

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ХАБАРОВСКОГО КРАЯ
КРАЕВОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ХАБАРОВСКИЙ ТЕХНИКУМ ТЕХНОСФЕРНОЙ БЕЗОПАСНОСТИ И
ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ»

СОГЛАСОВАНО
Работодатель
Директор ООО «ПРОФИТ ДВ»,
г. Хабаровск
Сёмин С. А.
« 04 » _____ 202_ г



**РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ**

Форма обучения

очная

09.02.06 «Сетевое и системное администрирование»

г. Хабаровск

2024 г.

Программа учебной дисциплины разработана на основе Федерального

государственного образовательного стандарта (далее – ФГОС) **на базе основного общего образования** по специальности среднего профессионального образования (далее СПО 09.02.06 «Сетевое и системное администрирование»

Организация-разработчик: КГБОУ «Хабаровский техникум техносферной безопасности и промышленных технологий»

Разработчики: Верховина Т.А. преподаватель спец дисциплин

Рассмотрено и одобрено на заседании ПЦК «Информатика и вычислительная техника»

Протокол №__от «__»_____20_____г.

Председатель ПЦК_____ (Верховина Т.А.).

Согласовано на заседании методического совета

Протокол № _____ от «__»_____ 202__ г

Председатель МС _____ (_Линевич О. Г.)

СОДЕРЖАНИЕ

- 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
«ПМ.03 Эксплуатация объектов сетевой инфраструктуры»**

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающихся должен освоить основной вид деятельности Эксплуатация объектов сетевой инфраструктуры и соответствующие ему общие компетенции, и профессиональные компетенции:

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
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

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	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

1.1.3 личные результаты

Личностные результаты реализации программы воспитания (дескрипторы)	Код личностных результатов реализации Программы воспитания
Портрет выпускника ПОО	
Осознающий себя гражданином и защитником великой страны	ЛР 1
Готовый использовать свой личный и профессиональный потенциал для защиты национальных интересов России	ЛР 2
Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России	ЛР 3
Принимающий семейные ценности своего народа, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания	ЛР 4
Занимающий активную гражданскую позицию избирателя, волонтера, общественного деятеля	ЛР 5
Принимающий цели и задачи научно-технологического, экономического, информационного развития России, готовый работать на их достижение	ЛР 6
Готовый соответствовать ожиданиям работодателей: проектно мыслящий, эффективно взаимодействующий с членами команды и сотрудничающий с другими людьми, осознанно выполняющий профессиональные требования, ответственный, пунктуальный, дисциплинированный, трудолюбивый, критически мыслящий, нацеленный на достижение поставленных целей; демонстрирующий профессиональную жизнестойкость	ЛР 7
Признающий ценность непрерывного образования, ориентирующийся в изменяющемся рынке труда, избегающий безработицы; управляющий собственным профессиональным развитием; рефлексивно оценивающий собственный жизненный опыт, критерии личной успешности	ЛР 8
Уважающий этнокультурные, религиозные права человека, в том числе с особенностями развития; ценящий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности»	ЛР 9

Принимающий активное участие в социально значимых мероприятиях, соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России; готовый оказать поддержку нуждающимся	ЛР 10
Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением	ЛР 11
Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих	ЛР 12
Способный в цифровой среде использовать различные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей; стремящийся к формированию в сетевой среде лично и профессионального конструктивного «цифрового следа»	ЛР 13
Способный ставить перед собой цели под возникающие жизненные задачи, подбирать способы решения и средства развития, в том числе с использованием цифровых средств; содействующий поддержанию престижа своей профессии и образовательной организации	ЛР 14
Способный генерировать новые идеи для решения задач цифровой экономики, перестраивать сложившиеся способы решения задач, выдвигать альтернативные варианты действий с целью выработки новых оптимальных алгоритмов; позиционирующий себя в сети как результативный и привлекательный участник трудовых отношений.	ЛР 15
Способный искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств; предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве.	ЛР 16
Гибко реагирующий на появление новых форм трудовой деятельности, готовый к их освоению	ЛР 17
Осознающий значимость системного познания мира, критического осмысления накопленного опыта	ЛР 18
Развивающий творческие способности, способный креативно мыслить	ЛР 19
Способный в цифровой среде проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающей информации	ЛР 20
Готовый к профессиональной конкуренции и конструктивной реакции на критику	ЛР 21
Демонстрирующий приверженность принципам честности, порядочности, открытости	ЛР 22
Самостоятельный и ответственный в принятии решений во всех сферах своей деятельности, готовый к исполнению разнообразных социальных ролей, востребованных бизнесом, обществом и государством	ЛР 23
Проявляющий эмпатию, выражающий активную гражданскую позицию, участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций, а также некоммерческих организаций, заинтересованных в развитии гражданского общества и оказывающих поддержку нуждающимся	ЛР 24
Препятствующий действиям, направленным на ущемление прав или унижение достоинства (в отношении себя или других людей)	ЛР 25

1.1.4. В результате освоения профессионального модуля обучающийся должен:

<p>Владеть навыками</p>	<ul style="list-style-type: none"> – 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
<p>Уметь</p>	<ul style="list-style-type: none"> – 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.

	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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.

	<ul style="list-style-type: none"> - 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
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов 700,

в том числе в форме практической подготовки 196 часов

Из них на освоение МДК 442 часа

в том числе самостоятельная работа 0 часов

практики, в том числе учебная 144 часов

производственная 108 часов

Экзамен по модулю 6 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Объем профессионального модуля, ак. час.							
				Всего	Обучение по МДК				Практики		
					В том числе				Учебная	Производственная	
					Лабораторных и практических занятий	Курсовых работ (проектов)	Самостоятельная работа	Промежуточная аттестация			
1	2	3	4	5	6	7	8	9	10	11	
ПК 3.1-3.5 ОК 01-09	Раздел 1. Эксплуатация сетевой инфраструктуры	220	114	218	114	0	0	2			
ПК 3.1-3.5 ОК 01-09	Раздел 2. Технологии автоматизации технологических процессов	106	36	104	36	30	0	2			
ПК 3.1-3.5 ОК 01-09	Раздел 3. Безопасность сетевой инфраструктуры	116	46	116	46	30	0	2			
ПК 3.1-3.5 ОК 01-09	Учебная практика (по профилю специальности)	144							144		
ПК 3.1-3.5 ОК 01-02, ОК 05-07, ОК 09	Производственная практика (по профилю специальности), часов	108									72
	Промежуточная аттестация	6	0					6			
	Всего:	700	196	436	196	60	0	12	144		108

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем, акад. ч / в том числе в форме практической подготовки, акад ч	Уровень освоения	ОК, ПК, ЛР
1	2	3		
Раздел 1. Эксплуатация сетевой инфраструктуры		216/114		
МДКн.03.01. Эксплуатация сетевой инфраструктуры		216/114		
Тема 1.1 Эксплуатация объектов сетевой инфраструктуры	Содержание	64/64		
	1. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.	64	1	ПК 3.1-3.5 ОК 01-09 ЛР
	2. Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб).		1	
	3. Нарращивание длины сегментов сети Замена существующей аппаратуры. Увеличение количества узлов сети; увеличение протяженности связей между объектами сети		1	
	4. Физическая карта всей сети Логическая топология компьютерной сети. Техническая и проектная документация. Паспорт технических устройств.		1	
	5. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры. Проверка объектов сетевой инфраструктуры и профилактические работы.		1	
	6. Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.		1	

<p>7. Программное обеспечение мониторинга компьютерных сетей и сетевых устройств. Анализ функциональных особенностей программного обеспечения мониторинга, определение методов и алгоритмов, используемых в процессе мониторинга, изучение основных принципов выбора программного обеспечения мониторинга для конкретной сети или устройства на основе учета их параметров и особенностей работы, анализ возможностей современного программного обеспечения мониторинга и определение эффективных подходов к использованию этих возможностей в практических задачах мониторинга компьютерных сетей и сетевых устройств.</p>		1	ПК 3.1-3.5 ОК 01-09 ЛР 1-25	
<p>8. Протокол SNMP, его характеристики, формат сообщений, набор услуг. Анализ основных характеристик протокола SNMP, его структуры и архитектуры, формата сообщений и спецификации синтаксиса</p>		1		
<p>9. Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.</p>		1		
<p>В том числе практических занятий и лабораторных работ</p>	64			
<p>Практическое занятие 1. Оконцовка кабеля витая пара</p>	64	2	ПК 3.1-3.5 ОК 01-09 ЛР 1-25	
<p>Практическое занятие 2. Заделка кабеля витая пара в розетку</p>		2		
<p>Практическое занятие 3. Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену</p>		2		
<p>Практическое занятие 4. Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы)</p>		2		
<p>Практическое занятие 5. Выполнение действий по устранению неисправностей. Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.</p>		2		
<p>Практическое занятие 6. Оформление технической документации, правила оформления документов</p>		2		
<p>Практическое занятие 7. Протокол управления SNMP. Основные характеристики протокола SNMP. Набор услуг (PDU) протокола SNMP. Формат сообщений SNMP.</p>		2		
<p>Практическое занятие 8. Задачи управления: анализ производительности сети, анализ надежности сети</p>		2		

	Практическое занятие 9. Управление безопасностью в сети. Учет трафика в сети		2	
	Практическое занятие 10. Средства мониторинга компьютерных сетей. Средства анализа сети с помощью команд сетевой операционной системы		2	
Тема 1.2 Эксплуатация систем IP-телефонии	Содержание	38/50		
	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.	38	1	ПК 3.1-3.5 ОК 01-09 ЛР
	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.		1	
	3. Установка и инсталляция программного коммутатора. Монтажные процедуры. Процедуры инсталляции. Управление аппаратными средствами и портами. Протоколы управления MGCP, H.248. Создание аналоговых абонентов. Внутрисканционная маршрутизация.		1	
	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.		1	
	5. Организация эксплуатации систем IP-телефонии. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт		1	
	6. Восстановление работы сети после аварии. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных;		1	
	В том числе практических занятий и лабораторных работ		50	
	Практическое занятие 1. Настройка аппаратных и программных IP-телефонов, факсов	50	2	

	Практическое занятие 2. Развертывание сети с использованием VLAN для IP-телефонии. Настройка шлюза		2	ПК 3.1-3.5 ОК 01-09 ЛР 1-25
	Практическое занятие 3. Установка, подключение и первоначальные настройки голосового маршрутизатора. Настройка таблицы пользователей, настройка групп, настройка голосовых сообщений в голосовом маршрутизаторе.		2	
	Практическое занятие 4. Настройка программно-аппаратной IP-АТС. Установка и настройка программной IP-АТС (например, Asterisk).		2	
	Практическое занятие 5. Мониторинг и анализ соединений по различным протоколам. Мониторинг вызовов в программном коммутаторе		2	
	Практическое занятие 6. Создание резервных копий баз данных		2	
	Практическое занятие 7. Диагностика и устранение неисправностей в системах IP-телефонии		2	
<p>Примерная тематика самостоятельной учебной работы при изучении раздела 1. Эксплуатация сетевой инфраструктуры</p> <p>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.</p> <p>Тематика домашних заданий, сообщений, рефератов:</p> <ol style="list-style-type: none"> 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.				
Раздел 2. Технологии автоматизации технологических процессов		102/36/30		
МДКн.03.02. Технологии автоматизации технологических процессов		102/36/30		
Тема 2.1. Автоматизированные системы управления технологическими процессами (АСУ ТП)	Содержание	36/18		
	1. Понятие об объекте управления. Свойства объекта управления.	18	1	ПК 3.1-3.5 ОК 01-09 ЛР
	2. Классификация технологических объектов управления по типу, характеру технологического процесса, по характеристике параметров управления		1	
	3. Классификация систем управления технологическими объектами по способу, цели и степени централизации управления.		1	
	4. Общие сведения об автоматизированных системах управления технологическими процессами (АСУТП) и системах автоматического управления (САУ)		1	
	5. Основные функции АСУТП и САУ. Техническое, программное и информационное обеспечение АСУТП		1	
	6. Структура АСУТП на базе микропроцессорной техники.		1	
	7. Средства измерения преобразования и регулирования в АСУТП		1	
	8. Основные понятия автоматизированной обработки информации		1	
	9. Методы и средства моделирования технологических процессов в АСУТП		1	
	10. Обзор современных технологий и тенденций развития АСУТП		1	
	11. Программирование и настройка АСУТП: языки программирования, методы и инструменты		1	
	12. Интеграция АСУТП с другими системами и оборудованием в производственном процессе		1	
	13. Оценка эффективности и экономическая оценка внедрения АСУТП		1	
	14. Особенности управления производственными системами в условиях неопределенности и переменных условий работы		1	

	15. Применение систем искусственного интеллекта в АСУТП: нейронные сети, генетические алгоритмы, экспертные системы		1	
	В том числе практических занятий и лабораторных работ	18		
	Практическое занятие 1. Определение свойств объектов управления на практике	18	2	ПК 3.1-3.5 ОК 01-09 ЛР
	Практическое занятие 2. Классификация технологических объектов управления на примере производственного предприятия		2	
	Практическое занятие 3. Анализ и сравнение систем управления технологическими объектами на примере различных отраслей промышленности		2	
	Практическое занятие 4. Изучение принципов работы АСУТП и САУ на примере реальных систем управления		2	
	Практическое занятие 5. Создание простой модели технологического процесса		2	
	Практическое занятие 6. Ознакомление с современными технологиями АСУТП на примере существующих проектов и исследований		2	
	Практическое занятие 7. Программирование элементов АСУТП на языках программирования на практике		2	
	Практическое занятие 8. Настройка и проверка работоспособности элементов АСУТП на примере конкретной системы управления		2	
	Практическое занятие 9. Интеграция АСУТП с другими системами и оборудованием в производственном процессе		2	
	Практическое занятие 10. Оценка эффективности и экономическая оценка внедрения АСУТП			
	Практическое занятие 11. Разработка системы управления производственными процессами в условиях неопределенности и переменных условий работы		2	
	Практическое занятие 12. Применение нейронных сетей в системах управления технологическими процессами		2	
	Практическое занятие 13. Применение экспертных систем в системах управления технологическими процессами		2	
	Практическое занятие 14. Создание проекта автоматизации управления технологическим процессом на основе АСУТП		2	
	Содержание	36/20		

Тема 2.2. Промышленные сетевые технологии и протоколы в АСУ ТП	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.	16	1	ПК 3.1-3.5 ОК 01-09 ЛР
	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.		1	
	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	
	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.		1	
	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.		1	
	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	
	7. Работа контроллера (master) в сети с модулями ввода/вывода (slave)		1	

	<p>Основные принципы взаимодействия контроллера и устройств ввода-вывода 2 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.</p>			
	<p>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.</p>	1		
	<p>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.</p>	1		
	<p>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.</p>	1		ПК 3.1-3.5 ОК 01-09 ЛР
	<p>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.</p>	1		

	<p>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.</p>		1	
	<p>13. Преобразователи интерфейсов Преобразователи интерфейсов для различных стандартов связи (RS-232, RS-485, Ethernet, USB). Выбор и настройка преобразователей интерфейсов в соответствии с требованиями конкретной задачи.</p>		1	
	<p>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.</p>		1	
	<p>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.</p>		1	
	<p>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.</p>		1	
	<p>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,</p>		1	ПК 3.1-3.5 ОК 01-09 ЛР

их преимущества и недостатки, области применения в промышленных сетях и АСУ ТП.			
18. Применение промышленных маршрутизаторов для обеспечения безопасности и надежности работы сетевой инфраструктуры. Роль промышленных маршрутизаторов в обеспечении безопасности и надежности работы сетевой инфраструктуры в промышленной среде. Основные функции промышленных маршрутизаторов (виртуальная частная сеть (VPN), брандмауэр, NAT-трансляция), их конфигурация и настройка. Методы защиты от внешних атак и обеспечения надежности работы сетевой инфраструктуры.		1	ПК 3.1-3.5 ОК 01-09 ЛР
В том числе практических занятий и лабораторных работ	20		
Практическое занятие 1. Работа с основными сетевыми технологиями в промышленной автоматизации	20	2	ПК 3.1-3.5 ОК 01-09 ЛР
Практическое занятие 2. Разработка схемы промышленной сети и выбор средств ее реализации		2	
Практическое занятие 3. Практическое применение протокола MODBUS для обмена данными между устройствами		2	
Практическое занятие 4. Создание конфигурации сети с использованием протокола MODBUS		2	
Практическое занятие 5. Организация работы контроллера (slave) и операторной панели (master) по протоколу MODBUS		2	
Практическое занятие 6. Выравнивание адресов переменных в поле памяти протокола MODBUS		2	
Практическое занятие 7. Настройка работы контроллера (master) с модулями ввода/вывода (slave) по протоколу MODBUS RTU		2	
Практическое занятие 8. Практическая работа с различными устройствами по протоколу MODBUS RTU		2	
Практическое занятие 9. Работа с протоколом MODBUS TCP		2	
Практическое занятие 10. Работа с типовыми проводными и кабельными протоколами в промышленности		2	
Практическое занятие 11. Изучение беспроводных локальных сетей для промышленного применения		2	
Практическое занятие 12. Практическое применение специализированных сетевых интерфейсов для умного дома		2	

	<p>Практическое занятие 13. Работа с преобразователями интерфейсов в промышленной сети</p> <p>Практическое занятие 14. Ознакомление с современными тенденциями в развитии сетевых технологий в АСУ ТП, включая web-серверы и облачные решения</p> <p>Практическое занятие 15. Особенности применения промышленных сетевых протоколов в условиях высоких нагрузок и плохой связи</p> <p>Практическое занятие 16. Сравнительный анализ промышленных Ethernet-технологий: EtherNet/IP, PROFINET, Modbus TCP</p> <p>Практическое занятие 17. Применение промышленных маршрутизаторов для обеспечения безопасности и надежности работы сетевой инфраструктуры</p> <p>Практическое занятие 18. Практическое использование промышленных маршрутизаторов</p> <p>Практическое занятие 19. Организация удаленного доступа к сетевым устройствам в промышленной сети</p> <p>Практическое занятие 20. Разработка и тестирование собственного промышленного протокола для обмена данными между устройствами в сети</p> <p>Практическое занятие 21. Организация кластера промышленных компьютеров для выполнения высокопроизводительных вычислений в АСУ ТП</p>		<p>2</p> <p>2</p> <p>2</p> <p>2</p> <p>2</p> <p>2</p> <p>2</p> <p>2</p> <p>2</p>	<p>ПК 3.1-3.5 ОК 01-09 ЛР</p>
<p>Примерная тематика самостоятельной учебной работы при изучении раздела 2. Технологии автоматизации технологических процессов</p> <p>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.</p> <p>Тематика домашних заданий, сообщений, рефератов:</p> <ol style="list-style-type: none"> 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 				

<p>Text (ST) и т.д.</p> <ol style="list-style-type: none"> 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. 			
<p>Учебная практика раздела 2. Технологии автоматизации технологических процессов</p> <p>Виды работ</p> <ol style="list-style-type: none"> 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. 	72		

<p>Производственная практика раздела 2. Технологии автоматизации технологических процессов</p> <p>Виды работ</p> <ol style="list-style-type: none"> 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 программного обеспечения серверов и рабочих станций. 4. Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли. 5. Установка прав доступа и контроль использования сетевых ресурсов. 6. Обеспечение своевременного копирования, архивирования и резервирования данных. 7. Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования. 8. Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению. 9. Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети. 	36		
<p>Курсовой проект (работа)</p> <p>Тематика курсовых проектов (работ)</p> <ol style="list-style-type: none"> 1. Разработка системы автоматизации процесса производства на базе промышленного контроллера. 2. Создание системы автоматического управления технологическими процессами на основе методов искусственного интеллекта. 3. Разработка программного обеспечения для автоматизации процесса сборки изделий на промышленном производстве. 4. Исследование и внедрение технологии RFID (Radio Frequency Identification) для автоматизации учета и контроля процессов на производстве. 5. Создание системы мониторинга технологических процессов с использованием датчиков и IoT-технологий. 6. Разработка системы автоматического управления энергопотреблением на производстве для повышения эффективности и экономии затрат. 7. Исследование и внедрение технологии 3D-печати в производственный процесс с целью автоматизации и оптимизации процессов. 8. Разработка системы автоматического контроля и управления качеством продукции на производстве. 9. Исследование и анализ существующих технологий автоматизации технологических процессов с целью выбора наиболее эффективной и оптимальной. 10. Создание системы автоматизации управления складскими процессами с использованием 	30		

технологий IoT и искусственного интеллекта. 11. Разработка программного обеспечения для автоматизации технологических процессов на малых предприятиях. 12. Исследование и внедрение системы автоматизации управления производственным циклом на основе принципов LEAN-производства. 13. Создание системы автоматизированного управления и контроля технологических процессов в сельском хозяйстве. 14. Разработка системы автоматизации процесса транспортировки грузов на складах и производстве с использованием робототехники. 15. Исследование и анализ существующих технологий автоматизации процессов в машиностроительной отрасли с целью выбора оптимальной для конкретного производства.				
Раздел 3. Безопасность сетевой инфраструктуры		102/46/30		
МДКн.03.03. Безопасность сетевой инфраструктуры		102/46/30		
Тема 3.1. Безопасность компьютерных сетей	Содержание	34/14		
	1. Фундаментальные принципы безопасной сети Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.	14	1	ПК 3.1-3.5 ОК 01-09 ЛР
	2. Безопасность сетевых устройств OSI Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.		1	
	3. Авторизация, аутентификация и учет доступа (AAA) Свойства AAA. Локальная AAA аутентификация. Server-based AAA		1	
	4. Реализация технологий брандмауэра ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах.		1	
	5. Реализация технологий предотвращения вторжения IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS		1	
	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	
	7. Криптографические системы Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей		1	

	<p>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 CDP. Реализация Remote-access VPN</p>		1	
	<p>9. Управление безопасной сетью Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасностью. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности.</p>		1	
	<p>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.</p>		1	ПК 3.1-3.5
	<p>11. Межсетевая безопасность Методы обеспечения безопасности взаимодействия между различными сетями. Реализация технологий маршрутизации и шлюзов, использование межсетевых экранов, технологии виртуальных локальных сетей.</p>		1	ОК 01-09 ЛР
	<p>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.</p>		1	
	<p>13. Защита от социальной инженерии Методы социальной инженерии, опасности, связанные с подделкой и манипулированием данными, а также методы защиты и обучения персонала.</p>		1	
	<p>В том числе практических занятий и лабораторных работ</p>	20		
	<p>Практическое занятие 1. Социальная инженерия</p>		2	ПК 3.1-3.5
	<p>Практическое занятие 2. Исследование сетевых атак и инструментов проверки защиты сети</p>	20	2	ОК 01-09
	<p>Практическое занятие 3. Настройка безопасного доступа к маршрутизатору</p>		2	ЛР

	Практическое занятие 4. Обеспечение административного доступа AAA и сервера Radius		2	ПК 3.1-3.5 ОК 01-09 ЛР
	Практическое занятие 5. Настройка политики безопасности брандмауэров		2	
	Практическое занятие 6. Настройка системы предотвращения вторжений (IPS)		2	
	Практическое занятие 7. Настройка безопасности на втором уровне на коммутаторах		2	
	Практическое занятие 8. Исследование методов шифрования		2	
	Практическое занятие 9. Настройка Site-to-SiteVPN используя интерфейс командной строки		2	
	Практическое занятие 10. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки		2	
	Практическое занятие 11. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM		2	
	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	
	Практическое занятие 13. Настройка Clientless Remote Access SSL VPNs используя ASDM		2	
	Практическое занятие 14. Настройка AnyConnect Remote Access SSL VPN используя ASDM		2	
	Практическое занятие 15. Комплексная лабораторная работа по безопасности		2	
Тема 3.2. Обеспечение сетевой безопасности	Содержание	48/26		
	1. Организация защищенных каналов передачи данных для объединения территориально распределенных офисов в одну сеть.	22	1	ПК 3.1-3.5 ОК 01-09 ЛР
	2. Механизмы шифрования и аутентификации для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам и сервисам.		1	
	3. Использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.		1	
	4. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети.		1	

5.	Методы минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.		1	ПК 3.1-3.5 ОК 01-09 ЛР	
6.	Введение системы обнаружения и предотвращения сетевых вторжений.		1		
7.	Технологии использования виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа.		1		
8.	Использование системы управления доступом для контроля доступа к корпоративной сети.		1		
9.	Обеспечение безопасности Wi-Fi-сетей.		1		
10.	Реализация мер по обеспечению безопасности электронной почты в корпоративной сети.		1		
11.	Защита от атак типа "фишинг".		1		
12.	Применение антивирусного программного обеспечения для защиты от вирусов и других вредоносных программ.		1		
13.	Использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.		1		
14.	Защита от DDoS-атак.		1		
15.	Реализация мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети.		1		
16.	Защита от внутренних угроз безопасности.		1		
17.	Обеспечение безопасности облачных сервисов.		1		
18.	Организация мониторинга сетевой безопасности и аудита.		1		
19.	Введение системы контроля целостности файлов для защиты от изменения или внедрения вредоносных программ в файловые системы.		1		
20.	Применение методов шифрования данных для защиты от несанкционированного доступа к конфиденциальной информации.		1		
В том числе практических занятий и лабораторных работ		26			
	Практическое занятие 1. Настройка VPN-туннелей для организации защищенных каналов передачи данных между территориально распределенными офисами.	26	2		ПК 3.1-3.5 ОК 01-09 ЛР

Практическое занятие 2. Работа с механизмами шифрования и аутентификации для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.	2	ПК 3.1-3.5 ОК 01-09 ЛР
Практическое занятие 3. Настройка и использование фаерволов и межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.	2	
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	
Практическое занятие 5. Разработка и внедрение мер по минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.	2	
Практическое занятие 6. Настройка и работа с системами обнаружения и предотвращения сетевых вторжений для раннего обнаружения и предотвращения угроз безопасности.	2	
Практическое занятие 7. Настройка и использование виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа к корпоративным информационным ресурсам и сервисам.	2	
Практическое занятие 8. Настройка и работа с системами управления доступом для контроля доступа к корпоративной сети.	2	
Практическое занятие 9. Обеспечение безопасности Wi-Fi-сетей: настройка безопасных точек доступа, использование сетевой аутентификации, шифрования трафика и других методов.	2	
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.	2	
Практическое занятие 11. Обучение пользователям основам защиты от атак типа "фишинг".	2	
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.	2	

	Практическое занятие 13. Настройка и использование систем обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.	2		ПК 3.1-3.5
	Практическое занятие 14. Настройка и использование межсетевых экранов и фаерволов для обеспечения комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.	2		ОК 01-09 ЛР
	Практическое занятие 15. Внедрение системы управления доступом для контроля доступа к корпоративной сети: настройка правил доступа, аутентификация пользователей, управление привилегиями.	2		
	Практическое занятие 16. Использование технологий виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа: настройка и управление VPN-туннелями, защита данных, маршрутизация трафика.	2		
	Практическое занятие 17. Обеспечение безопасности Wi-Fi-сетей: настройка и управление беспроводными точками доступа, защита сетевого трафика, аутентификация пользователей.	2		
	Практическое занятие 18. Защита от DDoS-атак: использование специализированных средств защиты от DDoS-атак, настройка маршрутизации трафика, мониторинг сетевой активности.	2		
	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.	2		
	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		
<p>Примерная тематика самостоятельной учебной работы при изучении раздела 3. Безопасность сетевой инфраструктуры</p> <p>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.</p> <p>Тематика домашних заданий, сообщений, рефератов:</p> <ol style="list-style-type: none"> 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 				

<p>к корпоративной сети.2</p> <ol style="list-style-type: none"> 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. 			
<p>Учебная практика раздела 2 Безопасность сетевой инфраструктуры Виды работ</p> <ol style="list-style-type: none"> 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 	72		
<p>Производственная практика раздела № 3 Безопасность сетевой инфраструктуры Виды работ</p>	72		

<p>1. Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия.</p> <p>2. Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций.</p> <p>3. Документирование всех произведенных действий.</p>			
<p>Курсовой проект (работа) Тематика курсовых проектов (работ)</p> <p>1. Анализ уязвимостей сетевой инфраструктуры предприятия и разработка плана обеспечения безопасности.</p> <p>2. Разработка и внедрение системы обнаружения и предотвращения сетевых вторжений.</p> <p>3. Исследование и анализ методов минимизации рисков внедрения вредоносного ПО через ограничение опасных коммуникаций в публичных сетях.</p> <p>4. Проектирование и реализация защиты от DDoS-атак в корпоративной сети.</p> <p>5. Анализ эффективности использования межсетевых экранов для комплексной защиты корпоративной сети от несанкционированного доступа через Интернет.</p> <p>6. Разработка системы управления доступом для контроля доступа к корпоративной сети.</p> <p>7. Исследование и разработка мер по обеспечению безопасности мобильных устройств, используемых в корпоративной сети.</p> <p>8. Проектирование и внедрение системы мониторинга сетевой безопасности и аудита.</p> <p>9. Анализ и разработка методов использования виртуальных частных сетей (VPN) для обеспечения безопасного удаленного доступа.</p> <p>10. Разработка и внедрение мер по обеспечению безопасности облачных сервисов.</p> <p>11. Исследование и анализ методов защиты от внутренних угроз безопасности.</p> <p>12. Разработка и внедрение системы контроля целостности файлов для защиты от изменения или внедрения вредоносных программ в файловые системы.</p> <p>13. Проектирование и реализация системы защиты Wi-Fi-сетей.</p> <p>14. Анализ содержимого трафика и контроль приложений и пользователей в системах безопасности сети.</p> <p>15. Разработка и внедрение механизмов шифрования и аутентификации для обеспечения защищенного удаленного доступа к корпоративным информационным ресурсам и сервисам.</p> <p>16. Исследование и разработка мер по защите от атак типа "фишинг".</p> <p>17. Разработка и внедрение механизмов защиты от вирусов и других вредоносных программ.</p> <p>18. Анализ эффективности использования системы обнаружения вторжений для раннего обнаружения и предотвращения угроз безопасности.</p>	<p>30</p>		
<p>Всего:</p>	<p>700</p>		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Лаборатории «Информационных технологий», «Направляющих систем» оснащенные в соответствии.

Мастерские «Монтажа и настройки объектов сетевой инфраструктуры, «Ремонта и обслуживания устройств инфокоммуникационных систем».

Оснащенные базы практики, в соответствии с п 6.1.2.5 примерной образовательной программы по специальности 09.02.06 Сетевое и системное администрирование.

3.2. Информационное обеспечение реализации программы

3.2.1. Основные печатные издания

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

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

3.2.2. Основные электронные издания

1. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры [Электронный ресурс]: учебник / А. В. Назаров, А. Н. Енгальчев, В. П. Мельников. – М.: КУРС; ИНФРА-М, 2020. — 360 с. —Режим доступа: <https://znanium.com/catalog/product/1071722>

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: учебное пособие / В. Ф. Шаньгин. — М.: ФОРУМ: ИНФРА-М, 2021. — 416 с. Режим доступа: <https://znanium.com/catalog/product/1189327>

3.2.3. Дополнительные источники (при необходимости)

1. <https://acti.ru/resheniya-i-uslugi/informatcionnaia-bezopasnost/bezopasnost-it-infrastruktury/zashchita-perimetra-i-setevaia-bezopasnost/>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование ПК и ОК, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Осуществлять проектирование сетевой инфраструктуры	Определение профессиональной задачи и этапов ее выполнения	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием
ПК 3.2. Обслуживать сетевые конфигурации программно-аппаратных средств	Эффективный поиск информации для решения	
ПК 3.3. Осуществлять защиту информации в сети с использованием программно-аппаратных средств		

ПК 3.4. Осуществлять устранение нетипичных неисправностей в работе сетевой инфраструктуры	профессиональной задачи	Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам
ПК 3.5. Модернизировать сетевые устройства информационно-коммуникационных систем	<p>Определение ресурсов для решения профессиональной задачи</p> <p>Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры.</p> <p>Оценка «хорошо» - алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.</p> <p>Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.</p>	<p>Защита отчетов по практическим и лабораторным работам</p> <p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы</p>
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	Подбор вариантов решения конкретной профессиональной задачи или проблемы	Оценка полноты перечня подобранных вариантов
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	Демонстрация навыков использования информационных порталов в сети Интернет, включая официальные информационно-правовые порталы	Оценка полноты перечня подобранных вариантов
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие,	Демонстрация интереса к выбранной специальности, к инновационным	Участие в мероприятиях (олимпиады, конкурсы профессионального

<p>предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях</p>	<p>технологиям в области профессиональной деятельности</p>	<p>мастерства, стажировки и др.), проводимых как образовательным заведением, так и ведущими предприятиями отрасли</p>
<p>ОК 04. Эффективно взаимодействовать и работать в коллективе и команде</p>	<p>Демонстрировать навыки межличностного общения с соблюдением общепринятых правил со сверстниками в образовательной группе, с преподавателями во время обучения, с руководителями производственной практики</p>	<p>Экспертное наблюдение поведенческих навыков в ходе обучения</p>
<p>ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста</p>	<p>Демонстрация навыков грамотной устной и письменной речи</p>	<p>Экспертное наблюдение навыков устного и письменного общения в ходе обучения</p>
<p>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</p>	<p>Формирование чувства патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества, закону и правопорядку, человеку труда и старшему поколению;</p> <p>взаимного уважения, бережного отношения к культурному наследию и традициям многонационального народа Российской Федерации;</p> <p>нетерпимости к коррупционным проявлениям</p>	<p>Участие в мероприятиях патриотической направленности, в проведении военно-спортивных игр; участие в программах антикоррупционной направленности</p>

<p>ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях</p>	<p>Формирование бережного отношения к природе и окружающей среде</p>	<p>Экспертное наблюдение демонстрации навыков соблюдения правил экологической безопасности в ведении профессиональной деятельности; формирование навыков эффективных действий в чрезвычайных ситуациях</p>
<p>ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности</p>	<p>Формирование бережного отношения к здоровью</p>	<p>Участие в спортивных мероприятиях, проводимых образовательным учреждением; ведение здорового образа жизни</p>
<p>ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках</p>	<p>Демонстрация умения составлять тексты документов, относящихся к профессиональной деятельности, на государственном и иностранном языках</p>	<p>Экспертная оценка соблюдения правил составления документов</p>