МИНИСТЕРСТВО ОБРАЗОВАНИЯ КРАСНОЯРСКОГО КРАЯ

Краевое государственное бюджетное профессиональное образовательное учреждение
«КРАСНОЯРСКИЙ МОНТАЖНЫЙ КОЛЛЕДЖ»

РАБОЧАЯ ПРОГРАММА

профессионального модуля **ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи**

для специальности **11.02.15 Инфокоммуникационные сети и системы связи**

г. Красноярск

2023 год

СОГЛАСОВАНО

Генеральный директор

АО КНМФ «ВОСТОКПРОМСВЯЗЬМОНТАЖ»

_____ В.В. Поткин

«15» 02 2023 г.

УТВЕРЖДАЮ

Заместитель директора

по учебной работе

_____ О. И. Моор

Программа составлена в соответствии с требованиями ФГОС СПО по специальности 11.02.15 Инфокоммуникационные сети и системы связи, утверждённого приказом Министерства просвещения РФ от «05» августа 2022 г. №675

ОДОБРЕНА
предметной (цикловой) комиссией
специальности «СС и СК»
протокол № 5 от 19.01 2023г.

Председатель ПЦК _____ И.В. Селина

Разработчик:
преподаватель КГБПОУ
«Красноярский монтажный колледж» _____ И. В. Селина

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

1.1. Область применения программы

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 11.02.15 Инфокоммуникационные сети и системы связи, входящей в состав укрупненной группы профессий 11.00.00 Электроника, радиотехника и системы связи.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и профессиональной подготовке работников в области технической эксплуатации телекоммуникационных систем и информационно-коммуникационных сетей связи при наличии среднего общего образования.

Максимальная учебная нагрузка обучающихся включает в себя вариативную часть, количество часов которой и вновь введенные профессиональные компетенции согласованы с работодателем.

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

С целью овладения видом профессиональной деятельности ВД.3 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи и соответствующими общими и профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

– анализировать сетевую инфраструктуру;

– выявлять угрозы и уязвимости в сетевой инфраструктуре;

– разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи;

– осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи;

– использовать специализированное программное обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи;

уметь:

– классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;

– проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;

– определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;

– осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;

– выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты;

– выполнять тестирование систем с целью определения уровня защищенности, определять оптимальные способы обеспечения информационной безопасности;

– проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;

– проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;

– разрабатывать политику безопасности сетевых элементов и логических сетей;

– выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;

– производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;

– конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;

– защищать базы данных при помощи специализированных программных продуктов;

– защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами;

знать:

– принципы построения информационно-коммуникационных сетей;

– международные стандарты информационной безопасности для проводных и беспроводных сетей;

– нормативно-правовые и законодательные акты в области информационной безопасности;

– акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;

– технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;

– способы и методы обнаружения средств съёма информации в радиоканале;

– классификацию угроз сетевой безопасности;

– характерные особенности сетевых атак;

– возможные способы несанкционированного доступа к системам связи,

– правила проведения возможных проверок согласно нормативным документам ФСТЭК;

– этапы определения конфиденциальности документов объекта защиты;

– назначение, классификацию и принципы работы специализированного оборудования;

– методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2;

– методы и средства защиты информации в телекоммуникациях от вредоносных программ;

– технологии применения программных продуктов;

– возможные способы, места установки и настройки программных продуктов,

– методы и способы защиты информации, передаваемой по кабельным направляющим системам;

– конфигурации защищаемых сетей;

– алгоритмы работы тестовых программ;

– средства защиты различных операционных систем и среды передачи информации;

– способы и методы шифрования (кодирование и декодирование) информации.

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 личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по 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 общечеловеческих 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	Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи
ПК 3.1.	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности
ПК 3.2.	Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи
ПК 3.3.	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования

Изучение дисциплины профессионального модуля ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи возможно с применением элементов дистанционного электронного обучения. Электронный УМК по данному профессиональному модулю разработаны и размещены на официальном сайте колледжа – http://krasdis.kraskmk.ru/login/ index.php.

1.3. Количество часов, отводимое на освоение профессионального модуля

Вид учебной работы	**Объем часов**
Максимальная учебная нагрузка (всего)	**228**
Обязательная аудиторная учебная нагрузка (всего)	**210**
в том числе:	
– теоретическое обучение	**56**
– практические занятия	**46**
Самостоятельная работа обучающегося (всего)	**6**
Промежуточная аттестация **4 семестр** в форме *дифференцированного зачёта* **4 семестр** в форме *экзамена по модулю*	 **24** **12**
Практика, в том числе: – учебная – производственная	 **36** **72**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных компетенций	Наименование разделов профессионального модуля	Суммарный объём нагрузки, час.	Объём профессионального модуля, час.						Самостоятельная работа
			Работа обучающихся во взаимодействии с преподавателем						
			Обучение по МДК				*Практики*		
			Всего	*В том числе*			Учебная	Производственная	
				Практических занятий	Курсовых работ (проектов)	Промежуточная аттестация			
ПК 3.1, ПК 3.2, ПК 3.3 ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09	Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	**108**	102	46					6
	УП.01.01 Учебная	**36**					**36**		
	ПП.01.01 Производственная	**72**						**72**	
	Экзамен по модулю	**12**							
	Всего:	**228**	**210**	**46**			**36**	**72**	**6**

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)		Объем, ак.ч / в том числе в форме практической подготовки, ак.ч	Коды компетенций, формированию которых способствует элемент программы
1	**2**		**3**	**4**
4 семестр				
Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи			**228**	
МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи			**228**	
Тема 1.1. Основы безопасности информационных технологий	**Содержание**		**12**	
	1	Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем. Основные причины обострения проблемы обеспечения безопасности информационных технологий.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	2	Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	3	Идентификация и аутентификация пользователей.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	4	Угрозы безопасности информационных технологий. Классификация угроз безопасности.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	5	Принципы обеспечения безопасности информационных технологий	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	6	Принципы построения системы обеспечения безопасности информации в автоматизированной системе.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	В том числе практических занятий		**6**	
	7	Анализ современных угроз ИБ	**2**	ПК 3.1–ПК 3.3
	8	Проектирование границ защиты	**2**	ПК 3.1–ПК 3.3
	9	Применение сертификатов для аутентификации и авторизации	**2**	ПК 3.1–ПК 3.3
Тема 1.2. Обеспечение	**Содержание**		**16**	
	10	Особенности обеспечения информационной безопасности в компьютерных сетях.	**2**	ПК 3.1–ПК 3.3

безопасности информационных технологий				ОК 01.–ОК 09.
	11	Спецификация средств защиты в компьютерных сетях	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	12	Сетевые модели передачи данных.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	13	Модель взаимодействия открытых систем OSI/ISO.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	14	Структура пакета. Шифрование	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	15	Типовые удаленные атаки и их характеристика.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	16	Принципы защиты распределенных вычислительных сетей.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	17	Принципы построения защищенных вычислительных сетей	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	В том числе практических занятий		**16**	
	18-19	Установка СЗИ (На примере IWTM)	**4**	ПК 3.1–ПК 3.3
	20-21	Установка межсетевого экрана	**4**	ПК 3.1–ПК 3.3
	22-23	Настройка правил фильтрации траффика DLP системой	**4**	ПК 3.1–ПК 3.3
	24-25	Настройка уровней доступа к различным подсетям (Применяется firewall)	**4**	ПК 3.1–ПК 3.3
Тема 1.3. Обеспечение безопасности стандартными средствами защиты	**Содержание**		**4**	
	26-27	Локальные политики безопасности	**4**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	В том числе практических занятий		**12**	
	28-29	Настройка локальных политик (windows системы)	**4**	ПК 3.1–ПК 3.3
	30-31	Создание пользователей, административная, пользовательская, гостевая учетные записи (windows системы)	**4**	ПК 3.1–ПК 3.3
	32-33	Сознание пользователей, права суперпользователя, ограничения пользователей, права доступа (unix системы)	**4**	ПК 3.1–ПК 3.3
Тема 1.4. Криптографическая	**Содержание**		**24**	
	34	Основы криптографии. Структура криптосистемы.	**2**	ПК 3.1–ПК 3.3

защита информации				ОК 01.–ОК 09.
	35	Основные методы криптографического преобразования данных	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	36	Симметричные криптосистемы.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	37	Ассимметричные криптосистемы	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	38	Криптосистемы с открытым ключом. Основы шифрования с открытым ключом.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	39	Алгоритм обмена ключами Диффи-Хеллмана.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	40	Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	41	Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	42	Технология работы электронной подписи.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	43	Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	44	Цифровые сертификаты. Отечественный стандарт цифровой подписи.	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	45	Понятие криптоанализа	**2**	ПК 3.1–ПК 3.3 ОК 01.–ОК 09.
	В том числе практических занятий		**12**	
	46-47	ЛР11 Шифрование данных симметричными и ассимметричными алгоритмами	**4**	ПК 3.1–ПК 3.3
	48-49	ЛР12 Криптоанализ	**4**	ПК 3.1–ПК 3.3
	50-51	ЛР13 Шифрование траффика, шифрование данных	**4**	ПК 3.1–ПК 3.3
Тематика самостоятельной учебной работы при изучении раздела. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим и лабораторным работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов и подготовка к их защите. Составление доклада по темам на основе публикаций в периодической специализированной аппаратуре.:			**6**	

1. Перспектива и направление развития программно-аппаратных средств защиты информации 2. Практическое применение антивирусных программ для защиты информации от несанкционированного доступа. 3. Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа. 4. Применение различных программ для оперативного и гарантированного восстановления информации на ПК. 5. Применение программно-аппаратных средств для обеспечения разграничения доступа к защищаемой информации. 6. Разработка комплекса организационно-административной защиты от вредоносных программ. 7. Самостоятельная разработка предложений по программно-аппаратной защите информации на определенном объекте. 8. Применение подсистемы безопасности WINDOWS XP/Vista/7 для предотвращения несанкционированного доступа к защищаемой информации.		
Учебная практика раздела. **Виды работ:** - установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов; - установка и настройка типовых программно-аппаратных средств защиты информации; - использование программно-аппаратных и инженерно-технических средств. - настройка, регулировка и ремонт оборудования средств защиты; - выбор способов и средств многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой; - проведение типовых операции настройки средств защиты операционных систем; - проведение аттестации объектов защиты; - определение источников несанкционированного доступа, исходя из модели угроз; - определение типа сигнала и технического средства в соответствии с алгоритмом программного продукта; - обнаружение и обезвреживание разрушающих программных воздействий с использованием программных средств; - защита телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК; - защита информации организационными методами в соответствии с инструкциями на объекте.	**36**	
Производственная практика раздела. **Виды работ:** 1. Участие в создании комплексной системы защиты на предприятии. 2. Применение программно-аппаратных средств защиты информации на предприятии 3. Применение инженерно-технических средств защиты информации на предприятии. 4. Применение криптографических средств защиты информации на предприятии.	**72**	
Промежуточная аттестация в форме *дифференцированного зачета и экзамена по модулю*	**12**	
Всего	**228**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Кабинет:

– «Компьютерного моделирования».

Лаборатории:

– «Информационной безопасности телекоммуникационных систем»;

– «Телекоммуникационных систем».

Кабинеты и лаборатории оснащены специальным оборудованием, инструментами, приспособлениями и измерительными приборами.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы, для использования в образовательном процессе.

При формировании библиотечного фонда образовательной организации выбираются не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

3.2.1. Основные печатные издания

1. Родичев, Ю.А. Информационная безопасность. Национальные стандарты Российской Федерации. Учебное пособие/ Ю.А. Родичев – СПб: Питер, 2019. – 304 с.: ил. – ISBN 978-5-4461-1275-3.

2. Нестеров, С.А. Основы информационной безопасности. Учебник для вузов/ С.А. Нестеров – М.: Лань, 2021. – 324 с.: ил. – ISBN 978-5-8114-6738-9.

3. Партыка Т.Л. Вычислительная техника: учеб. пособие / Т.Л. Партыка, И.И. Попов. — 3-е изд., перераб. и доп. — М.: ФОРУМ: ИНФРА-М, 2017. — 445 с.: ил. — (Среднее профессиональное образование). ISBN: 978-5-91134-646-1.

4. Назаров, А.В. Эксплуатация объектов сетевой инфраструктуры: учебник/ А. В.Назаров. - М.: Академия, 2018.- 368с. ISBN 978-5-44680347-7.

3.2.2. Основные электронные издания

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2.

2. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8.

3.2.3. Дополнительные источники

1. Сети и системы связи
2. Сводный реферативный журнал «Связь»
3. Журнал «Системы безопасности».

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности	классифицирование угроз информационной безопасности в инфокоммуникационных системах и сетях связи осуществляется верно; анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей обоснованный и полный; возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи определены верно; мероприятия по проведению аттестационных работ и выявлению каналов утечки осуществляются в полном объеме; недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выявлены в полном объеме, тестирование систем с целью определения уровня защищенности выполнено, уровень защищенности определен верно;	тестирование, экзамен, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.	для обеспечения информационной безопасности выбраны оптимальные способы; выбор средств защиты осуществлен в соответствии с выявленными угрозами в инфокоммуникационных сетях;	тестирование, экзамен, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3 Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.	мероприятия по защите информации на предприятиях связи определены в полном объеме, их организация, способы и методы реализации являются оптимальными и достаточными; политика безопасности сетевых элементов и логических сетей разработана в полном объеме; расчет и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей выполнены в соответствии с отраслевыми стандартами; установка и настройка средств защиты операционных систем, инфокоммуникационных систем и сетей связи	тестирование, экзамен, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

	выполнена в соответствии с отраслевыми стандартами; конфигурирование автоматизированных систем и информационно-коммуникационных сетей осуществлено в соответствии с политикой информационной безопасности и отраслевыми стандартами; базы данных максимально защищены при помощи специализированных программных продуктов; ресурсы инфокоммуникационных сетей и систем связи максимально защищены криптографическими методами;	
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач
ОК 02.	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач
ОК 03.	Планировать и реализовывать собственное профессиональное личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;
ОК 04.	Эффективно взаимодействовать и работать в коллективе и команде	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных	- соблюдение норм поведения во время учебных занятий и

	общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	прохождения учебной и производственной практик,
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках	понимание общего смысла четко произнесенных высказываний на известные темы (профессиональные и бытовые), текстов на базовые профессиональные темы, участие в диалогах на знакомые общие и профессиональные темы

Моор О.И.

Подписано цифровой подписью: Моор О.И.
DN: cn=Моор О.И., o=КГБПОУ "Краснорский монтажный колледж", ou=Зам.дир. по УР, email=kmkmo@mail.ru, c=RU
Дата: 2023.06.02 16:48:03 +07'00'