МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Грозненский государственный нефтяной технический университет имени академика М.Д. Миллионщикова

Согласовано
Генеральный директор
ГАУ «Фарммедтехснаб» МЗ ЧР
_____ И.М. Халадов
«25» 01 2024 г.

Первый проректор
ФГБОУ ВО «Грозненский государственный нефтяной технический университет имени академика М.Д. Миллионщикова»
_____ И.Г. Гайрабеков
«15» 01 2024 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 «Защита информации техническими средствами»

Специальность

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация

Техник по защите информации

Грозный – 2024 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ПМ.03 Защита информации техническими средствами»

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен освоить основной вид профессиональной деятельности техника по защите информации и соответствующие ему общие компетенции и профессиональные компетенции:

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 09	Использовать информационные технологии в профессиональной деятельности.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 03	Защита информации техническими средствами
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 (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.

1.1.3. В результате освоения профессионального модуля обучающийся 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 физической защиты.
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 информации и 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 защиты информации;
	основные принципы действия и характеристики технических средств физической защиты;
	основные способы физической защиты объектов информатизации;
	номенклатуру применяемых средств физической защиты объектов информатизации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего ОФО 526 часов
в том числе:
- на освоение МДК 244 часа;
- самостоятельная работа 44 часа;
- учебная практика 72 часов;
- производственная практика 144 часа;
- промежуточная аттестация 22 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час.	Объем профессионального модуля, ак. час.					
			Обучение по МДК				Практики	
			В том числе					
			Теоретических занятий	Практических занятий	Самостоя-тельная работа	Промежуточная аттестация	Учебная	Производственная
1	*2*	*3*	*6*	*7*	*8*	*9*	*10*	*11*
ПК 3.1 ПК 3.2, ПК 3.3, ПК 3.4 ПК 2.2, ПК 2.3, ПК 3.5 ОК 02, ОК 09	Раздел 1. Техническая защита информации	**150**	**78**	**44**	**22**	**6**	**-**	**-**
	Раздел 2. Инженерно-технические средства физической защиты объектов информатизации	**150**	**78**	**44**	**22**	**6**	**-**	**-**
	Учебная практика	**72**	-	-	-	-	**72**	-
	Производственная практика	**144**	-	-	-	-	**-**	**144**
	Промежуточная аттестация	**10**	**-**	**-**	**-**	**10**	**-**	**-**
	Всего:	***526***	***156***	***88***	***44***	***22***	***72***	***144***

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, акад. ч / в том числе в форме практической подготовки, акад ч	Код ПК, ОК
1	**2**	**3**	**4**
Раздел 1. Техническая защита информации		**78 /44**	
МДК.03.01 Техническая защита информации		**78 /44**	
Тема 1.1. Предмет и задачи технической защиты информации	**Теоретическое обучение**	**10**	
	1. Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности.	4	**ПК 3.1 ОК 02, ОК 09**
	2. Способы и технология ремонта механизмов и систем двигателя, а также их отдельных элементов.	2	**ПК 3.2 ОК 02, ОК 09**
	3. Основные параметры системы защиты информации.	4	**ПК 3.4, ОК 02, ОК 09**
	В том числе практических занятий	**2**	
	1.Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	2	**ПК 3.1 ОК 02, ОК 09**
Тема 1.2. Общие положения защиты информации	**Теоретическое обучение**	**12**	
	1. Задачи и требования к способам и средствам защиты информации техническими средствами.	*4*	**ПК 3.2, ПК 3.4 ОК 09**

техническими средствами			
	2. Принципы системного анализа проблем инженерно-технической защиты информации.	*4*	**ПК 3.2, ПК 3.4 ОК 02, ОК 09**
	3. Классификация способов и средств защиты информации.	*4*	**ПК 3.1 ОК 02**
	В том числе практических занятий	**4**	
	1.Классификация угроз безопасности информационных объектов	*4*	**ПК 3.2 ОК 02, ОК 09**
Тема 1.3. Информация как предмет защиты	**Теоретическое обучение**	***10***	
	1. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации.	*2*	**ПК 3.1 ОК 02, ОК 09**
	2. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов.	*4*	**ПК 3.2, ПК 3.3 ОК 02, ОК 09**
	3. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	*4*	**ПК 3.2, ПК 3.3 ОК 02, ОК 09**
	В том числе практических занятий	**10**	
	1. Инженерно-техническая защита информации.	*2*	**ПК 3.1 ОК 09**
	2. Признаки появления вирусов. Методы защиты.	*4*	**ПК 3.5, ОК 09**
	3. Выявление и фиксация следов противоправной деятельности связанной с использованием компьютерной техники.	*4*	**ПК 3.4, ПК 3.5 ОК 02, ОК 09**
Тема 1.4. Технические каналы утечки информации	**Теоретическое обучение**	***12***	
	1. Понятие и особенности утечки информации. Структура канала утечки информации.	*4*	**ПК 3.4, ПК 3.5 ОК 02, ОК 09**
	2. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации.	*4*	**ПК 3.3 ОК 02, ОК 09**

	3. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	*4*	**ПК 3.3, ПК 3.4 ОК 09**
	В том числе практических занятий	**8**	
	1. Классификация демаскирующих признаков. Основные виды угроз информации.	*4*	**ПК 3.3, ПК 3.4 ОК 02**
	2. Обоснование выбора кабинета как объекта защиты. Составление плана кабинета как объекта защиты.	*4*	**ПК 3.3, ПК 3.5 ОК 02, ОК 09**
Тема 1.5. Методы и средства технической разведки	**Теоретическое обучение**	**12**	
	1. Классификация технических средств разведки. Методы и средства технической разведки.	*4*	**ПК 3.1, ПК 3.5 ОК 02, ОК 09**
	2. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки.	*4*	**ПК 3.2, ПК 3.5 ОК 02, ОК 09**
	3. Средства дистанционного съема информации.	*4*	**ПК 3.5 ОК 02, ОК 09**
	В том числе практических занятий	**10**	
	1. Типовая структура технических каналов утечки. Моделирование каналов утечки утечки информации.	*4*	**ПК 3.1, ПК 3.5 ОК 02, ОК 09**
	2. Методы добавления информации о вещественных носителях.	*4*	**ПК 3.3, ОК 02, ОК 09**
	3. Дистанционный анализ веществ.	*2*	**ПК 3.3, ОК 02, ОК 09**
Тема 1.6. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Теоретическое обучение**	**14**	
	1. Физические основы побочных электромагнитных излучений и наводок.	*4*	**ПК 3.3, ПК 3.4 ОК 02, ОК 09**
	2. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.	*4*	**ПК 3.1, ПК 3.4 ОК 02, ОК 09**
	3. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.	*2*	**ПК 3.3, ПК 3.4 ОК 02**
	4. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей.	*4*	**ПК 3.4 ОК 02, ОК 09**
	В том числе практических занятий	**4**	
	1. Измерение параметров физических полей.	*2*	**ПК 3.4 ОК 02, ОК 09**

	2. Защита от утечки по акустическому каналу.	*2*	**ПК 3.5 ОК 02, ОК 09**
Тема 1.7. Физические процессы при подавлении опасных сигналов	**Теоретическое обучение**	**8**	
	1. Скрытие речевой информации в каналах связи.	*4*	**ПК 3.4 ОК 02, ОК 09**
	2. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	*4*	**ПК 3.4 ОК 02, ОК 09**
	В том числе практических занятий	**6**	
	1.Энергетическое скрытие акустических сигналов:звукоизоляция и звукопоглащение.	*6*	**ПК 3.1, ПК 3.4 ОК 02, ОК 09**
Примерная тематика самостоятельной учебной работы при изучении раздела 1 1. Направление комплексного проектирования систем защиты информации 2. Основные проблемы реализации систем защиты информации 3. Требования к КСЗИ 4. Задачи стратегии защиты информации 5. Верификация 6. Дискреционный контроль доступа 7. Биометрическая идентификация 8. Биометрия по клавиатурному почерку 9. Классификация признаков голоса и речи 10. Средства высоконадежной биометрической аутентификации 11. Шпионаж, сбор служебной информации, сканирование эфира, обработка неучтенных источников		***22***	
Раздел 2. Инженерно-технические средства физической защиты объектов информатизации		**78 /44**	
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**78 /44**	
Тема 2.1. Цели и задачи физической защиты объектов информатизации	**Теоретическое обучение**	**12**	
	1. Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации.	*4*	**ПК 3.1 ОК 02, ОК 09**
	2. Основные понятия инженерно-технических средств физической защиты.	*4*	**ПК 3.2 ОК 09**

	3. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.	*4*	**ПК 3.5** **ОК 02**
	В том числе практических занятий	**4**	
	1. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	*4*	**ПК 3.1** **ОК 02, ОК 09**
Тема 2.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Теоретическое обучение**	**12**	
	1. Общие принципы обеспечения безопасности объектов.	*2*	**ПК 3.2, ПК 3.5** **ОК 02, ОК 09**
	2. Жизненный цикл системы физической защиты.	*2*	**ПК 3.5** **ОК 02, ОК 09**
	3. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны.	*4*	**ПК 3.2** **ОК 02, ОК 09**
	4. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	*4*	**ПК 3.1, ПК 3.5** **ОК 02, ОК 09**
	В том числе практических занятий	**8**	
	1. Типовые инженерные конструкции	*2*	**ПК 3.1** **ОК 02, ОК 09**
	2. Исследование систем охраны	*2*	**ПК 3.3** **ОК 02, ОК 09**
	3. Способы и средства обнаружения злоумышленников и пожара	*4*	**ПК 3.2, ПК 3.4** **ОК 02, ОК 09**
Тема 2.3. Система обнаружения комплекса инженерно-	**Теоретическое обучение**	**14**	
	1. Информационные основы построения системы охранной сигнализации.	*2*	**ПК 3.2, ПК 3.3** **ОК 02, ОК 09**

технических средств физической защиты	2. Назначение, классификация технических средств обнаружения.	*4*	**ПК 3.3, ПК 3.4 ОК 02, ОК 09**
	3. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия.	*4*	**ПК 3.1 ОК 02, ОК 09**
	4. Объектовые средства обнаружения: назначение, устройство, принцип действия.	*4*	**ПК 3.1 ОК 02, ОК 09**
	В том числе практических занятий	**6**	
	1. Монтаж датчиков пожарной и охранной сигнализации	*6*	**ПК 3.1, ПК 3.5 ОК 02, ОК 09**
Тема 2.4. Система контроля и управления доступом	**Теоретическое обучение**	**16**	
	1. Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД.	*4*	**ПК 3.1, ПК 3.4 ОК 02, ОК 09**
	2. Структура и состав СКУД.	*2*	**ПК 3.1 ОК 02, ОК 09**
	3. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД.	*4*	**ПК 3.5 ОК 02, ОК 09**
	4. Классификация средств управления доступом. Средства идентификации и аутентификации.	*2*	**ПК 3.2 ОК 02, ОК 09**
	5. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	*4*	**ПК 3.1, ПК 3.4 ОК 02, ОК 09**
	В том числе практических занятий	**8**	
	1. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	*4*	**ПК 3.1, ПК 3.2 ОК 02, ОК 09**
	1. Рассмотрение принципов устройства, работы и применения средств контроля доступа	*4*	**ПК 3.5**

			ОК 02, ОК 09
Тема 2.5. Система телевизионного наблюдения	**Теоретическое обучение**	**12**	
	1. Аналоговые и цифровые системы видеонаблюдения.	*2*	**ПК 3.2, ПК 3.5 ОК 02, ОК 09**
	2. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения.	*4*	**ПК 3.2, ПК 3.5 ОК 02, ОК 09**
	3. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	*6*	**ПК 3.4, ПК 3.5 ОК 02, ОК 09**
	В том числе практических занятий	**6**	
	1. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	*6*	**ПК 3.2, ПК 3.5 ОК 02, ОК 09**
Тема 2.6. Система сбора, обработки, отображения и документирования информации	**Теоретическое обучение**	**12**	
	1. Классификация системы сбора и обработки информации.	*2*	**ПК 3.2 ОК 02, ОК 09**
	2. Схема функционирования системы сбора и обработки информации.	*4*	**ПК 3.2, ПК 3.5 ОК 02, ОК 09**
	3. Варианты структур построения системы сбора и обработки информации.	*4*	**ПК 3.4 ОК 02, ОК 09**
	4. Устройства отображения и документирования информации.	*2*	**ПК 3.5 ОК 02, ОК 09**
	В том числе практических занятий	**12**	
	1. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	*6*	**ПК 3.2, ПК 3.5 ОК 02, ОК 09**
	2. Исследование технических средств воздействия.	*6*	**ПК 3.4 ОК 02, ОК 09**

Примерная тематика самостоятельной учебной работы при изучении раздела 2 1.Понятие об информации и объектах информатизации. Физические свойства и характеристики информационных сигналов. 2.Нормативно-правовая база защиты объектов информатизации. Роль и место правового обеспечения физической защиты объектов информатизации. 3.Жизненный цикл системы инженерно-технических средств физической защиты. Основные методы внедрения инженернотехнических средств по объектам информатизации. 4.Основные этапы и маршруты проникновения к объектам информатизации. Групповые и одиночные маршруты проникновения на объекты. 5.Требования к инженерно-техническим средствам физической защиты объектов информатизации по обеспечению информационной безопасности предприятия. 6.Основные понятия и определения. Классификация комплексов инженерно-технических средств. Основные параметры по информационной безопасности на объектах. 7.Принцип построения интегрированных систем охраны информации на объектах. 8.Общая характеристика методов хищения информации, копирования, уничтожения, искажения, подавления информации. Утечка информации по каналам ПЭМРШ. 9.Классификация методов технической разведки. Способы ведения разведки на объектах информатизации. 10.Телевизионные датчики и телеохранные системы. Промышленные телевизионные установки контроля и охраны объекта информатизации. 11.Технические характеристики видеокамер охранного назначения. Наименования, классификация, форм-фактор камер охранного назначения.	***22***	
Учебная практика **Виды работ** 1. Измерение параметров физических полей. 2. Определение каналов утечки ПЭМИН. 3. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. 4. Установка и настройка технических средств защиты информации. 5. Проведение измерений параметров побочных электромагнитных излучений и наводок. 6. Проведение аттестации объектов информатизации. 7. Монтаж различных типов датчиков.	***72***	

8. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 9. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. 10. Рассмотрение системы контроля и управления доступом. 11. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 12. Рассмотрение датчиков периметра, их принципов работы. 13. Выполнение звукоизоляции помещений системы зашумления. 14. Реализация защиты от утечки по цепям электропитания и заземления. 15. Разработка организационных и технических мероприятий по заданию преподавателя; 16. Разработка основной документации по инженерно-технической защите информации.		
Производственная практика **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 технической охраны объектов, систем видеонаблюдения; 3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	***144***	
Промежуточная аттестация	***22***	
Всего	***526***	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Лаборатория Технических средств защиты информации**,** оснащенная в соответствии с п. 6.1.2.3 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Оснащенные базы практики в соответствии с п 6.1.2.5 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

3.2. Информационное обеспечение реализации программы

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

3.2.1. Основные электронные издания

1. Ворожейкин, В. Н. Технические средства и методы защиты информации / В. Н. Ворожейкин. — 2-е изд. — Самара : Самарский государственный технический университет, ЭБС АСВ, 2019. — 336 с. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/111432

2. Евстифеев, А.А. Основы защиты информации от утечки по техническим каналам : учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов [и др.]. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 267 с. — ISBN 978-5-9515-0426-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/101929

3. Запонов, Э. В. Методы и средства комплексной защиты информации в технических системах : учебное пособие / Э. В. Запонов, А. П. Мартынов, И. Г. Машин [и др.]. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2019. — 224 с. — ISBN 978-5-9515-0429-6. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/101925

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 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 (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	**Критерии оценивания рубежной аттестации:** **Аттестован** - выставляется обучающемуся, ответившему правильно на 6-20 вопросов. **Не аттестован** - выставляется обучающемуся, который ответил менее 5 вопроса. **Критерии оценивания зачета/экзамена:** **Отлично** - выставляется обучающемуся, ответившему на 31-40 вопросов. **Хорошо** - выставляется обучающемуся, ответившему на 21-30 вопросов. **Удовлетворительно** - выставляется обучающемуся, ответившему на 11 и более вопросов.	Рубежная аттестация Экзамен

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		
ОК 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. ОК 09. Использовать информационные технологии в профессиональной деятельности.		

Разработчик:

Преподаватель ФСПО _____ / А.А.Мидаева /

(подпись)

Согласовано:

Председатель ПЦК «Информационные технологии»

_____ / И.М.Дубаев/

(подпись)

Зам. декана по МР ФСПО _____ / И.В.Сулейманова/

(подпись)

Директор ДУМР _____ / М.А. Магомаева/

(подпись)