МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ САМАРСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ «ГУБЕРНСКИЙ КОЛЛЕДЖ Г. СЫЗРАНИ»

УТВЕРЖДЕНО

Приказ ГБПОУ «ГК г. Сызрани»
от « 16 » мая 2022 г. № 250-о

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

основной образовательной программы
по специальности:

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Сызрань, 2022 г.

РАССМОТРЕНА

Предметной (цикловой) комиссией

общепрофессиональных и

профессиональных циклов

Председатель Киреева М.В.

от «27» 04 2022 г. протокол № 8

СОГЛАСОВАНО

Директор

ООО «ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ»

_____ Д. А. Полоса

от «27» 04 2022 г. протокол № 8

Составитель: М.В. Киреева, преподаватель строительного профиля ГБПОУ «ГК г. Сызрани»

Внутренняя экспертиза (техническая и содержательная):

И.Н. Ежкова, методист строительного профиля ГБПОУ «ГК г. Сызрани»

Рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами разработана на основе ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем утвержденной приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1553.

Рабочая программа разработана с учетом профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», 06.030, утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25.11.2016 N 44449

Рабочая программа ориентирована на подготовку обучающихся к выполнению заданий, соответствующих требованиям регионального чемпионата «Молодые профессионалы» по компетенции Корпоративная защита от внутренних угроз информационной безопасности, требований демонстрационного экзамена по стандартам WorldSkills по компетенции Корпоративная защита от внутренних угроз информационной безопасности.

Рабочая программа разработана в соответствии с требованиями к оформлению, установленными в ГБПОУ «ГК г. Сызрани».

Содержание программы реализуется в процессе освоения обучающимися программы подготовки специалистов среднего звена в соответствии с требованиями ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

1.1. Область применения программы

Рабочая программа профессионального модуля (далее программа – ПМ) является частью основной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем углубленной подготовки, разработанной в ГБПОУ «ГК г. Сызрани».

Рабочая программа составляется для очной формы обучения.

1.2.Цель и задачи модуля – требования к результатам освоения модуля:

По результатам освоения ПМ 03. Защита информации техническими средствами у обучающихся должны быть сформированы образовательные результаты в соответствии с ФГОС СПО:

В результате освоения профессионального модуля студент должен:

Иметь практический опыт	установки, монтажа и настройки технических средств защиты информации; технического обслуживания технических средств защиты информации; применения основных типов технических средств защиты информации; выявления технических каналов утечки информации; участия в мониторинге эффективности технических средств защиты информации; диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физическойзащиты.

уметь	применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации
знать	порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информациии организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защитыинформации; основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации.

Вариативная часть:

По результатам освоения ПМ.03 Защита информации техническими средствами у обучающихся должны быть сформированы вариативные образовательные результаты, ориентированные на выполнение профессионального стандарта.

С целью реализации требований профессионального стандарта 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», 5 уровень квалификации и квалификационных запросов предприятий/ регионального рынка труда, обучающийся должен*:*

иметь практический опыт:

– восстановление процесса функционирования после сбоев и отказов СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД;

– восстановление значений показателей функционирования СССЭ, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты СССЭ от НСД.

уметь:

– проводить предусмотренные регламентом работы по восстановлению процесса и параметров функционирования СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД.

знать:

– последовательность действий в целях восстановления процесса и параметров функционирования СССЭ, а также средств и систем защиты СССЭ от НСД;
– организационные меры по защите информации;
– нормативные правовые акты в области связи, информатизации и защиты информации.

1.3. Количество часов на освоение программы профессионального модуля

Вид учебной деятельности	Объём часов
Объем образовательной программы (всего)	631
Нагрузка во взаимодействии с преподавателем	**622**
В том числе:	
Теоретическое обучение	90
Лабораторные работы и практические занятия	202
Консультации: По МДК 03.01 По МДК 03.02 По МДК 03.03	 6 6 6
Промежуточная аттестация По МДК 03.01 По МДК 03.02 По МДК 03.03	 6 6 6
Курсовая работа (проект) По МДК 03.02	 30
Учебная практика	180
Производственная практика	144
Промежуточная аттестация в форме	экзамена
Консультация к экзамену (квалификационному)	6
Экзамен (квалификационный)	6
Самостоятельная работа студента (всего) в том числе: *работа над курсовым проектом, оформление отчетов к практическим работам*	**9**

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

В результате изучения профессионального модуля обучающиеся должны освоить основной вид деятельности Защита информации техническими средствами и овладеть соответствующими ему профессиональными компетенциями (ПК), указанными в ФГОС СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем, перечень профессиональных компетенций:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	**Защита информации техническими средствами**
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживаниетехнических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

Результатом освоения профессионального модуля является овладение трудовой функцией профессионального стандарта:

-техническое обслуживание СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД.

В процессе освоения ПМ обучающиеся должны овладеть общими компетенциями (ОК):

Код	**Наименование видов деятельности и профессиональных компетенций**
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

3. 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.							Квалификационный экзамен	Самостоятельная работа
			Обучение по МДК, в час.					Практики			
			Теоретическое обучение	Лабораторных и практических занятий	Курсовых работ (проектов)	Консультации	Промежуточная аттестация	Учебная	Производственная (если предусмотрена рассредоточенная практика)		
1	2	3	4	5	6			7	8		9
ПК 3.1-3.2	Раздел 1. Применение технической защиты информации	**150**	36	98		*6*	*6*				4
ПК 3.3.-3.4.	Раздел 2. Применение инженерно-технических средств физической защиты объектов информатизации	**325**	54	104	*30*	*12*	*12*	108			5
	Производственная практика	**144**							144		
	Квалификационный экзамен	**12**								*12*	
	Всего:	***631***	***90***	***202***	***30***	***18***	***18***	***108***	***144***	***12***	***9***

3.2 Содержание обучения по профессиональному модулю

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Применение технической защиты информации			
МДК.03.01 Техническая защита информации			
Тема 1. Концепция инженерно-технической защиты информации			ПК 3.1, 3.2, ОК 01-10
Тема 1.1. Предмет ит задачи технической защиты информации	**Содержание**	**2**	
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защитыинформации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.		
	Лабораторные работы	Не предусмотрено	
	Практические занятия	Не предусмотрено	
Тема 1.2. Общие положения защитыинформации техническими средствами	**Содержание**	**2**	
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципысистемного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.		
	Лабораторные работы	Не предусмотрено	
	Практические занятия	Не предусмотрено	
Тема 2. Теоретические основы инженерно-технической защиты информации			ПК 3.1, 3.2, ОК 01-10
Тема 2.1. Информация как предмет защиты	**Содержание**	**2**	
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носителизащищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Ос-		

	новные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**6**	
	1	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.		
Тема 2.2. Техническиеканалы утечки информации	**Содержание**		**2**	
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**8**	
	2	Изучение устройств обнаружения и локализации закладных устройств для снятия информации		
	3	Тестирование шлейфовых линий для обнаружения несанкционированных подключений		
Тема 2.3. Методы и средства техническойразведки	**Содержание**		**2**	
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**28**	
	4	Изучение, диагностика отказов и практическое использование объемного датчика движения		
	5	Изучение, диагностика отказов датчика охраны границ объекта и его практическое использование		
	6	Изучение автомобильной сигнализации		
	7	Устройство кодового замка, диагностика отказов и восстановление работоспособности.		
	8	Изучение системы охранно- пожарной сигнализации и ее практическое применение.		
	9	Изучение устройства контроля и ограничения доступа.		
	10	Система видеонаблюдения и ее практическое использование		
Тема 3. Физические основы технической защиты информации				ПК 3.1, 3.2,

			ОК 01-10
Тема 3.1. Физические основы утечки информации по каналампобочных электромагнитных излучений и наводок	**Содержание**	**4**	
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочныхэлектромагнитных излучений и наводок, параметров фоновых шумов и физических полей		
	Лабораторные работы	Не предусмотрено	
	Практические занятия	**4**	
	11 Измерение параметров физических полей		
Тема 3.2. Физическиепроцессы при подавлении опасных сигналов	**Содержание**	**2**	
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.		
	Лабораторные работы	Не предусмотрено	
	Практические занятия	Не предусмотрено	
Тема 4. Системы защиты от утечки информации			ПК 3.1, 3.2, ОК 01-10
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**	**2**	
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации.Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации отнесанкционированной утечки по акустическому каналу.		
	Лабораторные работы	Не предусмотрено	
	Практические занятия	**4**	
	12 Защита от утечки по акустическому каналу		
Тема 4.2. Системызащиты от утечки информации по проводному каналу	**Содержание**	**2**	
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.		
	Лабораторные работы	Не предусмотрено	
	Практические занятия	Не предусмотрено	
Тема 4.3. Системы за-	**Содержание**	**2**	

щиты от утечки информации по вибрационному каналу	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средствзащиты информации от несанкционированной утечки по вибрационному каналу.		
	Лабораторные работы	Не предусмотрено	
	Практические занятия	**4**	
	13 Защита от утечки по виброакустическому каналу		
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	**2**	
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок.Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.		
	Лабораторные работы	Не предусмотрено	
	Практические занятия	**8**	
	14 Определение каналов утечки ПЭМИН		
	15 Защита от утечки по цепям электропитания и заземления		
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**2**	
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения ктелефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защитыинформации от несанкционированной утечки по телефонному каналу.		
	Лабораторные работы	Не предусмотрено	
	Практические занятия	**4**	
	16 Защита от утечки по телефонному каналу		
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**2**	
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации.Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.		
	Лабораторные работы	Не предусмотрено	
	Практические занятия	**4**	
	17 Защита от утечки по электросетевому каналу		

Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**		**2**	
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**4**	
	18	Защита от утечки по оптическому каналу		
Тема 5. Применение и эксплуатация технических средств защиты информации				ПК 3.1, 3.2, ОК 01-10
Тема 5.1. Применение технических средств защиты информации	**Содержание**		**4**	
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**10**	
	19	Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.		
	20	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		
Тема 5.2. Эксплуатациятехнических средств защиты информации	**Содержание**		**2**	
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.			
	Практические занятия		**14**	
	21.	Установка и настройка технических средств защиты информации		
	22	Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.		
	23	Организация ремонта технических средств защиты информации		
	24	Проведение аттестации объектов информатизации.		
Самостоятельная работа Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам,главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практическихработ, отчетов к их защите.			4	
Консультации			**6**	

Промежуточная аттестация по МДК.03.01			**6**	
Раздел 2. Применение инженерно-технических средств физической защиты объектов информатизации				
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации				
Тема 1. Построение и основные характеристики инженерно-технических средств физической защиты				ПК 3.3, 3.4, ОК 01-10
Тема 1.1.	**Содержание**		**6**	
Цели и задачи физической защитыобъектов информатизации	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектовинформатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Особенности задач охраны различных типов объектов.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**8**	
	1	Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.		
Тема 1.2. Общие сведения о комплексах инженерно-техническихсредств физической защиты	**Содержание**		**6**	
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты.Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**8**	
	2	Рассмотрение инженерных конструкций, применяемые для предотвращения проникновения злоумышленника к источникам информации.		
Тема 2. Основные компоненты комплекса инженерно-технических средств физической защиты				ПК 3.3, 3.4, ОК 01-10
Тема 2.1 Система обнаружения комплексаинженерно-техническихсредств физической защиты	**Содержание**		**6**	
	Информационные основы построения системы охранной сигнализации. Назначение, классификациятехнических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средстваобнаружения: назначение, устройство, принцип действия.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**10**	
	3	Монтаж датчиков пожарной и охранной сигнализации		

Тема 2.2. Система контроля и управлениядоступом	**Содержание**		**6**	
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийноеоборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов ирадиоактивных веществ.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**10**	
	4	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя		
	5	Рассмотрение принципов устройства, работы и применения средств контроля доступа		
Тема 2.3. Система телевизионного наблюдения	**Содержание**		**4**	
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотныесистемы. Инфракрасные осветители. Детекторы движения.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**8**	
	6	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.		
Тема 2.4. Система сбора,обработки, отображения и документирования информации	**Содержание**		**4**	
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора иобработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**8**	
	7	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.		
Тема 2.5 Система воздействия	**Содержание**		**2**	
	Назначение и классификация технических средств воздействия.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**8**	
	8.	Определение основных показателей технических средств воздействия		

Тема 3. Применение и эксплуатация инженерно-технических средств физической защиты				ПК 3.3, 3.4, ОК 01-10
Тема 3.1 Применение инженерно-техническихсредств физической защиты	**Содержание**		**4**	
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийнымоборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**12**	
	9	Управление системой телевизионного наблюдения с автоматизированного рабочего места.		
	10	Порядок применения устройств отображения и документирования информации.		
	11	Управление системой воздействия		
Тема 3.2. Эксплуатацияинженерно-техническихсредств физической защиты	**Содержание**		**2**	
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно- технических средств физической защиты.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**12**	
	12	Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.		
	13	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.		
	14	Организация ремонта технических средств физической защиты.		
Курсовой проект			**30**	
Примерная тематика курсового проекта (работы) 1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.				
Самостоятельная работа при изучении МДК.03.02 – Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты. – Размещение периметровых средств обнаружения на местности. – Самостоятельнее изучения порядка допуска субъектов на охраняемые объекты.			**5**	

Консультации			**6**	
Промежуточная аттестация по МДК.03.02			**6**	
МДК.03.03 Физические основы защиты информации				
Тема 1. Построение и основные характеристики средств физической защиты				ПК 3.3, 3.4, ОК 01-10
Тема 1.1. Введение. Технические каналы утечки информации. Постановка задачи. Физические основы.	**Содержание**		**10**	
	Физические процессы построения средств защиты от съема информации. Технические средствополучения информации. Задачи физических средств ЗИ. Защита информации от утечки по техническим каналам. Характеристика технических каналов утечкиинформации. Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации. Явления, процессы и действия, выполняемые и существующие при решении задач защиты информациио от утечки по техническим каналам. Характеристики радиоканала передачи информации. Оценка влияния мощности источника излучения(передатчика), влияние передающей антенны, влияние приемника (с оценкой достижимости характеристик по чувствительности, избирательности и другим), влияние приемных антенн. Возможности и ограничения методов защиты от утечки информации основанных на электромагнитномэкранировании, на применении генераторов шума. Методы обнаружения электромагнитных излучений и источников излучений с применением широкополосных индикаторов поля, узкополосных сканирующих приемников, анализаторов спектра,нелинейных локаторов.			
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**12**	
	1	Создание модели ситуаций возникновения утечки информации и описание этих каналов с оценкой их реальности, опасности, дальности действий, требуемых мер по защите		
Тема 1.2. Основы нормативной базы организации защиты информации в Российской федерации	**Содержание**		**-**	
	Лабораторные работы		Не предусмотрено	
	Практические занятия		**6**	
	2	Изучение Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 02.07.2013) "Об информации, информационных технологиях и о защите информации"		
Тема 1.3. Доктрина	**Содержание**		**4**	

информационной безопасности Российской Федерации.	Информационная безопасность Российской Федерации. Методы обеспечения информационной безопасности Российской Федерации. Основные положения государственной политики обеспечения информационной безопасности РФ ипервоочередные мероприятия по ее реализации. Организационная основа системы обеспечения информационной безопасности РФ		
	Лабораторные работы	Не предусмотрено	
	Практические работы	Не предусмотрено	
Консультации		**6**	
Промежуточная аттестация по МДК.03.03		**6**	
Учебная практика Измерение параметров физических полей.Определение каналов утечки ПЭМИН. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защитыинформации. Установка и настройка технических средств защиты информации. Проведение измерений параметров побочных электромагнитных излучений и наводок.Проведение аттестации объектов информатизации. Монтаж различных типов датчиков. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.Рассмотрение системы контроля и управления доступом. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.Рассмотрение датчиков периметра, их принципов работы. Выполнение звукоизоляции помещений системы зашумления. Реализация защиты от утечки по цепям электропитания и заземления. Разработка организационных и технических мероприятий по заданию преподавателя; Разработка основной документации по инженерно-технической защите информации.		***108***	
Производственная практика профессионального модуля **Виды работ** 1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и техническойохраны объектов, систем видеонаблюдения; 3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного		***144***	

съёма и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информациитехническими средствами.		
Экзамен (квалификационный) по профессиональному модулю	***12***	
Всего	***635***	

5. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1 Требования к минимальному материально-техническому обеспечению

Реализация программы ПМ.03 Защита информации техническими средствами требует наличия учебных кабинетов – лекционные аудиториис мультимедийным оборудованием; лаборатории «информационных технологий, программирования и баз данных, сетей и систем передачи информации, программных и программно-аппаратных средств защиты информации».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест – не менее 30, рабочее место преподавателя, проектор, персональныйкомпьютер, интерактивная доска, комплект презентаций.

Оборудование лаборатории «информационных технологий, программирования и баз данных, сетей и систем передачи информации, программных и программно-аппаратных средств защиты информации» и рабочих мест лаборатории:

1) рабочие места студентов, оборудованные персональными компьютерами;
2) лабораторные учебные макеты;
3) аппаратные средства аутентификации пользователя;
4) средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок;
5) средства измерения параметров физических полей;
6) стенд физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов;
7) рабочее место преподавателя;
8) учебно-методическое обеспечение модуля;
9) интерактивная доска, комплект презентаций.

4.2 Информационное обеспечение обучения (перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы)

Основные источники

Для преподавателей

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.

2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.

4. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

6. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012

8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

Для студентов

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.

2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.

4. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

6. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012

8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

Дополнительные источники

Для преподавателей

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

3. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

4. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

5. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

Для студентов

1. Информационно-справочная система по документам в области технической защитыинформации www.fstec.ru

2. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

3. Справочно-правовая система «Консультант Плюс» www.consultant.ru

4. Справочно-правовая система «Гарант» » www.garant.ru

5. Федеральный портал «Российское образование www.edu.ru

6. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

7. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

8. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

9. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

4.3 Общие требования к организации образовательного процесса

Освоение ПМ 03 Защита информации техническими средствами производится в соответствии с учебным планом по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем и календарным графиком, утвержденным директором ОО.

График освоения ПМ 03 Защита информации техническими средствами предполагает последовательное освоение МДК 03.01 Техническая защита информации, МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации, МДК 03.03 Физические основы защиты информации, включающих в себя как теоретические, так и практические занятия.

Освоению ПМ 03 Защита информации техническими средствами предшествует обязательное изучение учебных дисциплин ОП.02 Организационно-правовое обеспечение информационной безопасности.

В процессе освоения ПМ 03 Защита информации техническими средствами предполагается проведение текущего контроля знаний, умений у обучающихся. Выполнение практических занятий работ является обязательной для всех обучающихся. Наличие оценок по практическим занятиям (ПЗ) является для каждого студента обязательным. В случае отсутствия оценок за ПЗ студент не допускается до сдачи квалификационного экзамена по ПМ.

С целью оказания помощи обучающимся при освоении теоретического и практического материала, выполнения самостоятельной работы разрабатываются учебно-методические комплексы для студентов (кейсы студентов).

С целью методического обеспечения прохождения учебной и/или производственной практики (далее - УП/ПП), выполнения курсового проекта/курсовой работы разрабатываются методические рекомендации для студентов по выполнению КР/КП, прохождению УП/ПП.

При освоении ПМ консультации проводятся согласно графика проведения консультаций.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результаты (освоенные профессиональные и общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Фронтальный опрос, беседа, экзамен квалификационный, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Фронтальный опрос, беседа, экзамен квалификационный, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Фронтальный опрос, беседа, экзамен квалификационный, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.4 Осуществлять измерение параметров техническими средствами защиты информации	Проводить самостоятельные измерения техническими средствами защиты информации	Фронтальный опрос, беседа, экзамен квалификационный, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

ПК 3.5 Организовывать отдельные работы по	Проявлять знания в выборе способов решения задач по информатизации	Фронтальный опрос, беседа, экзамен квалификационный, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

6. ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ, ВНЕСЁННЫХ В РАБОЧУЮ ПРОГРАММУ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

№ п/п	Дата внесения изменения	Внесённые изменения	№ страницы

7. ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

Дата актуализации	Результаты актуализации	ФИО и подпись лица, ответственного за актуализацию

ПРИЛОЖЕНИЕ 1
к рабочей программе ПМ
ПМ.03 Защита информации техническими средствами

ПЛАНИРОВАНИЕ УЧЕБНЫХ ЗАНЯТИЙ С ИСПОЛЬЗОВАНИЕМ АКТИВНЫХ И ИНТЕРАКТИВНЫХ ФОРМ И МЕТОДОВ ОБУЧЕНИЯ

№ п/п	Тема учебного занятия	Активные и интерактивные формы и методы обучения	Код формируемыхкомпетенций
1.	Предмет и задачи технической защиты информации.	Урок презентация	ОК 02-04, ПК 3.1
2.	Классификация технических средств разведки.	семинар	ОК 05, ПК 3.1
3.	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.	Решение практической задачи	ПК 3.3, ОК 02, ОК 09
4.	Классификация системы сбора и обработки информации.	Работа в м/группах	ПК 3.3, ОК 02, ОК 09
5.	Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.	Урок с элементами проблемного обучения	ОК 01-ОК 05, ПК 3.2

ПРИЛОЖЕНИЕ 2
к рабочей программе профессионального модуля основной части ФГОС СПО

Ведомость соотнесения требований профессионального стандарта по профессии 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», 5 уровень квалификации и ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Обобщенная трудовая функция (ПРОФЕССИОНАЛЬНЫЙ СТАНДАРТ)	**Вид профессиональной деятельности (ФГОС СПО)**
Формулировка ОТФ: Выполнение комплекса мер по обеспечению функционирования СССЭ (за исключением сетей связи специального назначения) и средств их защиты от НСД	Формулировка ВПД: Защита информации техническими средствами
Трудовые функции	ПК
Техническое обслуживание СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД	ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5.

Результаты, заявленные в профессиональном стандарте	**Технические требования РЧ/ДЭ**	**Образовательные результаты ФГОС СПО по ПМ**
Техническое обслуживание СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД		ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации. ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа. ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации. ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

Результаты, заявленные в профессиональном стандарте	Технические требования РЧ/ДЭ	Образовательные результаты ФГОС СПО по ПМ		
Трудовые действия		**Практический опыт**	**Задания на практику**	**Самостоятельная работа**
Диагностика СССЭ штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами Диагностика программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами Выполнение		Технического обслуживания технических средств защиты информации; установки, монтажа и настройки технических средств защиты информации;применения основных типов технических средств защиты информации; участия в мониторинге эффективности технических средств защиты информации; установки, монтажа и	Измерение параметров физических полей. Определение каналов утечки ПЭМИН. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Установка и настройка технических средств защиты информации. Проведение измерений параметров побочных электромагнитных излучений и наводок. Проведение аттестации объектов информатизации. Монтаж различных типов датчиков. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. Применение промышленных осциллографов, частотомеров и генераторов, и другого оборудования для защиты информации. Рассмотрение системы контроля и управления доступом. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. Рассмотрение датчиков периметра, их принципов работы. Выполнение звукоизоляции помещений системы зашумления. Реализация защиты от утечки по цепям электропитания и заземления. Разработка основной документации по инженерно-технической защите информации.	– Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты. – Размещение периметровых средств обнаружения на местности. Самостоятельнее изучения порядка допуска субъектов на охраняемые объекты. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам,главам учебных пособий, составленным пре-

Результаты, заявленные в профессиональном стандарте	Технические требования РЧ/ДЭ	Образовательные результаты ФГОС СПО по ПМ		
предусмотренных регламентом операций по техническому обслуживанию средств и систем защиты СССЭ от НСД Обновление в соответствии с регламентом эксплуатации программных компонентов СССЭ, программных, программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НСД Устранение неисправностей СССЭ, а также программно-аппаратных (в том числе криптографических) и технических		настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты; диагностики, устранения проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;		подавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.

Результаты, заявленные в профессиональном стандарте	Технические требования РЧ/ДЭ	Образовательные результаты ФГОС СПО по ПМ		
средств и систем защиты СССЭ от НСД своими силами, если это допускается технической документацией		проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;		
		выявления технических каналов утечки информации;		
Направление в ремонт и прием из ремонта сторонними организациями СССЭ, а также программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД				

Результаты, заявленные в профессиональном стандарте	Технические требования РЧ/ДЭ	Образовательные результаты ФГОС СПО по ПМ		
Ведение эксплуатационной документации СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД				
Необходимые умения		**Умение**	**Практические задания**	
Обнаруживать неисправности СССЭ, а также средств и подсистем защиты СССЭ от НСД согласно технической документации Взаимодействовать с организациями, осуществляющими гарантий-	Интерпретировать пользовательские запросы и требования с точки зрения корпоративных требований; Применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении;	применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные мето-	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Защита от утечки по виброакустическому каналу Определение каналов утечки ПЭМИН Защита от утечки по цепям электропитания и заземления Защита от утечки по электросетевому каналу Защита от утечки по оптическому каналу Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Рассмотрение инженерных конструкций, применяемые для предотвращения проникновения злоумышленника к источникам информации.	

Результаты, заявленные в профессиональном стандарте	Технические требования РЧ/ДЭ	Образовательные результаты ФГОС СПО по ПМ		
ный и послегарантийный ремонт СССЭ, а также средств и подсистем защиты СССЭ от НСД Проводить работы по техническому обслуживанию, в том числе по обновлению версий программного обеспечения, СССЭ, а также средств и систем защиты СССЭ от НСД Устранять неисправности СССЭ, а также средств и подсистем защиты СССЭ от НСД, если это предусмотрено технической документацией	Настраивать сетевые устройства; Администрирование автоматизированных технические средства управления и контроля информации и информационных потоков; Навыки системного администрирования в операционных системах , Server, Linux (Red Hat Enterprise Linux, CentOS и др.); Навыки системного администрирования в защищенных операционных системах (AstraLinux и др.); Настройка в операционных системах прав доступа в соответствие с ролевой и/или мандатной моделью; Настройка средств виртуализации под	дические документы по обеспечению защиты информации техническими средствами; применять применять средства охранной сигнализации, охранного телевидения и системконтроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя Рассмотрение принципов устройства, работы и применения средств контроля доступа Рассмотрение принципов устройства, работы и применения средств видеонаблюдения. Определение основных показателей технических средств воздействия. Практическое занятие № 169-172 Управление системой воздействия. Изучение Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 02.07.2013) "Об информации, информационных технологиях и о защите информации"	

Результаты, заявленные в профессиональном стандарте	Технические требования РЧ/ДЭ	Образовательные результаты ФГОС СПО по ПМ		
	операционными системам; Конфигурирование операционных систем для правильного и защищенного использования средств безопасности, в т.ч. системы корпоративной защиты от внутренних угроз.: Установка серверной части системы корпоративной защиты от внутренних угроз; Установка СУБД различного вида; Установка агентской части системы корпоративной защиты от внутренних угроз; Запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров;			

Результаты, заявленные в профессиональном стандарте	Технические требования РЧ/ДЭ	Образовательные результаты ФГОС СПО по ПМ		
	Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом; Использовать дополнительные утилиты если это необходимо; Уметь проверять работоспособность системы и выявлять неисправности, устранять проблемы и проводить контрольные проверки; Подходить к проблеме с необходимым уровнем уверенности для успокоения пользователя в случае 22 необходимости; Уметь сконфигурировать систему, чтобы она получала теневые копии; Регулярно проверять результаты			

Результаты, заявленные в профессиональном стандарте	Технические требования РЧ/ДЭ	Образовательные результаты ФГОС СПО по ПМ		
	собственной работы во избежание проблем на последующих этапах; Демонстрировать уверенность и упорство в решении проблем; Быстро узнавать и понимать суть неисправностей и разрешать их в ходе самостоятельной управляемой работы, точно описывать проблему и документировать её решение; Тщательно расследовать и анализировать сложные, комплексные ситуации и проблемы, применять методики поиска неисправностей; Выбирать и принимать диагностирующее ПО и инструменты для поиска неисправ-			

Результаты, заявленные в профессиональном стандарте	Технические требования РЧ/ДЭ	Образовательные результаты ФГОС СПО по ПМ		
	ностей;			
Необходимые знания		**Знание**	**Темы/ЛР**	
Организация и содержание диагностики и технического обслуживания СССЭ, а также средств и систем защиты СССЭ от НСД	Сетевое окружение; Сетевые протоколы; Знать методы выявления и построения путей движения информации в организации; Подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия; Типы сетевых устройств; Разнообразие операционных систем, их возможности с точки зрения использования пользователями и для развёртывания компонент систем защиты от внутренних угроз; Процесс выбора под-	порядок технического обслуживания технических средств защиты информации; физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим	Концепция инженерно-технической защиты информации Теоретические основы инженерно-технической защиты информации Физические основы технической защиты информации Системы защиты от утечки информации Применение и эксплуатация технических средств защиты информации Построение и основные характеристики инженерно-технических средств физической защиты Основные компоненты комплекса инженерно-технических средств физической защиты Применение и эксплуатация инженерно-технических средств физической защиты Построение и основные характеристики средств физической защиты	
Правила ведения				

Результаты, заявленные в профессиональном стандарте	Технические требования РЧ/ДЭ	Образовательные результаты ФГОС СПО по ПМ		
эксплуатационной документации СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД	ходящих драйверов и программного обеспечения для разных типов аппаратных средств и операционных систем; Важность следования инструкциям и последствия, цену пренебрежения ими; Меры предосторожности, рекомендуемые к принятию перед установкой ПО или обновлением системы; Этапы установки системы корпоративной защиты от внутренних угроз; Знать отличия различных версий систем корпоративной защиты от внутренних угроз; Знать какие СУБД поддерживаются системой; Знать назначение	каналам; номенклатуру применяемых средств физической защиты объектов информатизации. номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защитыинформации; основные принципы действия и характеристики технических средств физической защиты; порядок устранения неисправностей технических средств защиты информации и		

Результаты, заявленные в профессиональном стандарте	Технические требования РЧ/ДЭ	Образовательные результаты ФГОС СПО по ПМ		
Методики и приемы ремонта СССЭ, а также средств и систем защиты СССЭ от НСД	различных компонент версий систем корпоративной защиты от внутренних угроз; Знать технологии программной и аппаратной виртуализации; Знать особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, VMWare Workstation; Цель документирования процессов обновления и установки. Важность спокойного и сфокусированного подхода к решению проблемы; 14,00 21 Значимость систем ИТ-безопасности и зависимость пользователей и организаций от их до-	организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; основные способы физической защиты объектов информатизации.		

Результаты, заявленные в профессиональном стандарте	Технические требования РЧ/ДЭ	Образовательные результаты ФГОС СПО по ПМ		
	ступности; Популярные аппаратные и программные ошибки; Знать разделы системы корпоративной безопасности, которые обычно использует системный администратор; Аналитический и диагностический подходы к решению проблем; Границы собственных знаний, навыков и полномочий; Ситуации, требующие вмешательства службы поддержки; Стандартное время решения наиболее популярных проблем.			

ПРИЛОЖЕНИЕ 2.1

к рабочей программе профессионального модуля Защита информации техническими средствами, разработанного на основе изучения квалификационных требований работодателей

Перечень квалификационных требований производственных компаний/организаций, установленных в ходе изучения квалификационных запросов к деятельности рабочих по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Трудовая функция	Техническое обслуживание СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД
Трудовые действия	Диагностика СССЭ штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами Диагностика программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими силами Выполнение предусмотренных регламентом операций по техническому обслуживанию средств и систем защиты СССЭ от НСД Обновление в соответствии с регламентом эксплуатации программных компонентов СССЭ, программных, программно-аппаратных (в том числе криптографических) средств и систем защиты СССЭ от НСД Устранение неисправностей СССЭ, а также программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД своими силами, если это допускается технической документацией Направление в ремонт и прием из ремонта сторонними организациями СССЭ, а также программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД Ведение эксплуатационной документации СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД
Умения	Обнаруживать неисправности СССЭ, а также средств и подсистем защиты СССЭ от НСД согласно технической документации Взаимодействовать с организациями, осуществляющими гарантийный и послегарантийный ремонт СССЭ, а также средств и подсистем защиты СССЭ от НСД Проводить работы по техническому обслуживанию, в том числе по обновлению версий программного обеспечения, СССЭ, а также средств и систем защиты СССЭ от НСД Устранять неисправности СССЭ, а также средств и подсистем защиты СССЭ от НСД, если это предусмотрено технической документацией
Знания	Организация и содержание диагностики и технического обслуживания СССЭ, а также средств и систем защиты СССЭ от НСД Правила ведения эксплуатационной документации СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД Методики и приемы ремонта СССЭ, а также средств и систем защиты СССЭ от НСД

Руководитель рабочей группы
(методист) _____ И.Н. Ежкова

Член рабочей группы
(преподаватель) _____ М.В. Киреева

Представитель ООО «Центр защиты информации»:

Директор _____ Д.А. Полоса

М.П.

ПРИЛОЖЕНИЕ 2.2

к рабочей программе профессионального модуля Защита информации техническими средствами, разработанного на основе профессионального стандарта и/или WS, квалификационных требований работодателей

Конвертация трудовых функций ПС, квалификационных требований работодателей и технических требований WS в образовательные результаты в содержание профессионального модуля Защита информации техническими средствами

10.02.05 Обеспечение информационной безопасности автоматизированных систем

06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», 5 уровень квалификации		**Содержание ПМ «Защита информации техническими средствами»**		
Название трудовой функции: Техническое обслуживание СССЭ, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем их защиты от НСД	**Технические требования РЧ/НЧ/ДЭ**	**Профессиональная компетенция** Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации, а также проводить обслуживание программных и программно-аппаратных средств и систем защиты от НСД.		**Кол-во часов**
Трудовое действие.. Диагностика программно-аппаратных (в том числе криптографических) и технических средств и систем защиты СССЭ от НСД штатными средствами в целях принятия решения о направлении в ремонт изготовителем или своими	Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз	Защита техническими средствами	Виды работ на практику: 1. Участие в диагностике программно-аппаратных средств и систем защиты СССЭ от НСД штатными средствами. 2. Участие в выполнении предусмотренных регламентом операций по техническому обслуживанию средств и систем защиты СССЭ от НСД	

06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», 5 уровень квалификации	Технические требования РЧ/НЧ/ДЭ	Содержание ПМ «Защита информации техническими средствами»		
силами Выполнение предусмотренных регламентом операций по техническому обслуживанию средств и систем защиты СССЭ от НСД				
Умение обнаруживать неисправности СССЭ, а также средств и подсистем защиты СССЭ от НСД согласно технической документации	Применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении; Настраивать сетевые устройства; Администрирование автоматизированных технические средства управления и контроля информации и информационных потоков; Навыки системного администрирования	Умение обнаружить неисправность системы	Тематика практических занятий: 1. Настройка сетевых устройств. 2. Администрирование автоматизированных технических средств управления и контроля информации и информационных потоков. 3. Работа с операционными системами Linux (Red Hat Enterprise Linux, CentOS. 4. Администрирование в защищенных операционных системах. 5. Настройка в ОС прав доступа. 6. Конфигурирование ОС.	

06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», 5 уровень квалификации	Технические требования РЧ/НЧ/ДЭ	Содержание ПМ «Защита информации техническими средствами»		
	в операционных системах , Server, Linux (Red Hat Enterprise Linux, CentOS и др.); Навыки системного администрирования в защищенных операционных системах (AstraLinux и др.); Настройка в операционных системах прав доступа в соответствие с ролевой и/или мандатной моделью; Настройка средств виртуализации под операционными системам; Конфигурирование операционных систем для правильного и защищенного использования средств безопасности, в т.ч. системы корпоративной защиты от внутренних			

06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», 5 уровень квалификации	Технические требования РЧ/НЧ/ДЭ	Содержание ПМ «Защита информации техническими средствами»		
	угроз.: Установка серверной части системы корпоративной защиты от внутренних угроз; Запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров; Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом.			
Знание организация и содержание диагностики и технического обслуживания СССЭ, а также средств и систем защиты СССЭ от НСД	Сетевое окружение; Сетевые протоколы; Подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия; Типы сетевых устройств;	Знание технического обслуживания и средств систем защиты СССЭ от НСД	Теоретические темы, ЛР: 1. Подходы к построению сети 2. Типы сетевых устройств 3. Этапы установки системы корпоративной защиты от внутренних угроз 4. Технологии программной и аппаратной виртуализации 5. Особенности работы основных гипервизоров (мониторов виртуальных машин), например, VirtualBox, VMWare Workstation. 6. Программные и аппаратные ошибки	

06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», 5 уровень квалификации	Технические требования РЧ/НЧ/ДЭ	Содержание ПМ «Защита информации техническими средствами»		
	Разнообразие операционных систем, их возможности с точки зрения использования пользователями и для развёртывания компонент систем защиты от внутренних угроз; Этапы установки системы корпоративной защиты от внутренних угроз; Знать отличия различных версий систем корпоративной защиты от внутренних угроз; Знать какие СУБД поддерживаются системой; Знать назначение различных компонент версий систем корпоративной защиты от внутренних угроз; Знать технологии программной и аппаратной вирту-			

06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», 5 уровень квалификации	Технические требования РЧ/НЧ/ДЭ	Содержание ПМ «Защита информации техническими средствами»		
	ализации; Знать особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, VMWare Workstation; Популярные аппаратные и программные ошибки; Знать разделы системы корпоративной безопасности, которые обычно использует системный администратор; Аналитический и диагностический подходы к решению проблем; Границы собственных знаний, навыков и полномочий.			
Самостоятельная работа				9