МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ МОРДОВИЯ

Государственное бюджетное профессиональное образовательное учреждение Республики Мордовия «Саранский электромеханический колледж»

САРАНСКИЙ ЭЛЕКТРОМЕХАНИЧЕСКИЙ КОЛЛЕДЖ

Подписано цифровой подписью: Махалов Сергей Анатольевич
DN: E=uc_fk@roskazna.ru, S=г. Москва, ИНН=007710568760, ОГРН=1047797019830, STREET="Большой Златоустинский переулок, д. 6, строение 1", L=Москва, C=RU, O=Федеральное казначейство, CN=Федеральное казначейство
Причина: Я являюсь автором этого документа
Дата: 13 Декабрь 2022 г. 21:39:28

У Т В Е Р Ж Д А Ю
Заместитель директора по учебной работе
ГБПОУ РМ «Саранский электромеханический колледж»
_____ Н.А. Адушкина
«31» августа 2020 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ. 03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

Основная профессиональная образовательная программа по специальности

11.02.15 Инфокоммуникационные сети и системы связи
(базовая подготовка)

Саранск 2020

Рабочая программа профессионального модуля разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.15 Инфокоммуникационные сети и системы связи.

Рассмотрена на заседании МК Компьютерные сети и комплексы, Многоканальные телекоммуникационные системы, Инфокоммуникационные сети и системы связи, Техническое обслуживание и ремонт радиоэлектронной техники, Информационные системы и программирование

«31» августа 2020 г. протокол № 1

Председатель МК	преподаватель	(подпись)	Н. В. Володина
Согласовано заведующий методическим кабинетом		(подпись)	О. В. Спицина
Разработчики рабочей программы:	ГБПОУ РМ «Саранский электромеханический колледж»	преподаватели	Г. В. Первушина Т. С. Астахова
Эксперты: Внутренняя экспертиза	ГБПОУ РМ «Саранский электромеханический колледж»	преподаватель	А. А. Войнов
Внешняя экспертиза	(место работы)	Начальник подразделения «РостелекомКонтакт-центр» в г. Саранске (занимаемая должность)	Е. А. Дягелева

СОДЕРЖАНИЕ

1.ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 4

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 7

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 24

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 25

ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В ПРОГРАММУ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

1.1. Область применения рабочей программы

Рабочая программа профессионального модуля является частью основной образовательной программы в соответствии с ФГОС СПО 11.02.15 Инфокоммуникационные сети и системы связи, утвержденной приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 г. № 158, входящей в укрупненную группу специальностей 11.00.00 Электроника, радиотехника и системы связи.

1.2. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи и соответствующие ему общие и профессиональные компетенции:

1.2.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.

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.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт:	- выявления угроз и уязвимостей в сетевой инфраструктуре с использованием системы анализа защищенности; - разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи; - осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.
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 нормативных документов 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.

1.3. Количество часов, отводимое на освоение профессионального модуля

Всего часов 604 ч.

Из них на освоение МДК 454 ч.

на практики: учебную 72 ч.

Производственную 72 ч.

самостоятельная работа 10 ч.

2. Структура и содержание профессионального модуля

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

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля**	Суммарный объем нагрузки, час.		Занятия во взаимодействии с преподавателем, час					Самостоятельная работа
				Обучение по МДК			Практики		
			Всего	Лабораторных и практических занятий	Курсовых работ (проектов)	консультации	Учебная	Производственная	
1	*2*	*3*	*4*	*5*	*6*		*7*	*8*	*9*
ПК 3.1, 3.2, 3.3 ОК 01-10	**Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи**	232	222	74		6			4
ПК 33.1, 3.2, 3.3 ОК 01-10	**Раздел 2. Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи**	222	210	94		6			6
ПК 3.1, 3.2, 3.3 ОК 01-10	Учебная практика	72					72		
ПК 3.1, 3.2, 3.3 ОК 01-10	Производственная практика практика)	*72*						*72*	
	Промежуточная аттестация (экзамен)	6							
	Всего:	***604***	***432***	***168***		***12***	***72***	***72***	***10***

2.2. Тематический план и содержание профессионального модуля ПМ.03. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов
1	2	3
Раздел 1. **Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи**		**232**
МДК 03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи		**232**
Тема 1.1.Основы безопасности информационных технологий	**Содержание**	**36(22/14)**
	1. Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечения безопасности информационных технологий.	22
	2. Основные понятия в области безопасности информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их безопасность.	
	3. Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности	
	4. Принципы обеспечения безопасности информационных технологий. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.	
	5. Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры.	
	6. Государственная система защита информации. 7.Организация защиты информации в системах и средствах информатизации и связи. 8.Контроль состояния защиты информации.	
	9 Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей. 10.Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. 11Регистрация и оперативное оповещение о событиях безопасности.	
	Тематика практических занятий и лабораторных работ	**14**
	1. Сканирование логических дисков с помощью СПО ЗИ (например, РЕВИЗОР-1ХР)	2
	2. Получение списка пользователей с помощью СПО ЗИ (например, РЕВИЗОР-1ХР)	2

	3. Создание отчетов на базе СПО ЗИ (например, РЕВИЗОР-1ХР)	2
	4. Установка прав доступа с помощью СПО ЗИ (например, РЕВИЗОР-1ХР)	2
	5. Считывание прав доступа с помощью СПО ЗИ (например, РЕВИЗОР-1ХР)	2
	6. Сканирования дерева ресурсов с помощью СПО ЗИ (например, РЕВИЗОР-1ХР)	2
	7. Регистрация пользователей с помощью СПО ЗИ (например, РЕВИЗОР-1ХР)	2
	Самостоятельная работа	
	Контрольная работа №1 ВКР	
Тема 1.2. Обеспечение безопасности информационных технологий	**Содержание**	**44 (34/10)**
	1. Понятие технологии обеспечения безопасности информации. Влияние на безопасность со стороны руководства организаций. 2. Институт ответственных за обеспечение безопасности ИТ.	34
	3. Обязанности пользователей и ответственных за обеспечение безопасности ИТ. Общие правила обеспечения безопасности ИТ при работе сотрудников. 4. Ответственность за нарушения. Порядок работы с носителями ключевой информации.	
	5. Документы, регламентирующие правила парольной и антивирусной защиты. Инструкция по организации парольной защиты. 6. Инструкция по организации антивирусной защиты.	
	7. Документы, регламетирующие порядок допуска к работе и изменения полномочий пользователей. Регламентация допуска сотрудников. 8. Правила именования пользователей. Процедур авторизации сотрудников.	
	9. Порядок изменения конфигурации программно-аппаратных средств. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированной системы. Экстренная модификация.	
	10 Регламентация процессов разработки, внедрения и сопровождения задач. Взаимодействие подразделений на всех этапах внедрения автоматизированных подсистем.	
	11. Определение требований к защите и категорирование ресурсов. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. 12 Категорирование защищаемых ресурсов. Проведение информационных обследований и документирование защищаемых ресурсов.	
	13. Планы защиты и планы обеспечения непрерывной работы и восстановления. Составные части планов защиты и обеспечения непрерывной работы. 14Средства обеспечения непрерывной работы. Обязанности и действия персонала по обеспечению непрерывной работы.	
	15. Основные задачи подразделений обеспечения безопасности ИТ. Организационная структура подразделения безопасности. 16Организационно-правовой статус службы обеспечения безопасности информации.	
	17. Концепция безопасности информационных технологий предприятия. Назначение и статус документа. Вопросы, которые должны быть отражены в Концепции.	

	Тематика практических занятий и лабораторных работ	**10**
	8. Установка и снятие СЗИ с помощью программы СЗИ НСД (например, Страж NT)	2
	9. Исследование программной среды с помощью СЗИ НСД (например, Страж NT)	2
	10. Исследование возможностей управления пользователями с помощью СЗИ НСД (например, Страж NT)	2
	11. Исследование учета пользователей и контроля устройств с помощью СЗИ НСД (например, Страж NT)	2
	12. Исследование избирательного управления с помощью СЗИ НСД (например, Страж NT)	2
	Самостоятельная работа	
	Контрольная работа №2 ОКР	
	Контрольная работа №3 ДКР	
ИТОГО за I семестр		**80 (56/24/)**
Тема 1.3. Средства защиты информации от несанкционированного доступа	**Содержание**	**80 (56/24)**
	1. Назначение и возможности средств защиты информации от НСД.	56
	2. Назначение и возможности средств защиты информации от НСД.	
	3. Защита от вмешательства в процесс функционирования АС посторонних лиц.	
	2. Регистрация действий пользователей.	
	5. Обеспечение аутентификации абонентов.	
	6. Рекомендации по выбору средств защиты информации от НСД.	
	7. Распределение показателей защищенности по классам для автоматизированных систем.	
	8. Требования руководящих документов ФСТЭК к средствам защиты информации.	
	9. Требования руководящих документов ФСТЭК к средствам защиты информации.	
	10. Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации (например, DALLASLOCK)	
	11. Назначение, состав и возможности СЗИ (например, «Блокпост-2000».)	
	12. Назначение, состав и возможности СЗИ (например, «Блокхост-сеть».)	
	13. Назначение и особенности применения СЗИ НСД	
	14. Назначение и особенности применения СЗИ НСД (например, «Страж NT»)	
	15. Назначение и специфика применения комплекса ЗИ	
	16. Назначение и специфика применения комплекса ЗИ (например, «Соболь»)	
	17. Устройства аутентификации на базе смарт-карт и USB-токенов.	

	18. Реализация схем аутентификации.	
	19. Программные средства, реализующие инфраструктуру открытых ключей.	
	20. Программные средства, реализующие инфраструктуру открытых ключей.	
	21. Назначение и функциональные возможности eToken и Рутокен.	
	22. Алгоритм генерации одноразовых паролей.	
	23. Формирование электронной цифровой подписи.	
	24. Вычисление ключа согласования Диффи-Хеллмана.	
	25. Особенности разграничения доступа к ресурсам системы.	
	26. Избирательное разграничение доступа..	
	27. Полномочное разграничение доступа	
	28. Регистрация событий, имеющих отношение к безопасности	
	Тематика практических занятий и лабораторных работ	**24**
	13. Ввод информации в САПР СЗИ (например, «Гроза-К»)	2
	14. Расчет радиуса контролируемой зоны с помощью САПР СЗИ (например, «Гроза-К»)	2
	15. Исследование защищенности с помощью САПР СЗИ (например, «Гроза-К»)	2
	16. Формирование и вывод проекта протокола в САПР СЗИ (например, «Гроза-К»)	2
	17. Исследование плана тестирования при помощи СПО ЗИ (например, «Ревизор-2ХР»)	2
	18. Исследование режима тестирования при помощи СПО ЗИ (например, «Ревизор-2ХР»)	2
	19. Исследование содержимого текущего диска с помощью СПО ЗИ (например, «Terrier»)	2
	20.Исследование содержимого текущего диска с помощью СПО ЗИ (например, «Terrier»)	2
	21.Исследование механизма доступа в систему с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	22.Исследование механизма доступа в систему с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	23. Исследование механизма разграничения доступа с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	24.Исследование механизма разграничения доступа с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	Самостоятельная работа	
	Контрольная работа №1 ВКР	
	Контрольная работа №2 ОКР	
	Контрольная работа №3 ДКР	
ИТОГО за II семестр		**80 (56/24)**
ИТОГО за год		**160**

		(112/48)
Тема 1.4. Обеспечение безопасности компьютерных систем и сетей	**Содержание**	**62 (36/26)**
	1.Проблемы обеспечения безопасности в компьютерных системах и сетях.	36
	2.Типовая корпоративная сеть.	
	3. Уязвимости и их классификация.	
	4. Назначение, возможности и защитные механизмы межсетевых экранов.	
	5. Угрозы, связанные с периметром сети.	
	6. Типы межсетевых экранов.	
	7. Сертификация межсетевых экранов.	
	8. Анализ содержимого почтового и WEB-трафика. HTTP-трафик.	
	9. Виртуальные частные сети. Решение на базе ОС Windows.	
	10.VPN на основе криптошлюза (например, «Континент-К»)	
	11. Обнаружение и устранение уязвимостей.	
	12. Архитектура систем управления уязвимостями	
	13.Особенности сетевых агентов сканирования..	
	14. Специализированный анализ защищенности	
	15. Обзор средств анализа защищенности.	
	16. Мониторинг событий безопасности.	
	17. Инфраструктура управления журналами событий.	
	18. Категории журналов событий. Введение в технологию обнаружения атак. Классификация систем обнаружения атак.	
	Тематика практических занятий и лабораторных работ	**26**
	25.Исследование механизма контроля и регистрации с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	26Исследование механизма контроля и регистрации с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	27 Исследование функции отслеживания событий НСД с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	28 Исследование функции отслеживания событий НСД с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	29 Исследование возможности обновления клиента с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	30 Исследование возможности обновления клиента с использованием СПО ЗИ и УП (например, «SecretNet»)	2

	31 Исследование возможности обновления клиента с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	32 Исследование порядка удаления клиента с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	33 Исследование порядка удаления клиента с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	34 Исследование порядка удаления клиента с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	35 Исследование проблемных ситуаций с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	36 Исследование проблемных ситуаций с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	37 Исследование проблемных ситуаций с использованием СПО ЗИ и УП (например, «SecretNet»)	2
	Самостоятельная работа	
	Контрольная работа №1 ВКР	
	Контрольная работа №2 ОКР	
	Контрольная работа №3 ДКР	
ИТОГО за I семестр		**62(36/26)**
ИТОГО за год		**62(36/26)**
ВСЕГО		**222 (148/74)**
Самостоятельная работа при изучении раздела 1 ПМ 03. - Дополнительное конспектирование материала по темам из рекомендуемой преподавателем литературы. - Самостоятельное изучение постановлений правительства, законов и других руководящих документов в области защиты информации. - Изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности. - Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации. **Примерная тематика внеаудиторной самостоятельной работы:** 1. Составление доклада по перспективе и направлению развития программно-аппаратных средств защиты информации на основе публикаций в периодической специализированной аппаратуре. 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.		**4**

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов
1	2	3
Раздел 2. **Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи**		**222**
МДК 03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи		**222**
Тема 2.1. Основы информационной безопасности	**Содержание**	**24**
	1. Основные понятия информационной безопасности. Сущность и понятия защиты информации.	**2**
	2. Значение информационной безопасности и ее место в системе национальной безопасности.	**2**
	3. Основные составляющие национальных интересов Российской Федерации в информационной сфере.	**2**
	4. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.	**2**
	5. Виды и источники угроз информационной безопасности Российской Федерации.	**2**
	6. Органы по технической защите информации в РФ	**2**
	7. Доктрина информационной безопасности Российской Федерации.	**2**
	8. Состояние информационной безопасности РФ и основные задачи по ее обеспечению.	**2**
	9. Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности.	**2**
	10. Построения системы информационной безопасности.	**2**
	11. Защита информации в информационных системах и компьютерных сетях.	**2**
	12. Обеспечение интегральной безопасности.	**2**
	Лабораторные работы- не предусмотрены	**-**
	Практические занятия	**20**
	1. Исследование возможностей профессионального нелинейного радиолокатора (например, NR-900EMS)	**2**
	2. Исследование возможностей профессионального нелинейного радиолокатора (например, NR-900EMS)	**2**
	3.Исследование возможностей многофункционального поискового прибора (например, ST 033P Пиранья)	**2**

	4. Исследование возможностей многофункционального поискового прибора (например, ST 033P Пиранья)	**2**
	5. Исследование возможностей анализатора спектра (например, OSCORGreen-8)	**2**
	6. Исследование возможностей анализатора спектра (например, OSCORGreen-8)	**2**
	7. Исследование возможностей имитатора источника радиосигналов с различными видами модуляции (например, АВРОРА-3)	**2**
	8. Исследование возможностей имитатора источника радиосигналов с различными видами модуляции (например, АВРОРА-3)	**2**
	9. Исследование возможностей комплекса обнаружения радиоизлучающих средств и радиомониторинга (например, КРОНА-ПРО)	**2**
	10. Исследование возможностей комплекса обнаружения радиоизлучающих средств и радиомониторинга (например, КРОНА-ПРО)	**2**
	Самостоятельная работа	
	Контрольные работы – не предусмотрены	**-**
Тема 2.2. Организационно-правовые аспекты защиты информации	**Содержание**	**14**
	1. Структура правовой защиты информации. Система документов в области защиты информации.	**2**
	2. Организационные основы защиты информации. Принципы организационной защиты информации.	**2**
	3. Государственные регуляторы в области защиты информации, их полномочия и сфера компетенции.	**2**
	4. Обзор стандартов и методических документов в области защиты информации. Регулирующие организации в области защиты информации.	**2**
	5. Классификация информации по категориям доступа. Критерии оценки информации. Категории нарушений по степени важности.	**2**
	6. Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность.	**2**
	7. Виды ответственности за правонарушения в информационной сфере.	**2**
	Лабораторные работы- не предусмотрены	**-**
	Практические занятия	**12**
	1. Исследование возможностей скоростного приемника сигналов (например, СКОРПИОН-XL)	**2**
	2. Исследование возможностей скоростного приемника сигналов (например, СКОРПИОН-XL)	**2**
	3. Исследование принципов работы индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165)	**2**
	4. Исследование принципов работы индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165)	**2**

	5. Исследование возможностей работы фильтров сетевых помехоподавляющих (например, ЛФС-10-1Ф и ФСП-1Ф-10А) и исследование работы генератора шума для защиты от ПЭМИН (например, ЛГШ-501)	**2**
	6.Исследование возможностей работы фильтров сетевых помехоподавляющих (например, ЛФС-10-1Ф и ФСП-1Ф-10А) и исследование работы генератора шума для защиты от ПЭМИН (например, ЛГШ-501)	**2**
	Самостоятельная работа	
	Контрольные работы	1
Тема 2.3.Комплексная система защиты информации	**Содержание**	**20**
	1. Общая характеристика комплексной защиты информации. Основы обеспечения комплексной защиты информации. Сущность и задачи комплексной защиты информации.	**2**
	2. Стратегии комплексной защиты информации. Структура и основные характеристики комплексной защиты информации.	**2**
	3. Конфиденциальные сведения. Виды конфиденциальной информации.	**2**
	4. Персональные данные. Коммерческая тайна. Банковская тайна.	**2**
	5. Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны.	**2**
	6. Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение.	**2**
	7. Способы и средства обнаружения угроз. Комплексное обследования защищенности информационной системы.	**2**
	8. Способы и средства обнаружения угроз. Средства нейтрализации угроз.	**2**
	9. Требования и рекомендации по защите информации	**2**
	10. Объект информатизации. Классификация объектов защиты	**2**
	Лабораторные работы- не предусмотрены	**-**
	Практические занятия	**12**
	1. Разработка комплексной системы инженерно-технической защиты информации на объекте.	**2**
	2. Разработка комплексной системы инженерно-технической защиты информации на объекте.	**2**
	3. Исследование возможностей устройства для защиты объектов информатизации (например, СОНАТА-Р2, САЛЮТ 2000Б).	**2**
	4. Исследование возможностей устройства для защиты объектов информатизации (например, СОНАТА-Р2, САЛЮТ 2000Б).	**2**
	5. Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств (например, ПРОКРУСТ-2000)	**2**

	6. Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств (например, ПРОКРУСТ-2000)	**2**
	Самостоятельная работа	
	Контрольные работы – не предусмотрены	-
Тема 2.4. Инженерно-техническая защита информации	**Содержание**	**42**
	1. Основы инженерно-технической защиты информации. Подразделения технической защиты информации и их основные задачи.	2
	2. Основы инженерно-технической защиты информации. Механические системы защиты.	2
	3. Понятие несанкционированного доступа к защищаемой информации. Понятие НСД к информации. Виды НСД к информации.	**2**
	4. Технические каналы утечки информации. Общая структура канала утечки информации.	**2**
	5. Технические каналы утечки информации. Классификация каналов утечки информации.	**2**
	6. Основные способы и средства НСД к защищаемой информации. Активные способы НСД к информации.	**2**
	7. Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД.	**2**
	8. Обеспечение безопасности телефонных переговоров. Противодействие незаконному подключению к линиям связи.	**2**
	9. Обеспечение безопасности телефонных переговоров. Противодействие контактному и бесконтактному подключению.	**2**
	10. Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации.	**2**
	11. Защита от перехвата. Защита информации в каналах связи.	**2**
	12. Акустический контроль. Понятие разборчивости речи при перехвате информации.	**2**
	13. Акустический контроль. Способы и средства информационного скрытия речевой информации от подслушивания.	**2**
	14. Демаскирующие признаки закладных устройств. Классификация средств обнаружения и локализации закладных устройств и их излучений.	**2**
	15. Демаскирующие признаки закладных устройств. Классификация средств обнаружения неизлучающих закладок.	**2**
	16. Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных ли-	**2**

	ний и цепей электропитания и заземления. Принципы контроля цепей электропитания.	
	17. Контроль слаботочных цепей. Принципы контроля линий заземления.	**2**
	18. Средства нелинейной радиолокации. Принципы работы устройств нелинейной радиолокации.	**2**
	19. Средства нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации.	**2**
	20. Методы поиска радиоизлучений закладных устройств. Индикаторы поля. Обнаружение радиоизлучений.	**2**
	21. Методы поиска радиоизлучений закладных устройств. Панорамные радиоприемники. Сканирующие приемники.	**2**
	Лабораторные работы- не предусмотрены	**-**
	Практические занятия	**28**
	1. Исследование возможностей автоматизированной системы изменений сверхмалых величин (например, ТАЛИС-НЧ-ЛАЙТ)	**2**
	2. Исследование возможностей автоматизированной системы изменений сверхмалых величин (например, ТАЛИС-НЧ-ЛАЙТ)	**2**
	3. Исследование технических средств и отходящих от них линий с помощью системы измерений сверхмалых величин (например, ТАЛИС-НЧ-ЛАЙТ)	**2**
	4. Исследование технических средств и отходящих от них линий с помощью системы измерений сверхмалых величин (например, ТАЛИС-НЧ-ЛАЙТ)	**2**
	5. Исследование возможностей системы оценки защищенности оптических линий связи (например, ЛАЗУРИТ)	**2**
	6. Исследование возможностей системы оценки защищенности оптических линий связи (например, ЛАЗУРИТ)	**2**
	7. Измерение параметров ВОСП с помощью системы оценки защищенности оптических линий связи (например, ЛАЗУРИТ)	**2**
	8. Измерение параметров ВОСП с помощью системы оценки защищенности оптических линий связи (например, ЛАЗУРИТ)	**2**
	9. Оценка защищённости с использованием системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН, измерение параметров и расчет показателей защищенности технического средства (например, СИГУРД-М19)	**2**
	10. Оценка защищённости с использованием системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН, измерение параметров и расчет показателей защищенности технического средства (например, СИГУРД-М19)	**2**
	11. Измерение уровня звукового давления вблизи и на удалении от источника с помощью комплекса оценки защищенности выделенных помещений (например, ШЕПОТ)	**2**

	12. Измерение уровня звукового давления вблизи и на удалении от источника с помощью комплекса оценки защищенности выделенных помещений (например, ШЕПОТ)	**2**
	13. Измерение уровня виброускорения в ограждающих конструкциях. Расчет и оценка защищенности помещения по акустическому каналу (например, с помощью комплекса ШЕПОТ)	**2**
	14. Измерение уровня виброускорения в ограждающих конструкциях. Расчет и оценка защищенности помещения по акустическому каналу (например, с помощью комплекса ШЕПОТ)	**2**
	Самостоятельная работа	
	Контрольные работы – не предусмотрены	**-**
Тема 2.5. Криптографическая защита информации	**Содержание**	**10**
	1. Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных.	**2**
	2. Симметричные криптосистемы. Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования	**2**
	3. Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	**2**
	4. Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие криптоанализа.	**2**
	5. Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC.	**2**
	Лабораторные работы- не предусмотрены	**-**
	Практические занятия	**10**
	1. Поиск и локализация скрытых видеокамер (например, с помощью прибора ОПТИК-2)	**2**
	2. Исследование методов защиты сотовых телефонов от несанкционированного прослушивания (например с помощью изделия Ладья-ИВТ)	**2**
	3. Исследование методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов (например, с помощью устройства КЕДР-1М)	**2**
	4. Поиск устройств негласного съема информации с помощью профессионального нелинейного радиолокатора (например, с помощью NR-900EMS)	**2**
	5. Оценка защищенности помещения с помощью многофункционального поискового прибора (например, ST 033P Пиранья)	**2**
	Самостоятельная работа	
	Контрольные работы – не предусмотрены	**-**

Тема 2.6. Аттестация и лицензирование объектов защиты	**Содержание**	**6**
	1. Общие вопросы по аттестации ОИ по требованиям безопасности информации. Основные стадии создания системы защиты информации на ОИ.	**2**
	2. Порядок проведения аттестации объектов информатизации. Организационная структура системы аттестации объектов информатизации.	**2**
	3.Порядок проведения аттестации объектов информатизации. Программа и методика проведения аттестационных испытаний. Лицензирование деятельности в области защиты конфиденциальной информации. Документы, разрабатываемые на объектах информатизации. Документы, разрабатываемые на аттестуемое помещение. Порядок действий при лицензировании.	**2**
	Лабораторные работы- не предусмотрены	**-**
	Практические занятия	**12**
	1. Обнаружение, идентификация и локализация цифровых радиопередающих устройств с помощью индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165)	**2**
	2.Обнаружение, идентификация и локализация цифровых радиопередающих устройств с помощью индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165)	**2**
	3. Исследование работы генератора шума по сети электропитания и линиям заземления (например, ЛГШ-221)	**2**
	4. Исследование работы генератора шума по сети электропитания и линиям заземления (например, ЛГШ-221)	**2**
	5. Поиск и обнаружение радиоизлучающих средств (например, с помощью комплекса КРОНА-ПРО)	**2**
	6. Поиск и обнаружение радиоизлучающих средств (например, с помощью комплекса КРОНА-ПРО)	**2**
	Самостоятельная работа	
	Контрольные работы	
Самостоятельная работа при изучении раздела 2 ПМ 03.: - изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере; - ознакомление с нормативными документами по ИБ; - изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности; - составление доклада по перспективным направлениям развития средств комплексной защиты информации; - разработка пакета документации по инженерно-технической защите информации на объекте; - изучение возможностей инженерно-технических средств защиты информации; - изучение технических характеристик инженерно-технических средств защиты информации; - разработка предложений по инженерно-технической защите информации на определенном объекте; - составление списка уязвимостей предложенного объекта. Самостоятельная разработка комплекта документации на объекте информатизации.		**6**

Учебная практика (по профилю специальности) по ПМ 03 **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.	**72**
Производственная практика (по профилю специальности) по ПМ **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 (экзамен)	**6**
Всего	**604-**

2.3. Содержание домашних заданий обучающихся

Наименование темы	Содержание домашнего задания
Тема 1.1.Основы безопасности информационных технологий	1.Составление доклада по перспективе и направлению развития программно-аппаратных средств защиты информации на основе публикаций в периодической специализированной аппаратуре. 2. Практическое применение антивирусных программ для защиты информации от несанкционированного доступа.
Тема 1.2. Обеспечение безопасности информационных технологий	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.
Тема 1.3. Средства защиты информации от несанкционированного доступа	5. Применение программно-аппаратных средств для обеспечения разграничения доступа к защищаемой информации. 6. Разработка комплекса организационно-административной защиты от вредоносных программ.
Тема 1.4. Обеспечение безопасности компьютерных систем и сетей	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.
Тема 2.1. Основы информационной безопасности	9.Изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере; 10 ознакомление с нормативными документами по ИБ;
Тема 2.2. Организационно-правовые аспекты защиты информации	11 составление доклада по перспективным направлениям развития средств комплексной защиты информации;
Тема 2.3.Комплексная система защиты информации	12 составление доклада по перспективным направлениям развития средств комплексной защиты информации;
Тема 2.4. Инженерно-техническая защита информации	13 составление доклада по перспективным направлениям развития средств комплексной защиты информации;
Тема 2.5. Криптографическая защита информации	14.разработка пакета документации по инженерно-технической защите информации на объекте; 15 изучение возможностей инженерно-технических средств защиты информации;
Тема 2.6. Аттестация и лицензирование объектов защиты	16 изучение технических характеристик инженерно-технических средств защиты информации; 17 разработка предложений по инженерно-технической защите информации на определенном объект.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Кабинет «Основы компьютерного моделирования», «Тестирование цифровых устройств», оснащенный оборудованием:

– компьютеры в комплекте (системный блок, монитор, клавиатура, манипулятор «мышь») или ноутбуки (моноблоки),
– локальная сеть с выходом в Интернет,
– комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном)
– программное обеспечение (системы электротехнического моделирования).

Оснащенные базы практики, в соответствии с п 6.2.3 Примерной программы по специальности 11.02.15.

3.2. Информационное обеспечение реализации программы

3.2.1. Печатные издания

1. Арутюнов, В. В. Защита информации : учебно-методическое пособие / В. В. Арутюнов. - Москва : Либерея-Бибинформ, 2016. - 55, [1] с. : рис. ; 21 см. - (Библиотекарь и время. XXI век ; № 99). - ISBN 5-85129-175-3

2. Васильков А. В., Васильков А. А., Васильков И. А. Информационные системы и их безопасность: Учебное пособие. - М.: Форум, 2016. - 528 с.: 60x90 1/16. - (Профессиональное образование) (Переплёт) ISBN 978-5-91134-289-0

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

3.2.2. Электронные издания (электронные ресурсы)

1.

3.2.3. Дополнительные источники

Научно-технические и реферативные журналы:

1. Электросвязь
2. Вестник связи
3. Сети и системы связи
4. Мобильные системы
5. Цифровая обработка сигналов
6. Сводный реферативный журнал "Связь".

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 за-

		дач, 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 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;	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

ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЕННЫХ В РАБОЧУЮ ПРОГРАММУ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

№ изменения, дата изменения; № страницы	Основания изменения	Было	Стало	Подпись
№1 24.06.2021	О внесении изменений в Федеральный закон «Об образовании в Российской Федерации» по вопросам воспитания обучающихся: Федеральный закон от 31.07.2020. № 304-ФЗ, О внедрении примерной программы воспитания: Письмо Министерства просвещения РФ от 04.08.2020 № ДГ-1249/06	-	Рабочая программа воспитания колледжа. Внедрены личностные результаты воспитания ЛР 1 –ЛР 23	
№2 01.09.2022 стр.	Письмо Министерства просвещения РФ от 18.07.2022 №АБ-1951/06 Об актуализации примерной рабочей программы воспитания. Программа воспитания колледжа, утвержденная 01.09.2022 г.	Рабочая программы воспитания колледжа, рабочая программа воспитания специальностей. (Приложение 1)	Актуализация рабочей программы воспитания колледжа, рабочих программ воспитания специальностей. Изменены ЛР. (Приложение 1)	
№3 26.10.2022 с. 12	В связи с переходом 26.10.2022 г. на новую Образовательную платформу «Юрайт» (договор № 8528 от «12» августа 2022 г.) Протокол №1 от 30.08.2022	Электронно-библиотечная система издательского центра «Академия» http://academia-moscow.ru/	Образовательная платформа «Юрайт» https://urait.ru/.	

Приложение 1

Было

Личностные результаты реализации программы воспитания	**Код личностных результатов реализации программы воспитания**
Осознающий себя гражданином и защитником великой страны	**ЛР 1**
Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций	**ЛР 2**
Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих	**ЛР 3**
Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»	**ЛР 4**
Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России	**ЛР 5**
Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях	**ЛР 6**
Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности	**ЛР 7**
Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства	**ЛР 8**
Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях	**ЛР 9**
Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой	**ЛР 10**
Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры	**ЛР 11**
Принимающий семейные ценности, 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 12**

Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности	
Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации	**ЛР 13**
Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм	**ЛР 14**
Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.	**ЛР 15**
Личностные результаты реализации программы воспитания, определенные субъектом Российской Федерации	
Использовать информационные технологии в профессиональной деятельности	**ЛР 16**
Пользоваться профессиональной документацией на государственном и иностранном языке	**ЛР 17**
Личностные результаты реализации программы воспитания, определенные ключевыми работодателями	
Креативно мыслящий, готовый разрабатывать новые виды продукции	**ЛР 18**
Активно применяющий полученные знания на практике	**ЛР 19**
Способный анализировать производственную ситуацию, быстро принимать решения	**ЛР 20**
Личностные результаты реализации программы воспитания, определенные субъектами образовательного процесса	
Креативно мыслящий, готовый разрабатывать новые виды продукции	**ЛР 21**
Способный анализировать производственную ситуацию, быстро принимать решения	**ЛР 22**
Проявлять доброжелательность к окружающим, деликатность, чувство такта и готовность оказать услугу каждому кто в ней нуждается	**ЛР 23**

Стало

Личностные результаты реализации программы воспитания *(дескрипторы)*	**Код личностных результатов реализации программы воспитания**
Осознающий себя гражданином России и защитником Отечества, выражающий свою российскую идентичность в поликультурном и многоконфессиональном российском обществе и современном мировом сообществе. Сознающий свое единство с народом России, с Российским государством, демонстрирующий ответственность за развитие страны. Проявляющий готовность к защите Родины, способный аргументированно отстаивать суверенитет и достоинство народа России, сохранять и защищать историческую правду о Российском государстве	**ЛР 1**
Проявляющий активную гражданскую позицию на основе уважения закона и правопорядка, прав и свобод сограждан, уважения к историческому и культурному наследию России. Осознанно и деятельно выражающий неприятие дискриминации в обществе	**ЛР 2**

по социальным, национальным, религиозным признакам; экстремизма, терроризма, коррупции, антигосударственной деятельности. Обладающий опытом гражданской социально значимой деятельности (в студенческом самоуправлении, добровольчестве, экологических, природоохранных, военно-патриотических и др. объединениях, акциях, программах). Принимающий роль избирателя и участника общественных отношений, связанных с взаимодействием с народными избранниками	
Демонстрирующий приверженность традиционным духовно-нравственным ценностям, культуре народов России, принципам честности, порядочности, открытости. Действующий и оценивающий свое поведение и поступки, поведение и поступки других людей с позиций традиционных российских духовно-нравственных, социокультурных ценностей и норм с учетом осознания последствий поступков. Готовый к деловому взаимодействию и неформальному общению с представителями разных народов, национальностей, вероисповеданий, отличающий их от участников групп с деструктивным и девиантным поведением. Демонстрирующий неприятие социально опасного поведения окружающих и предупреждающий его. Проявляющий уважение к людям старшего поколения, готовность к участию в социальной поддержке нуждающихся в ней	**ЛР 3**
Проявляющий и демонстрирующий уважение к труду человека, осознающий ценность собственного труда и труда других людей. Экономически активный, ориентированный на осознанный выбор сферы профессиональной деятельности с учетом личных жизненных планов, потребностей своей семьи, российского общества. Выражающий осознанную готовность к получению профессионального образования, к непрерывному образованию в течение жизни Демонстрирующий позитивное отношение к регулированию трудовых отношений. Ориентированный на самообразование и профессиональную переподготовку в условиях смены технологического уклада и сопутствующих социальных перемен. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»	**ЛР 4**
Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, народу, малой родине, знания его истории и культуры, принятие традиционных ценностей многонационального народа России. Выражающий свою этнокультурную идентичность, сознающий себя патриотом народа России, деятельно выражающий чувство причастности к многонациональному народу России, к Российскому Отечеству. Проявляющий ценностное отношение к историческому и культурному наследию народов России, к национальным символам, праздникам, памятникам, традициям народов, проживающих в России, к соотечественникам за рубежом, поддерживающий их заинтересованность в сохранении общероссийской культурной идентичности, уважающий их права	**ЛР 5**
Ориентированный на профессиональные достижения, деятельно выражающий познавательные интересы с учетом своих способностей, образовательного и профессионального маршрута, выбранной квалификации	**ЛР 6**
Осознающий и деятельно выражающий приоритетную ценность каждой человеческой жизни, уважающий достоинство личности каждого человека, собственную и чужую уникальность, свободу мировоззренческого	**ЛР 7**

выбора, самоопределения. Проявляющий бережливое и чуткое отношение к религиозной принадлежности каждого человека, предупредительный в отношении выражения прав и законных интересов других людей	
Проявляющий и демонстрирующий уважение законных интересов и прав представителей различных этнокультурных, социальных, конфессиональных групп в российском обществе; национального достоинства, религиозных убеждений с учётом соблюдения необходимости обеспечения конституционных прав и свобод граждан. Понимающий и деятельно выражающий ценность межрелигиозного и межнационального согласия людей, граждан, народов в России. Выражающий сопричастность к преумножению и трансляции культурных традиций и ценностей многонационального российского государства, включенный в общественные инициативы, направленные на их сохранение	**ЛР 8**
Сознающий ценность жизни, здоровья и безопасности. Соблюдающий и пропагандирующий здоровый образ жизни (здоровое питание, соблюдение гигиены, режим занятий и отдыха, физическая активность), демонстрирующий стремление к физическому совершенствованию. Проявляющий сознательное и обоснованное неприятие вредных привычек и опасных наклонностей (курение, употребление алкоголя, наркотиков, психоактивных веществ, азартных игр, любых форм зависимостей), деструктивного поведения в обществе, в том числе в цифровой среде	**ЛР 9**
Бережливо относящийся к природному наследию страны и мира, проявляющий сформированность экологической культуры на основе понимания влияния социальных, экономических и профессионально-производственных процессов на окружающую среду. Выражающий деятельное неприятие действий, приносящих вред природе, распознающий опасности среды обитания, предупреждающий рискованное поведение других граждан, популяризирующий способы сохранения памятников природы страны, региона, территории, поселения, включенный в общественные инициативы, направленные на заботу о них	**ЛР 10**
Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры. Критически оценивающий и деятельно проявляющий понимание эмоционального воздействия искусства, его влияния на душевное состояние и поведение людей. Бережливо относящийся к культуре как средству коммуникации и самовыражения в обществе, выражающий сопричастность к нравственным нормам, традициям в искусстве. Ориентированный на собственное самовыражение в разных видах искусства, художественном творчестве с учётом российских традиционных духовно-нравственных ценностей, эстетическом обустройстве собственного быта. Разделяющий ценности отечественного и мирового художественного наследия, роли народных традиций и народного творчества в искусстве. Выражающий ценностное отношение к технической и промышленной эстетике	**ЛР 11**
Принимающий российские традиционные семейные ценности. Ориентированный на создание устойчивой многодетной семьи, понимание брака как союза мужчины и женщины для создания семьи, рождения и воспитания детей, неприятия насилия в семье, ухода от родительской ответственности, отказа от отношений	**ЛР 12**

со своими детьми и их финансового содержания	
Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности	
Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации	**ЛР 13**
Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм	**ЛР 14**
Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности.	**ЛР 15**
Личностные результаты реализации программы воспитания, определенные субъектом Российской Федерации	
Использовать информационные технологии в профессиональной деятельности	**ЛР 16**
Пользоваться профессиональной документацией на государственном и иностранном языке	**ЛР 17**
Личностные результаты реализации программы воспитания, определенные ключевыми работодателями	
Креативно мыслящий, готовый разрабатывать новые виды продукции	**ЛР 18**
Активно применяющий полученные знания на практике	**ЛР 19**
Способный анализировать производственную ситуацию, быстро принимать решения	**ЛР 20**
Личностные результаты реализации программы воспитания, определенные субъектами образовательного процесса	
Креативно мыслящий, готовый разрабатывать новые виды продукции	**ЛР 21**
Способный анализировать производственную ситуацию, быстро принимать решения	**ЛР 22**
Проявлять доброжелательность к окружающим, деликатность, чувство такта и готовность оказать услугу каждому кто в ней нуждается	**ЛР 23**