Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение высшего образования
"Российский экономический университет имени Г.В. Плеханова"
МОСКОВСКИЙ ПРИБОРОСТРОИТЕЛЬНЫЙ ТЕХНИКУМ

РАБОЧАЯ ПРОГРАММА

профессионального модуля ПМ.03 «Эксплуатация объектов сетевой инфраструктуры»

код, специальность: **09.02.02 Компьютерные сети**

Квалификация: техник по компьютерным сетям

2017

СОГЛАСОВАНА:
Предметной (цикловой) комиссией

Профессиональных модулей
09.02.02 и 09.02.06

Протокол № 1-17/18 КС
от «31» августа 2017 года

Разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования
09.02.02 Компьютерные сети

Председатель предметной (цикловой) комиссии

О.П. Каторгина
Подпись Инициалы Фамилия

Заместитель директора по учебной работе

/ Д.А. Клопов /
Подпись Инициалы Фамилия

УТВЕРЖДЕНА:
Директор техникума

/ А.В. Чурилов /
Подпись Инициалы Фамилия

Составители (авторы): О.П. Каторгина, преподаватель ФГБОУ ВО «РЭУ им. Г.В.Плеханова»
Д.С. Харченко, преподаватель ФГБОУ ВО «РЭУ им. Г.В.Плеханова»

СОГЛАСОВАНО
с работодателем : Немых Кирилл Владимирович, генеральный директор ООО «БУТ ГРУПП»
Ф.И.О., ученая степень, звание, должность, наименование ФГБОУ

Лист актуализации

рабочей программы профессионального модуля

В рабочую программу профессионального модуля на 2018/19 уч. год внесены следующие изменения:

1. На основании Указа Президента РФ от 15.01.2018 года №215 на титульном листе исправлено Министерство образования и науки Российской Федерации на Министерство науки и высшего образования Российской Федерации

Дата актуализации: 30.08.2018 г

СОДЕРЖАНИЕ

1. Паспорт рабочей программы профессионального модуля…….4
2. Результаты освоения профессионального модуля……...7
3. Структура и содержание профессионального модуля…….9
4. Условия реализации профессионального модуля……..23
5. Контроль и оценка результатов освоения профессионального модуля…...25

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Эксплуатация объектов сетевой инфраструктуры

1.1. Область применения программы

Рабочая программа профессионального модуля является частью программы подготовки специалистов среднего звена (далее - ППССЗ) по специальности 09.02.02 «Компьютерные сети». Год начала подготовки по учебному плану 2017.

Эксплуатация объектов сетевой инфраструктуры и соответствующих профессиональных компетенций (ПК):

1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей;
2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях;
3. Эксплуатировать сетевые конфигурации;
4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации;
5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования;
6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и профессиональной подготовке работников в области информатики и вычислительной техники при наличии среднего (полного) общего образования. Опыт работы не требуется. Год начала подготовки по учебному плану 2018.

1.2. Цели и задачи профессионального модуля – требования к результатам освоения профессионального модуля

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

иметь практический опыт:

– обслуживания сетевой инфраструктуры, восстановления работоспособности сети после сбоя;
– удаленного администрирования и восстановления работоспособности сетевой инфраструктуры;
– организации бесперебойной работы системы по резервному копированию и восстановлению информации;
– поддержки пользователей сети, настройки аппаратного и программного обеспечения сетевой инфраструктуры;

уметь:

– выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
– использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры;
– осуществлять диагностику и поиск неисправностей технических средств;
– выполнять действия по устранению неисправностей в части, касающейся полномочий техника;
– тестировать кабели и коммуникационные устройства;
– выполнять замену расходных материалов и мелкий ремонт периферийного оборудования;
– правильно оформлять техническую документацию;
– наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;
– устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;

знать:

– архитектуру и функции систем управления сетями, стандарты систем управления;
– задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;
– средства мониторинга и анализа локальных сетей;
– классификацию регламентов, порядок технических осмотров, проверок и профилактических работ;
– правила эксплуатации технических средств сетевой инфраструктуры;
– расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;
– методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;
– основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем (ИС), требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы

повышения безопасности функционирования программных средств и баз данных;

– основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

всего – **852** часа, в том числе:

максимальной учебной нагрузки обучающегося – **582** часов;
обязательной аудиторной учебной нагрузки обучающегося – 425 часа;
теоретические занятия – 235 часов;
лабораторные занятия – 140 часов;
самостоятельной работы обучающегося – 151 час;
консультаций – 6 часов;
курсовой проект – 50 часов;
учебной практики – 54 часа;
производственной практики – 216 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД) **Участие в проектировании сетевой инфраструктуры**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 3.1.	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей
ПК 3.2.	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях
ПК 3.3.	Эксплуатировать сетевые конфигурации
ПК 3.4.	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации
ПК 3.5.	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после ремонта
ПК 3.6.	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды

	(подчиненных), за результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

1. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.		Занятия во взаимодействии с преподавателем, час						Консультации	Самостоятельная работа
				Обучение по МДК				*Практики*			
			Всего	Теоретические занятия	Лабораторных и практических занятий	Курсовых работ (проектов)	Промежуточная аттестация	Учебная	Производственная		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6.	**Раздел 1.** Эксплуатация объектов сетевой инфраструктуры.	171	125	75	50	0	0	0	0	0	46
ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6.	**Раздел 2.** Безопасность функционирования информационных систем.	257	196	116	60	20	0	0	0	0	61
ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6.	**Раздел 3.** Техническое обслуживание средств вычислительной техники и КС	154	104	44	30	30	0	0	0	6	44
ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6.	**Раздел 4. УП 03.01. Т**ехническое обслуживание средств вычислительной техники и КС	54		0	0	0	0	54	0	0	0
ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ПК 3.6.	**Раздел 5. ПП 03.01.** Эксплуатация объектов сетевой инфраструктуры.	216		0	0	0	0	0	216	0	0
	Всего:	***852***	***425***	***235***	***140***	***50***	***0***	***54***	***216***	***6***	***151***

3.2. Содержание обучения по профессиональному модулю «Эксплуатация объектов сетевой инфраструктуры»

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Раздел 1 ПМ 3. Эксплуатация объектов сетевой инфраструктуры		**171**	
МДК 03.01 Эксплуатация объектов сетевой инфраструктуры		**171**	
Введение	**Объекты сетевой инфраструктуры и их эксплуатация**	**2**	**2**
Тема 3.1.1 Виртуализация Linux	**Содержание**	**54**	
	1. **Общие сведения о виртуализации Docker.** Сравнение виртуализации и контейнеризации, методы, применение контейнеризации, история, область применения	34	**1**
	2. **Работа с файлами в контейнерах Docker.** Монтирование файловой системы, работа с конфигурационными файлами.		
	3. **Взаимодействие контейнеров Docker.** Виртуальные сети между контейнерами, настройка сетевых имен, управление взаимодействием.		
	4. **Работа с образами Docker.** Анализ систем мониторинга, системы поддержки пользователей, обработка заявок, управление заявками, оформление технической документации		
	5. **Технологические основы и роль контейнеризации.** Создание и отладка работы контейнеров, настройка сетевых подключений, разворачивание готовых веб-приложений на базе созданных контейнеров.		
	6. **Жизненный цикл Docker-контейнера.**		
	7. **Dockerfile.** Структура, общие сведения, правила написания, процесс создания образа		
	8. **Docker-compose.** Общие сведения, процесс работы, разбор docker-compose laradock		

	Лабораторные работы		**20**	
	1.	Создание и установка виртуальной машины Linux	20	**2**
	2.	Установка Docker-engine		
	3.	Запуск первого контейнера. Запуск с разными параметрами.		
	4.	Создание собственного Dockerfile.		
	5.	Запуск собственного контейнера с различными параметрами		
	6.	Установка docker-compose. Запуск Docker-compose		
	7.	Установка и настройка laradock.		
	8.	Развертывание приложения в docker-compose laradock		
Тема 3.1.2 IP-телефония	**Содержание**		**32**	
	1.	**Аналоговая и цифровая телефония.** Введение в телефонию, сравнение аналоговой и цифровой телефониию	16	**1**
	2.	**IP-телефония. Сетевое взаимодействие.** Конвергенция сетей связи, передача голоса по IP-сетям, кодирование сигнала, кодеки.		
	Лабораторные работы		**16**	
	1.	Установка и настройка дистрибутива для IP-телефонии	16	**2**
	2.	Настройка Asterisk		
	3.	Настройка sip конфигурации		
	4.	Настройка номерного плана		
	5.	Настройка внутренних вызовов		
	6.	Настройка внешних вызовов		
	7.	Настройка переадресации вызовов		
	8.	Настройка голосоовго меню		
Тема 3.1.3 Резервное копирование	**Содержание**		**8**	
	1.	**Резервное копирование.** Методы восстановление резервных копий, создание резервных копий, разновидности резервного копирования	2	**1**
	Лабораторные работы		**6**	
	1.	Резервное копирование данных Windows Server	2	**2**
	2.	Резервное копирование данных Linux	2	
	3.	Резервное копирование конфигураций сетевого оборудования	2	
Тема 3.1.4 Беспроводные сети	**Содержание**		**29**	
	1.	**Беспроводные сети.**	21	**1**

		Стандарты, методы кодирования, радиообследование, модуляция сигналов, Архитектура беспроводных сетей, анализ производительность сети		
	Лабораторные работы		**8**	
	1.	Радиообследование. Анализ частот беспроводной сети.	8	**2**
	2.	Настройка Syslog-сервера и сбор данных с сетевого оборудования		
	3.	Настройка удаленного доступа сервера		
Самостоятельная работа обучающихся по МДК 03.01: Повторение пройденного материала; Примерная тематика внеаудиторной работы: Правила СКС; Кодирование сигналов в беспроводных сетях; Программы анализа производительности сети; Способы восстановления удаленных данных; Восстановление RAID-массивов, возможные ошибки; Системы заявок, структура работы; Системы мониторинга, протокол SNMP;			**46**	
Раздел 2 Безопасность функционирования информационных систем			**257**	
МДК 03.02 Безопасность функционирования информационных систем			257	
Тема 3.2.1 Основные понятия информационной безопасности.	**Содержание**		**2**	
	1.	**Введение в информационную безопасность. Основные аспекты информации безопасности.** Определение информационной безопасности. Виды информационной безопасности. Существенные признаки понятия: конфиденциальность, целостность, доступность, апеллируемость, подотчётность, достоверность. Безопасность информации. Безопасность автоматизированных информационных систем. Ценность информации. Уровень секретности.	2	**1**

Тема 3.2.2 Криптографические основы защиты информации.	**Содержание**		**14**	
	1.	**Введение в криптографию.** Определение науки криптография. Криптографические примитивы. Шифры перестановки. Шифры простой замены. Описание методов взлома: метод частотного анализа, коллективный доступ, слабые пароли, дефекты программирования.	12	**1**
	2.	**Симметричные алгоритмы шифрования.** Алгоритм Data Encryption Standart (DES) описание, принцип работы. Тройной DES. Шифрование паролей. Алгоритм AES.		
	3.	**Асимметричные алгоритмы шифрования.** Алгоритм RSA. Генерация ключей RSA. Алгоритм Эль-Гамаля. Алгоритм цифровой подписи. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм DSA.		
	4.	**Криптографические хеш-функции.** Описание хеш-функций. Алгоритм SHA, описание, принцип работы. Алгоритм MD, описание, принцип работы. Безопасность хеш-функций.		
	5.	**Инфраструктура открытых ключей.** Описание инфраструктуры открытых ключей PKI. Объекты PKI. Основные задачи PKI. Архитектура PKI. Алгоритм обмена ключами Диффи-Хеллмана.		
	Лабораторные работы.			2
	1.	Настройка сервера выдачи цифровых сертификатов.		
Тема 3.2.3 Виртуальные частные сети	**Содержание**		**28**	
	1.	**Определение виртуальной частной сети. Классификация виртуальных частных сетей. Туннелирование.** Сети VPN. Преимущества VPN. Типы VPN-сетей. Сети VPN site-to-site. Сети VPN удалённого доступа. Типы сетей VPN для удалённого доступа.	16	**1**
	2.	**Технологии туннелирования сетевого трафика. Протокол GRE. Настройка технологии GRE.** Основы GRE. Характеристики GRE. Настройка и проверка туннеля GRE. Протокол IP-IP принцип работы настройка.		
	3.	**Стек протоколов IPSec.** Общие сведения о IPsec. Сервисы безопасности IPsec. Структура протокола IPsec. Конфиденциальность и алгоритмы шифрования. Целостность и алгоритмы хеширования. Набор протоколов IPsec. Аутентификация IPsec.		
	4.	**Настройка VPN тунеля с применением технологии IPSec.**		

		Базовая настройка IPSec туннельного тапа с аутентификацией по ключу. Создание политики crypto map, transform set.		
	5.	**Виртуальные частные сети канального уровня. Настройка VPN соединений с применением протоколов L2TP и PPTP.** Протоколы PPTP, L2TP принцип работы, настройка.		
	6.	**Технология DMVPN. Описание принцип работы DMVPN. Настройка технологии DMVPN.** Описание, принцип работы технологии DMVPN. Описание принципа работы технологий NHRP и mGRE. Настройка DMVPN		
	7.	**Виртуальные частные сети с применение протокола SSL. Настройка технологии OpenVPN.** Описание принципа работы протокола SSL. Настройка технологии OpenVPN.		
	8.	**L2, L3 VPN. Технология коммутации по меткам. Настройка технологии MPLS VPN.** Технология быстрой коммутации по меткам: описание, принцип работы. Определения: L1 VPN,L2 VPN ,L3 VPN. Технология VRF: описание, принцип работы. Настройка MPLS VPN.		
	Лабораторные работы			
	1.	Настройка GRE туннеля.		
	2.	Настройка виртуальной частной сети с применением протокола IPSec.		
	3.	Настройка виртуальной протокола GRE поверх частной сети IPSec.	12	**2**
	4.	Настройка протокола L2TP на сетевом маршрутизаторе.		
	5.	Настройка протокола PPTP на сетевом маршрутизаторе.		
	6.	Настройка технологии OpenVPN.		
Тема 3.2.4 Безопасность компьютерных сетей построенных на основе стека протоколов TCP/IP.	**Содержание**		**42**	
	1.	**Классы атак в сетях на основе TCP/IP.** Атаки на сетевом и транспортном уровне: ping flood, IP spoofing, пассивное сканирование. MITM атаки. Способы предотвращение атак.		
	2.	**Безопасность серверной инфраструктуры. Демилитаризованная зона.**		
	3.	**DOS и DDOS атаки.** Атаки отказа в обслуживании DDOS. Виды DDOS атак. Предотвращение DDOS атак.		
	4.	**Технологии аутентификация протоколов динамической маршрутизации.**		

		Настойка аутентификации протоколов динамической маршрутизации OSPF и EIGRP. Принцип работы аутентификации протоколов маршрутизации EIGRP, OSPF: аутентификация по ключу, с помощью MD5. Настройка аутентификации.		
	5.	**Обеспечение безопасности канального уровня.** MITM атаки канального уровня: ARP-spoofing, DHCP-spoofing, VLAN-hopping, MAC-flooding, атаки на протокол STP. Способы предотвращения атак на канальном уровне.		
	6.	**Протокол контроль доступа в сеть 802.1X. Настройка технологии 802.1X.** Стандарт для настройки аутентификации и авторизации пользователей и рабочих станций в сети предприятия. Исследование принципа работы стандарта IEEE 802.1x. Настройка стандарта IEEE 802.1x на сетевом оборудование.		
	7.	**Расширенные списки контроля доступа. Настройка списков контроля доступа.** Принцип работы и настройка расширенных ACL.		
	8.	**Протоколы SSL/TLS.** Основные понятия протоколов SSL и TLS. Устройство, принцип работы протокола SSL. Цифровые сертификаты. Аутентификация и обмен ключами.	26	**1**
	9.	**Безопасность веб-сервиса. Настройка протокола HTTPS.** Развертывание веб сервера, выпуск самоподписанного сертификата.		
	10.	**Безопасность беспроводных соединений.** Современные беспроводные технологии. Архитектуры беспроводных технологий. Безопасность передачи данных в беспроводных технологиях. Аутентификация рабочих станций. Алгоритм Wired Equivalent Privacy (WEP). Формат кадра, ключи, инкапсуляция и декапсуляция алгоритма WEP. Технология Wi-Fi Protected Access (WPA и WPA 2). Программная платформа аутентификации Extensible Authentication Protocol. Конфиденциальность рабочих станций. Механизм конфиденциальности Rivest cipher 4 (RC4). Целостность рабочих станций. Идентификатор набора служб. Обнаружение Wireless Local Area Network (WLAN). Прослушивание беспроводного сигнала. Активные атаки на беспроводное соединение. Атаки на внутренние системы организации. Атаки на внешние системы организации. Реализация безопасности беспроводных сетей. Безопасность точек доступа. Безопасность передачи данных.		
	11.	**Технологии зеркалирования сетевого трафика. Настройка технологий SPAN/RSPAN.** Принцип работы и способы применения зеркалирования сетевого трафика на		

		коммутаторе. Настройка SPAN/RSPAN.		
	12.	**Аудит безопасности сети с применением программного решения Check Point Security CheckUP.** Развертывание Check Point CheckUP базовая настройка для анализа сетевого трафика.		
	13.	**Система контроля учета доступа Cisco ACS.** Cisco ACS принцип работы, описание, настройка.		
	Лабораторные работы		16	**2**
	1.	Настройка аутентификации протокола EIGRP.		
	2.	Настройка аутентификации протокола OSPF.		
	3.	Обеспечение безопасности канального уровня.		
	4.	Настройка протокола 802.1X на коммутаторе.		
	5.	Настройка протокола HTTPS.		
	6.	Обеспечение безопасности WI-FI соединения.		
	7.	Установка и настройка Check Point Security CheckUP.		
	8.	Настройка ACS сервера.		
Тема 3.2.5 Виртуальные частные сети.	**Содержание**		**10**	
	1	**Безопасность баз данных. Методы и средства защиты СУБД.** Основы обеспечения безопасности баз данных.	10	**1**
	2	**Антивирусные программы. Построение антивирусной защиты в корпоративной сети.** Определение антивирусного программного обеспечения. Целевые платформы антивирусного ПО. Классификация антивирусного продукта: по используемым технологиям антивирусной защиты, по функционалу продуктов, по целевым платформам, по объектам защиты. Антивирусное ПО для веб-сайтов: серверные, скрипты или компоненты CMS, SaaS сервисы. Типы антивирусного ПО: программы-детекторы, программы-доктора, программы-ревизоры, программы-фильтры, вакцины. Принцип работы антивирусного программного обеспечения. Базы антивирусного продукта.		
	3.	**Технологии аутентификации и авторизации. Многофакторная аутентификация.** Определение аутентификации. Элементы системы аутентификации: субъект, характеристика субъекта, хозяин системы аутентификации, механизм аутентификации, механизм управления доступом. Факторы аутентификации. Способы аутентификации: Аутентификация при помощи электронной подписи,		

		Аутентификация по паролям, аутентификация при помощи SMS, биометрическая аутентификация, аутентификация через географическое местоположение, многофакторная аутентификация. Протоколы аутентификации.		
	4.	**Системы предотвращеня утечек конфиденциальной информации. Системы управления инцидентами ИБ.** Принцип работы и развертывание DLP – систем и SIEM – систем.		
	5.	**Социальная инженерия.** Основы социальной инженерии. Методы и средства социальной инженерии.		
Тема 3.2.6 Программные и аппаратные средства защиты информации	**Содержание:**		**42**	
	1.	**Технологии фильтрации трафика.** Технология инспектирования трафика CBAC принцип работы, настройка. Рефлексивные ACL – списки, настройка.	12	**1**
	2.	**Программный и аппаратный межсетевой экран.** Определение и назначение. Классификации: управляемые коммутаторы, пакетные фильтры, шлюзы сеансового уровня, посредники прикладного уровня, инспекторы состояния. Принцип работы.		
	3.	**Аппаратный межсетевой экран Cisco ASA.** Cisco ASA принцип работы, описание, настройка.		
	4.	**Система обнаружения и предотвращения вторжения IPS/IDS.** Определение и назначение систем обнаружения и предотвращения вторжения. Виды систем обнаружения вторжения: сетевая СОВ, основанная на протоколе СОВ, основанная на прикладных протоколах СОВ, узловая СОВ, гибридная СОВ. Архитектура систем обнаружения вторжения. Пассивные и активные системы обнаружения вторжения.		
	5.	**Система предотвращения вторжения Cisco FirePower.** Система предотвращения вторжения Cisco FirePower: описание, принцип работы, внедрение, лицензирование.		
	Лабораторные работы:		30	**2**
	1	Настройка рефлексивных ACL-списков на маршрутизаторе.		
	2	Настройка технологии CBAC на маршрутизаторе.		
	3	Настройка Zone-Based Firewall на маршрутизаторе.		
	4	Базовая настройка Cisco ASA.		
	5	Настройка ACL - списков на межсетевом экране Cisco ASA.		
	6	Настройка инспектирования тафика на межсетевом экране Cisco ASA		
	7	Настройка AnyConnect VPN на Cisco ASA.		

	8	Настройка IPSec на Cisco ASA.		
	9	Настройка Clientless VPN на межсетевом экране Cisco ASA.		
	10	Настройка NAT на межсетевом экране Cisco ASA.		
	11	Настройка Cisco ASA в Transparent режиме.		
	12	Настройка технологии identity firewall на Cisco ASA.		
	13	Настройка системы IPS/IDS на маршрутизаторе.		
	14	Настройка системы предотвращения вторжения Snort.		
Тема 3.2.7 Защита персональных данных.	**Содержание:**		**10**	
	1.	**Персональные данные в организации.** Персональные данные, обработка персональных данных, оператор персональных данных, субъект персональных данных, неавтоматизированная обработка, автоматизированная обработка.	10	**1**
	2.	**Техническая защита персональных данных в информационных системах.** Уровни защищенности персональных данных при их обработке в информационных системах персональных данных (ИСПДн) в зависимости от угроз безопасности этим данным, категорий персональных данных и количества субъектов, чьи данные обрабатываются в ИСПДн. Модель угроз персональным данным. Базовая модель угроз. Перечень источников угроз. Уровень исходной защищенности. Методика актуализации угроз. Каналы утечки информации при обработке персональных данных в информационных системах. Построение системы защиты персональных данных.		
	3.	**Лицензирование деятельности по технической защите конфиденциальной информации.** Понятие технической защиты как лицензируемого вида деятельности. Лицензионные требования. Ответственность за незаконную деятельность в области защиты информации. Незаконное предпринимательство. Оценка и управление риском, связанным с отсутствием лицензии на техническую защиту конфиденциальной информации.		
	4.	**Аутсорсинг обработки персональных данных и их технической защиты.** Требования, выдвигаемые законом к порядку обработки персональных данных внешней организацией, содержание договора на обработку персональных данных. Передача внешней организации функций технической защиты персональных данных. Передача внешней организации функций лица, ответственного за организацию обработки персональных данных. Достоинства и недостатки аутсорсинга обработки персональных данных и их защиты.		
	5.	**Контроль и надзор за соблюдением законодательства о персональных данных.**		

		Система государственного контроля и надзора за обеспечением безопасности персональных данных. Принципы защиты прав юридических лиц, индивидуальных предпринимателей при осуществлении государственного контроля (надзора). Порядок планирования, организации и проведения проверок. Права и обязанности проверяемых и проверяющих. Меры, принимаемые должностными лицами органа госконтроля (надзора) при выявлении фактов нарушений.		
Тема 3.2.8 Системы контроля и учета доступа.	**Содержание:**		**14**	
	1.	**Назначение, классификация и состав СКУД .** Определение системы контроля и учёта доступа. Основные и дополнительные задачи.	14	**1**
	2.	**Архитектура построения СКУД.** Применение СКУД. Программное обеспечение. Сетевые и автономные системы.		
	3.	**Устройства, средства идентификации.** Идентификатор. Идентификация личности. Основные технологии идентификации.		
	4.	**Биометрические средства идентификации личности.** Определение и основные принципы биометрии. Основные понятия биометрии. Эффективность биометрических систем. Биометрические технологии. Схемы работ биометрических технологий.		
	5.	**Контроллеры СКУД.** Преграждающие устройства. Контроллер. Считыватель. Конвертеры сред. Вспомогательное оборудование.		
	6.	**Исполнительные устройства СКУД.** Исполнительные устройства (ИУ). Виды ИУ. Принцип работы и применение.		
	7.	**Варианты реализации СКУД.** Автономные СКУД. Сетевые системы контроля и управления доступом. Семейство СКУД Flex. Биометрические СКУД. Интегрированные СКУД.		
Тема 3.2.9. Организация и технологии системы видеонаблюдения	**Содержание:**		**14**	
	1.	**Система видеонаблюдения. Виды.** Основные понятия систем видеонаблюдения. Аналоговые и цифровые системы видеонаблюдения. Сравнение систем.		
	2.	**Аппаратное и программное обеспечение. Построение систем IP - видеонаблюдения.** Программное обеспечение систем видеонаблюдения. Сервер IP-видеонаблюдения. Архитектура построение систем видеонаблюдения. Алгоритмы анализа и синтеза систем видеонаблюдения.		

	3.	**IP DVR. Назначение, принцип работы.** Основные понятия, назначение технологии IP DVR. Способы реализации и настройка технологии IP DVR.	14	**1**
	4.	**Передача трафика в сетях с IP - видеонаблюдением.** Сетевые технологии используемые в IP – видеонаблюдении. Технология PoE. Сервер выдачи IP-адресов. Виртуальные локальные сети.		
	5.	**Способы сжатия видеопотока. Кодеки.** Основные понятия кодека. Виды кодеков. Механизмы сжатия видеопотока.		
	6.	**Технология подключения P2P.** Основные понятия технологии P2P. Способы реализации и настройка технологии P2P.		
	7.	**Преоретизация трафика в сетях с IP - видеонаблюдением.** Реализация QOS в сетях с IP-видеонаблюдением. Конфигурация очередей при передаче трафика.		
Обязательная аудиторная учебная нагрузка по курсовой работе (проекту)			**20**	
Примерная тематика курсовых работ (проектов) по МДК 3.2 модуля: 1. Применение двухфакторной авторизации; 2. Настройка виртуальной частной сети с применением протокола IPSec; 3. Обеспечение безопасности Web-сервера; 4. Анализ сетевых угроз в корпоративной сети; 5. Программно-аппаратные средства защиты информации; 6. Применение систем обнаружения и предотвращения вторжения; 7. Методы защиты персональных данных; 8. Аудит систем информационной безопасности; 9. Применение систем мониторинга безопасности; 10. Исследование принципа работы антивирусного программного обеспечения; 11. Настройка виртуальной частной сети с применением протокола GRE; 12. Исследование систем шифрования с открытым ключом; 13. Обеспечение безопасности данных в СУБД; 14. Применение цифровой подписи для обеспечения безопасности данных; 15. Обеспечение безопасности беспроводного сигнала.			20	

Самостоятельная работа при изучении раздела 2 ПМ 3: Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. **Примерная тематика внеаудиторной самостоятельной работы:** Службы каталогов. Подготовка индивидуального задания по теме «Аудит информационной безопасности компьютерных систем».			**61**	
Раздел 3 Техническое обслуживание средств вычислительной техники			**154**	
МДК 03.03 Техническое обслуживание средств вычислительной техники			**154**	
Введение			**2**	**1**
Тема 3.3.1 Понятия и составляющие технического обслуживания.	**Содержание**		**8**	**1**
	1.	Понятия и составляющие технического обслуживания.	8	
Тема 3.3.2 Диагностика функционирования СВТ.	**Содержание**		**18**	**3**
	1.	Диагностика функционирования СВТ.	8	
	Лабораторные работы		10	
	1.	Диагностические программы общего и специального назначения.		
	2.	Диагностика аппаратных неисправностей с применением диагностического оборудования.		
	3.	Диагностика программных неисправностей.		
Тема 3.3.3 Восстановление работоспособности СВТ.	**Содержание**		**22**	**3**
	1.	Восстановление работоспособности СВТ.	10	
	Лабораторные работы		12	
	1.	Конфигурирование базовой системы ввода-вывода.		
	2.	Восстановление работоспособности ОС и программ.		
	3.	Восстановление данных.		
	4.	Подбор компонентов ПК.		

Тема 3.3.4 Текущее техническое обслуживание.	**Содержание**		**16**	**3**
	1.	Текущее техническое обслуживание.	8	
	Лабораторные работы		8	
	1.	Системные утилиты.		
	2.	Оптимизация и повышение быстродействия СВТ.		
	3.	Настройка электропитания СВТ. Режимы запуска СВТ.		
Тема 3.3.5 Ресурсосберегающие и энергосберегающие технологии использования СВТ.	**Содержание**		**8**	**3**
	1.	Ресурсосберегающие и энергосберегающие технологии использования СВТ.	8	
Обязательная аудиторная учебная нагрузка по курсовой работе (проекту)				
Примерная тематика курсовых работ (проектов) по МДК 03.03 модуля: 1. Устранение аппаратных неисправностей персонального компьютера 2. Модернизация персонального компьютера 3. Типовые неисправности материнских плат, диагностика и выявление неисправностей 4. Обслуживание и ремонт жидкокристаллических мониторов 5. Восстановление данных с жестких дисков 6. Неисправности видеосистемы персонального компьютера 7. Ремонт и техническое обслуживание оптических накопителей 8. Анализ средств резервного копирования данных, создание копии, восстановление			**30**	
Самостоятельная работа обучающихся по разделу МДК 03.03. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторно-практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов и подготовка к их защите. **Примерная тематика внеаудиторной самостоятельной работы:** Поиск неисправностей по принципу локализации неисправностей конкретного оборудования; Изучить и понять принцип работы новых контрольно-измерительных аппаратов			44	
Консультации			6	
Учебная практика 03.01 Виды работ: - Компоновка системного блока - Устранение неисправностей оборудования системного блока. - Диагностика и локализация неопределенных неисправностей - Использование измерительных приборов			**54**	

- Восстановление данных на носителях информации после удаления - Диагностика неисправностей периферийных устройств - Создание и настройка RAID массивов		
Производственная практика (по профилю специальности) ПП 03.01 **Виды работ:** Использование пассивного оборудования сети. Заполнение технической документации. Построение физической карты локальной сети. Регламенты технических осмотров. Профилактические работы в объектах сетевой инфраструктуры. Мониторинг и анализ сети с помощью программных и аппаратных средств Структура системы управления, архитектура системы управления. Управление областями сети: ошибками, конфигурацией, доступом, производительностью, безопасностью. Работа с протоколами SNMP; CMIP; TMN; LNMP; ANMP. Отслеживание работы сети. Работа с сервером, чтение голов, работа над ошибками Работа с сервером. Контроль доступа, сохранение целостности данных и журналирование. Удаленное администрирование рабочих станций с сервера Удаленное администрирование сервера с рабочих станций, программы для удаленного доступа. Анализ трафика сети. Работа с кабельными сканерами и тестерами. Работа со встроенными сканерами диагностики и управления. Работа с базами данных, создание таблиц, внесение данных в таблицы, редактирование данных таблиц. Восстановление сети после сбоя. Создание плана восстановления сети. Использование в работе контрольно-измерительной аппаратуры, сервисных плат, комплексов. Разработка функциональных схем элементов автоматизированной системы защиты информации. Разработка алгоритма и интерфейса программы анализа информационных рисков и её тестирование. Анализ входящего и исходящего трафика. Контроль утечки конфиденциальной информации. Разработка политик безопасности и внедрение их в операционные системы. Настройка IPSec и VPN. Настройка межсетевых экранов. Проверка mail и web трафика на наличие вредоносного ПО с помощью антивирусных средств. Настройка защиты беспроводных сетей с помощью систем шифрования. Архивация и восстановление ключей в Windows Server (PKI). Установка и настройка системы обнаружения атак Snort.	216	
Консультации	48	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы профессионального модуля предполагает наличия

- Лаборатория эксплуатации объектов сетевой инфраструктуры

№ п/п	Оборудование	Технические средства обучения	Количество рабочих мест
1	Парты 16 шт	12 автоматизированных рабочих мест учащихся	13
2	доска маркерная	1 автоматизированное рабочее место преподавателя	
3	стол преподавателя 2 шт	проектор	
4	стулья - 28 шт		

Программное обеспечение:

Androind Studio, Brackets, Google Chrome, IIS Express, IntelliJ IDEA Community Edition, Java SE Development Kit, Microsoft Visual Studio Code, PascalABC.Net, PostgreSQL 12, Unity, Visual Studio Community 2019, WinRAR, XAMPP, Windows 10 Pro, Microsoft Office 2016, Visio 2016, Adobe Photoshop

- Лаборатория программно-аппаратной защиты объектов сетевой инфраструктуры

№ п/п	Оборудование	Технические средства обучения	Количество рабочих мест
1	столов 12	Системный блок 16	16
2	стульев 26	монитор 16	
3	сетевой шкаф 1	клавиатура 16	
4	доска 1	мышь 16	
5	стенды 1	проектор 1	
6	кабели различного типа	экран проектора 1	
7	обжимной инструмент	коммутаторы 2	
8	коннекторы RJ-45		
9	тестеры для кабеля		
10	кросс-ножи		
11	кросспанели		

Программное обеспечение:

Windows 10 pro, Microsoft office2016, visio, 1С Предприятие; Visual Studio 2019; arduino, unity,php, Notepad++,1С Предприятие; Visual Studio 2019; arduino, unity,php, Notepad++,SQL Server, My SQL,Adobe Illustrator, AutoCAD, Autodesk, ColerDraw, Mozila Firefox, Microsoft Edge, Google Chrome, Opera

- Полигон технического контроля и диагностики сетевой инфраструктуры

№ п/п	Оборудование	Технические средства обучения	Количество рабочих мест
1	парты 16 шт	Проектор	29
2	стол преподавателя 1шт	8 автоматизированных рабочих мест учащихся	
3	доска маркерная		
4	шкаф 4 шт		
5	стулья 29 шт		

Программное обеспечение:
Androind Studio, Brackets, Google Chrome, IIS Express, IntelliJ IDEA Community Edition, Java SE Development Kit, Microsoft Visual Studio Code, PascalABC.Net, PostgreSQL 12, Unity, Visual Studio Community 2019, WinRAR, XAMPP, Windows 10 Pro, Microsoft Office 2016, Visio 2016, Adobe Photoshop

- Мастерская монтажа и настройки объектов сетевой инфраструктуры

№ п/п	Оборудование	Технические средства обучения	Количество рабочих мест
1	доска маркерная	Проектор	40
2	парты 27 шт	Системный блок - 1	
3	стулья 40 шт	Монитор -1	
4	стол преподавателя 1 шт	Клавиатура - 1	
5	шкаф металлический 2 шт	Мышь – 1	

Программное обеспечение:
Windows 10 pro, Microsoft Office, Mozilla Firefox, Google Chrome, 7-zip, K-Lite Codec Pack

4.2. Информационное обеспечение обучения

Печатные издания не используются. ПМ полностью обеспечен электронными изданиями.

Электронные издания

1. Основы теории массового обслуживания: Учебник для вузов / В.Г. Карташевский. - М.: Гор. линия-Телеком, 2017. - 130 с.: ил.; 60x88 1/16. (обложка) ISBN 978-5-9912-0346-3, 500 экз. http://znanium.com/catalog/product/430028
2. Практикум по методам оптимизации: Практикум / Сдвижков О.А. - М.:Вузовский учебник, НИЦ ИНФРА-М, 2016. - 231 с.: 60x90 1/16 (Переплёт 7БЦ) ISBN 978-5-9558-0372-2 http://znanium.com/catalog/product/459517
3. Технические средства наблюдения в охране объектов / В.А. Ворона, В.А. Тихонов. - М.: Гор. линия-Телеком, 2016. - 184 с.: ил.; 60x90 1/16. (обложка) ISBN 978-5-9912-0143-8, 500 экз. http://znanium.com/catalog/product/253652
4. Основы информационной безопасности: Учебное пособие для вузов / Е.Б. Белов и др. - М.: Гор. линия-Телеком, 2017. - 558 с.: ил.; 60x88 1/16. - (Специальность; Учебное пособие для высших учебных заведений). (о) ISBN 5-93517-292-5, 100 экз.

http://znanium.com/catalog/product/405159
5. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области ...: Уч. пос./НовиковВ.К. - М.: Гор. линия-Телеком, 2016.- 176с.:60x88 1/16 (О) ISBN 978-5-9912-0525-2, 500 экз.
http://znanium.com/catalog/product/536932
6. Вопросы управления информационной безопасностью: Учебное пособие для вузов. Основы управления информационной безопасностью / Курило А.П., Милославская Н.Г., Сенаторов М.Ю. - М.:Гор. линия-Телеком, 2016. - 244 с.: 60x90 1/16. - (Вопросы управления информационной безопасностью) ISBN 978-5-9912-0271-8
http://znanium.com/catalog/product/560780
7. Периферийные устройства вычислительной техники: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 3-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2016. - 432 с.: ил.; 60x90 1/16. - (Профессиональное образование). (п) ISBN 978-5-91134-594-5
http://znanium.com/catalog/product/424031
8. Вычислительная техника, сети телекоммуникации: Учебное пособие для ВУЗов / Гребешков А.Ю., Попова Н.А. - М.: Гор. линия-Телеком, 2015. - 190 с.: 60x90 1/16. - (Учебник для высших учебных заведений) (Обложка) ISBN 978-5-9912-0492-7
http://znanium.com/catalog/product/524144
9. Догадин, Н.Б. Архитектура компьютера [Электронный ресурс] : учебное пособие / Н.Б. Догадин. — 3-е изд. (эл.). — Электрон. текстовые дан. (1 файл pdf : 274 с.). — М. : БИНОМ. Лаборатория знаний, 2015.—(Педагогическое образование).—Систем. требования: Adobe Reader XI ; экран 10". - ISBN 978-5-9963-2638-9
http://znanium.com/catalog/product/539585
10. Технические средства информатизации: Учебник / Зверева В.П., Назаров А.В. - М.:КУРС, НИЦ ИНФРА-М, 2017. - 256 с.: 60x90 1/16. - (Среднее профессиональное образование) (Переплёт 7БЦ) ISBN 978-5-906818-88-1
http://znanium.com/catalog/product/615331
11. Современные технологии и технические средства информатизации: Учебник / Шишов О. В. - М.: НИЦ ИНФРА-М, 2016. - 462 с.: 60x90 1/16. - (Высшее образование: Бакалавриат) (Переплёт 7БЦ) ISBN 978-5-16-011776-8
http://znanium.com/catalog/product/543015
12. Росс, Д. Телевизоры и мониторы. Ремонт, устройство и техническое обслуживание [Электронный ресурс] / Джон Росс; Пер. с англ. А. В. Карелина. - М. : ДМК Пресс, 2017. - 73 с. : ил. - ISBN 5-94074-230-0.
http://znanium.com/catalog/product/406862

Профессиональные базы данных и справочные системы

- Федеральная служба государственной статистики - https://rosstat.gov.ru/
- Наукометрическая и реферативная база данных SCOPUS - https://www.scopus.com
- Информационно-справочная система "КонсультантПлюс"

4.3. Общие требования к организации образовательного процесса

Изучение профессионального модуля «Участие в проектировании сетевой инфраструктуры» практически не базируется на изучении других профессиональных модулей или учебных дисциплин и поэтому может проводиться и на ранних стадиях обучения по специальности. При работе над курсовой работой (проектом) для обучающихся проводятся консультации.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 3.1 Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей	- точность и скорость настройки сети; - качество рекомендаций по повышению работоспособности сети; - выбор технологического оборудования для настройки сети; - расчет времени для настройки сети; - точность и грамотность оформления технологической документации.	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических занятиях, -при решении ситуационных задач, -при выполнении определенных видов работ производственной практики, -зачет по разделу практики
ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях	- точность и скорость настройки сети; - качество анализа свойств сети, исходя из ее служебного назначения; - качество рекомендаций по повышению технологичности сети; - точность и грамотность оформления технологической документации.	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических занятиях, -при решении ситуационных задач, -при выполнении определенных

		видов работ производственной практики, -зачет по разделу практики
ПК 3.3. Осуществлять эксплуатацию сетевых конфигураций	- точность и скорость настройки сети; - качество анализа и рациональность выбора сетевых конфигураций; - выбор способов настройки и технологически грамотное назначение технологической базы	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических занятиях, -при решении ситуационных задач, -при выполнении определенных видов работ производственной практики, -зачет по разделу практики
ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации	- выбор и использование пакетов прикладных программ для разработки конструкторской документации и проектирования технологических процессов	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических занятиях, -при решении ситуационных задач, -при выполнении определенных видов работ производственной практики, -зачет по разделу практики
ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль	- выбор и использование пакетов прикладных программ для разработки конструкторской документации и проектирования	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических

поступившего из ремонта оборудования	технологических процессов	занятиях, -при решении ситуационных задач, -при выполнении определенных видов работ производственной практики, -зачет по разделу практики
ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.	- выбор и использование пакетов прикладных программ для разработки конструкторской документации и проектирования технологических процессов	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы - на практических занятиях, -при решении ситуационных задач, -при выполнении определенных видов работ производственной практики, -зачет по разделу практики

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК.01 Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес	- участие в работе научно-студенческих обществ; - выступления на научно-практических конференциях; - участие во внеурочной деятельности, связанной с будущей профессией/специальностью (конкурсы профессионального мастерства, выставки и т.п.); - высокие показатели	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы: - на практических занятиях (при решении ситуационных

	производственной деятельности.	задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов и т.д.); - при выполнении и защите курсовой работы (проекта); - при выполнении работ на различных этапах производственной практики; - при проведении: контрольных работ, зачетов, экзаменов по междисциплинарным курсам, экзамена (квалификационного) по модулю.
ОК.02 Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	- выбор и применение методов и способов решения профессиональных задач, оценка их эффективности и качества.	
ОК.03. Решать проблемы, оценивать риски и принимать решения в нестандартных ситуациях.	- анализ профессиональных ситуации; - решение стандартных и нестандартных профессиональных задач.	
ОК.04. Осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития.	- эффективный поиск необходимой информации; - использование различных источников, включая электронные при изучении теоретического материала и прохождении различных этапов производственной практики.	
ОК.05. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	- использование в учебной и профессиональной деятельности различных видов программного обеспечения, в том числе специального, при оформлении и презентации всех видов работ.	
ОК.06 Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.	Взаимодействие: - с обучающимися при проведении деловых игр, выполнении коллективных заданий (проектов); - с преподавателями, мастерами в ходе обучения; - с потребителями и коллегами в ходе производственной практики.	
ОК.07 Ставить цели, мотивировать деятельность подчиненных, организовывать и контролировать их работу с принятием на себя ответственности за результат выполнения заданий.	- самоанализ и коррекция результатов собственной деятельности при выполнении коллективных заданий (проектов); - ответственность за результат выполнения заданий.	

ОК.08 Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	- планирование и качественное выполнение заданий для самостоятельной работы при изучении теоретического материала и прохождении различных этапов производственной практики; - определение этапов и содержания работы по реализации самообразования.	
ОК.09 Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	- адаптация к изменяющимся условиям профессиональной деятельности; - проявление профессиональной маневренности при прохождении различных этапов производственной практики.	