Лицензионное программное обеспечение:

Microsoft Windows 7
(14 лицензий WinPro 7 RUS Upgrd OLP NL Acdmc
Торговый посредник: Softline Дата заказа: 2010-10-27
Код лицензии: 47592665 Родительская программа: OPEN 67582704ZZE1210)
Microsoft Office 2007 Professional
(9 лицензий OfficeProPlus 2007 RUS OLP NL Acdmc
Торговый посредник: ООО Рэдком Дата заказа: 2007-12-04
Лицензия: 43136305 Родительская программа: OPEN 63126856ZZE0912;
5 лицензий OfficeProPlus 2007 RUS OLP NL Acdmc
Торговый посредник: ООО Рэдком Дата заказа: 2008-09-19
Код Лицензии: 44544996 Родительская программа: OPEN 63786020ZZE1004)
Kaspersky Endpoint Security 11 для Windows
(Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 250-499 Node 2 year Educational Renewal License
№ лицензии: 1096-181214-111355-563-621
Срок использования ПО: с 2018-12-14 до 2021-03-02
Поставщик (реселлер): BENEF.IT Бенефит, ООО)
АСКОН КОМПАС-3D V12 Университетская лицензия с библиотеками и приложениями
(Лицензионное соглашение Кк-10-01408 от 03.12.2010 г. Кол-во копий: 50
Ключ аппаратной защиты HASP HL Net 50 v2 ID 1579998279)

Свободное программное обеспечение:

Libre Office 5.4
Oracle VM VirtualBox
Microsoft Visual C++ 2008 Express Edition
Microsoft Visual C# 2008 Express Edition
Microsoft Visual Basic 2008 Express Edition
Python 3.4
Maxima 5.3.7
Pascal ABC.NET

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры: учебник / А.В. Назаров, А.Н. Енгалычев, В.П. Мельников. — Москва: КУРС: ИНФРА-М, 2023. — 360 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-06-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/1999922.
2. 2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие/ В.Ф. Шаньгин. – М.: ИД «ФОРУМ» - ИНФРА-М, 2023. – 416 с.
3. Ковган, Н.М. Компьютерные сети : учебное пособие : [16+] / Н.М. Ковган. – Минск : РИПО, 2023. – 180 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book_view_red&book_id=599948 (дата обращения: 16.05.2024). – Библиогр. в кн. – ISBN 978-985-503-947-2. – Текст : электронный.
4. Максимов, Н. В. Компьютерные сети : учебное пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2024. — 464 с. – Текст: непосредственный.
5. Сергеев А.Н. Основы локальных компьютерных сетей: учебное пособие. СПО. – Москва: Лань, 2024. – 184 с. – Текст: непосредственный.

Дополнительные источники:

1. Куль, Т. П. Операционные системы. Программное обеспечение учебник для СПО / Т. П. Куль. — 3-е изд., стер. — Санкт-Петербург: Лань, 2023. — 248 с. — ISBN 978-5-507-46005 Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/2929943.
2. Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2020. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/viewer/kompyuternye-seti-i-telekommunikacii-marshrutizaciya-v-ip-setyah-v-2-ch-chast-1-452574#page/1 (дата обращения: 16.05.2024).
3. Сети и телекоммуникации : учебник и практикум для вузов / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2020. — 363 с. — (Высшее образование). — ISBN 978-5-534-00949-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/viewer/seti-i-telekommunikacii-450234#page/1 (дата обращения: 16.05.2024).

Программное обеспечение и Интернет-ресурсы:

1. ЭБС «Университетская библиотека онлайн». – Режим доступа: http://biblioclub.ru.
2. Образовательный портал. Режим доступа: Intuit.ru.
3. ЭБС IPRBooks/ - Режим доступа: http://www.iprbookshop.ru/

4.3. Общие требования к организации образовательного процесса

Профессиональный модуль изучается параллельно с изучением учебных дисциплин общепрофессионального цикла: «Основы программирования и баз данных», «Электротехнические основы источников питания».

Выполнение практических занятий предполагает деление группы по числу рабочих мест, оборудованных персональным компьютером. Текущий контроль освоения содержания МДК осуществляется в форме тестовых заданий и практических занятий.

Учебная практика по модулю проходит изучения теоретической части МДК.

Учебная практика проводится в компьютерных лабораториях ЕГУ им.И.А. Бунина.

Производственная практика проходит в организациях города. Обязательным условием допуска к производственной практике в рамках ПМ является освоение учебной практики для получения первичных профессиональных навыков.

В процессе обучения используются различные виды информационно-коммуникационных технологий.

4.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарному курсу (курсам): наличие среднего специального или высшего инженерного или высшего педагогического образования, соответствующего профилю.

Требования к квалификации педагогических кадров, осуществляющих руководство практикой: высшее педагогическое образование, соответствующего профилю модуля «Эксплуатация объектов сетевой инфраструктуры» и специальности «Компьютерные сети».

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	**Коды формируемых профессиональных и общих компетенций**	**Формы и методы контроля и оценки результатов обучения**
ПК 3.1. Осуществлять проектирование сетевой инфраструктуры. ПК 3.2. Обслуживать сетевые конфигурации программно-аппаратных средств. ПК 3.3. Осуществлять защиту информации в сети с использованием программно-аппаратных средств. ПК 3.4. Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры. ПК 3.5. Модернизировать сетевые устройства информационно-коммуникационных систем.	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	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Защита отчетов по практическим и лабораторным работам Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

	со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.	