МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
государственное бюджетное профессиональное
образовательное учреждение Московской области
«Шатурский энергетический техникум»
(ГБПОУ МО «ШЭТ»)

УТВЕРЖДАЮ
зам. директора по УМР
_____ С.А. Косова
«02» 06 2023 г.

РАБОЧАЯ ПРОГРАММА

ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

г. Шатура
2023 г.

Рабочая программа учебной дисциплины разработана в соответствии Федеральным государственным образовательным стандартом (далее - ФГОС) по специальности программы подготовки специалистов среднего звена (далее ППССЗ) 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (базовой подготовки).

Организация-разработчик: ГБПОУ МО «ШЭТ»

Разработчики:

Краснолобов Дмитрий Михайлович, преподаватель специальных дисциплин

ОДОБРЕНО

цикловой комиссией преподавателей специальности УГС Информатика и вычислительная техника и Информационная безопасность (09.02.06, 10.02.04)

Протокол № 11 от «01» 06 2023 г.

Председатель ЦК: _____ Е.А. Еремина

Внутренний рецензент: _____ Е.В. Лялина, методист ГБПОУ МО «ШЭТ»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности и соответствующие ему общие и профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно-телекоммуникационных системах и сетях
ПК 3.2.	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях
ПК 3.3.	Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями
ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

1.1.1. Общие компетенции

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 9.	Использовать информационные технологии в профессиональной деятельности.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации; проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление 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 формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; структуру и условия формирования 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 информации; номенклатуру применяемых средств физической защиты объектов информатизации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов: **442 часа.**

Из них на освоение МДК **436 часов:**

МДК.03.01Защита информации в ИТКС с использованием технических средств защиты- **141 час;**

МДК.03.02Физическая защита линий связи ИТКС –**120 часов.**

На практики учебную и производственную -**175 часов.**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуляПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					Самостоятельная работа[1]	Консультации
			Обучение по МДК			Практики			
			всего, часов	Лабораторных и практических занятий	Курсовых работ (проектов)*	Учебная	Производственная		
ПК 3.1- ПК.3.4 ОК1 – ОК7, ОК 9 ЛР 3, 4, 7, 14, 19	**Раздел 1.** Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	**203**	194	92	-	-	-	4	5
ПК 3.5 ОК1 – ОК7, ОК 9 ЛР 3, 4, 7, 14, 19	**Раздел 2.** Физическая защита линий связи информационно-телекоммуникационных систем и сетей	**143**	138	68	-	-	-	2	3
ПК 3.1 – 3.5 ОК 1-10 ЛР 3, 4, 7, 14, 19	Учебная практика	**108**	-	-	-	108	-	-	-
ПК 3.1 – 3.5 ОК 1-10 ЛР 3, 4, 7, 14, 19	Производственная практика	**72**	-	-	-	-	72	-	-
	Промежуточная аттестация	**8**	8	-	-	-	-	-	-
	Всего:	**534**	**340**	**160**	**-**	**108**	**72**	**6**	**8**

2.2. Тематический план и содержание профессионального модуля ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов
1	2	3
Раздел 1. Защита информации в ИТКС с использованием технических средств защиты		**203**
МДК.03.01.Защита информации в ИТКС с использованием технических средств защиты		194
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	**2**
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание**	**2**
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.	
Тема 2.1. Информация как предмет защиты	**Содержание**	**2**
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства, и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	
	Практические и лабораторные работы	**2**

	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	2
Тема 2.2. Технические каналы 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.	
	Практические и лабораторные работы	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	4
Тема 2.3. Методы и средства технической разведки	**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.	
	Тематика практических занятий и лабораторных работ	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**2**
	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 побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	
	Тематика практических занятий и лабораторных работ	**4**
	Измерение параметров физических полей	4
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание**	**2**
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	
	Практические и лабораторные работы	**4**

	Тематика учебных занятий формируется образовательной организацией самостоятельно	
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 от несанкционированной утечки по акустическому каналу.	
	Практические и лабораторные работы	**4**
	Защита от утечки по акустическому каналу	
Тема 4.2. Системы защиты 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.	
	Практические и лабораторные работы	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**2**
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	
	Практические и лабораторные работы	**4**
	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 закладках. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	

	Практические и лабораторные работы	**8**
	Определение каналов утечки ПЭМИН	
	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 к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	
	Практические и лабораторные работы	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**4**
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
	Практические и лабораторные работы	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
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.	
	Практические и лабораторные работы	**2**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
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. Проведение измерений параметров побочных электромаг-	

	нитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	
	Практические и лабораторные работы	**10**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	10
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**	**4**
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.	
	Практические и лабораторные работы	**16**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	16
Самостоятельная учебная работа при изучении раздела 1 ПМ		**4**
Рекомендуемая тематика самостоятельной работы: 1. Классификация способов и средств защиты информации. 2. Основные и вспомогательные технические средства, и системы. 3. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. 4. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика. 5. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу. 6. . Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу. 7. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу. 8. Технические средства для уничтожения информации и носителей информации, порядок применения.		

Раздел 2. Физическая защита линий связи ИТКС		**143**
МДК.03.02. Физическая защита линий связи ИТКС		**138**
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**2**
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.	
	Практические и лабораторные работы	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	4
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**3**
	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. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	
	Практические и лабораторные работы	**12**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	12
Тема 2.1. Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**	**2**
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	
	Практические и лабораторные работы	**8**
	Монтаж датчиков пожарной и охранной сигнализации	8
	Содержание	**2**

Тема 2.2. Система контроля и управления доступом	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование 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 и радиоактивных веществ.	
	Практические и лабораторные работы	**6**
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	6
	Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Тема 2.3. Система телевизионного наблюдения	**Содержание**	**2**
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	
	Практические и лабораторные работы	**6**
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	6
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание**	**2**
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	
	Практические и лабораторные работы	**2**
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	2
Тема 2.5. Система воздействия	**Содержание**	**2**
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	
	Практические и лабораторные работы	**6**

	Тематика учебных занятий формируется образовательной организацией самостоятельно	6
Тема 3.1. Применение инженерно-технических средств физической защиты	**Содержание**	**2**
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	
	Практические и лабораторные работы	**14**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	14
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**2**
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.	
	Практические и лабораторные работы	
	Тематика учебных занятий формируется образовательной организацией самостоятельно	**12**
Самостоятельная учебная работа при изучении раздела модуля 2 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.		**2**
Учебная практика по профессиональному модулю 1. Монтаж различных типов датчиков. 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.		

4. Рассмотрение системы контроля и управления доступом. 5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 6. Рассмотрение датчиков периметра, их принципов работы. 7. Выполнение звукоизоляции помещений системы зашумления. 8. Реализация защиты от утечки по цепям электропитания и заземления. 9. Разработка организационных и технических мероприятий по заданию преподавателя; 10. Разработка основной документации по инженерно-технической защите информации.	**100**
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 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.	
Промежуточная аттестация (экзамен по модулю)	**8**
Всего по ПМ	**534**

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Лаборатория «Защиты информации от утечки по техническим каналам».

Оборудование мастерской:

- рабочее место преподавателя;
- посадочные места обучающихся (по количеству обучающихся);
- учебные наглядные пособия (таблицы, плакаты);
- тематические папки дидактических материалов;
- комплект учебно-методической документации;
- комплект учебников (учебных пособий) по количеству обучающихся.

Технические средства обучения:

- персональный компьютер с лицензионным программным обеспечением;
- мультимедиа проектор (проектор, экран);
- Маркерная доска;
- Программное обеспечение общего и профессионального назначения.

3.2. Информационное обеспечение обучения

Основные источники:

1. Технологии защиты информации в компьютерных сетях / Н.А.Руденков. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.
http://biblioclub.ru/index.php?page=book&id=428820

2. Бубнов, А. А.: Техническая защита информации в объектах информационной инфраструктуры : учебник для студентов средних профессиональных заведений учебное пособие /, 2019. - 270 с. ISBN 978-5-4468-8718-7
https://mdk-arbat.ru/book/3372534

3. Технические средства автоматизации и управления: Учебное пособие/ Шишов О. В. - М.: НИЦ ИНФРА-М, 2018. - 396 с.: 60x90 1/16. - (Высшее образование: Бакалавриат) (Переплёт) ISBN 978-5-16-010325-9
https://znanium.com/read?id=361160

4. Технические средства информатизации: Учебное пособие. Гагарина Лариса Геннадьевна; Москва : Издательский Дом "ФОРУМ" : ООО "Научноиздательский центр ИНФРА-М", 2019. - 256 с. - ISBN 978-5-8199-0734-4
http://znanium.com/go.php?id=1021128

5. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2019. - 352 с.: ил.;

60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-00091-557-8. https://znanium.com/catalog/document?id=364477

6. Технологии защиты информации в компьютерных сетях / Н.А. Руденков. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. ttp://biblioclub.ru/index.php?page=book&id=428820

7. Магауенов Р. Г. Системы охранной сигнализации: основы теории и принципы построения: Учеб. пособие. 3-е изд., перераб. и доп. / Р. Г. Магауенов. - М.: Горячая линия Телеком, 2017. - 494с.

8. Бурькова Е. В. Физическая защита объектов информатизации: учебное пособие / Оренбургский государственный университет 2017 – 158 с.

Дополнительные источники:

1. Технические средства автоматизации и управления: Учебное пособие / Шишов О. В. - М.: НИЦ ИНФРА-М, 2020. - 396 с.: 60x90 1/16. - ISBN 978-5-16-010325-9 https://znanium.com/read?id=361160

2. Бондарев П.В. Физическая защита ядерных объектов: Учебное пособие П.В. Бондарев, А.В. Измайлов, А.И. Толстой; Под ред. Н.С. Погожина. – М.: МИФИ, 2008. – 584 с.20

3. Козинный, А. Сейсмические средства обнаружения для охраны территориально распределенных объектов / А. Козинный, А. Косарев, В. Матвеев // БДИ, 2006. № 4. С. 74-77.

4. Груба И. И. Системы охранной сигнализации. Технические средства обнаружения. — М.: СОЛОН-ПРЕСС, 2012. — 220 с

5. Зенов, А. Ю. Концепция организации обработки информации в системах диагностики и распознавания / А. Ю. Зенов, М. П. Берестень // Инженерный вестник Дона: электрон, научн. журн. 2013. №1. [Электронный ресурс]. -URL: http://ivdon.ru/magazine/archive/nly2013/1568

6. Гагарина, Лариса Геннадьевна. Технические средства информатизации: Учебное пособие. - 1. - Москва: Издательский Дом "ФОРУМ" : ООО "Научно-издательский центр ИНФРА-М", 2019. - 256 с. - ISBN 978-5-8199-0734-4 http://znanium.com/go.php?id=1021128

7. Технические средства автоматизации и управления: Учебное пособие / Шишов О. В. - М.: НИЦ ИНФРА-М, 2021. - 396 с.: 60x90 1/16. - https://znanium.com/read?id=361160

8. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2021. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-00091-557-8.

https://znanium.com/catalog/document?id=364477

9. Периметровая пассивная сейсмическая система охраны объекта https://cyberleninka.ru/article/n/perimetrovaya-passivnaya-seysmicheskaya-sistemaohrany-obekta/viewer

10. Введенский, Б. С. Оборудование для охраны периметров / Б. С. Введенский-М.: «Мир безопасности», 2002. -112 с.

11. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. - М.: Горячая линия Телеком, 2010. - 272

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации».

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ (редакция, действующая с 1 марта 2021 года) «О персональных данных».

- Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1 (с изменениями на 9 марта 2021 года)

- Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ (с изменениями на 9 марта 2021 года)

- Доктрина информационной безопасности Российской Федерации21

- Положение «О государственной системе защиты информации в российской федерации от иностранных технических разведок

- и от ее утечки по техническим каналам» (извлечения). Утверждено Постановлением Совета Министров – Правительства Российской

- Федерации от 15.09.1993 № 912-51.

- Указ Президента Российской Федерации от 12 мая 2009 года № 537 «О Стратегии национальной безопасности Российской Федерации»

- Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

- Указ Президента Российской Федерации от 22 декабря 2017 года № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ (с изменениями на 22 декабря 2020 года) «О техническом регулировании».

- Федеральный закон от 4 мая 2011 г. № 99-ФЗ (с изменениями на 31 июля 2020 года) «О лицензировании отдельных видов деятельности».

- Федеральный закон от 30.12. 2001 № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» (с изменениями на 9 марта 2021 года) (редакция, действующая с 27 марта 2021 года).

- Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (с изменениями на 31 августа 2020 года).

- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями на 13 июля 2015 года).

- Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

- Положение о сертификации средств защиты информации. Постановление Правительства Российской Федерации от 26.06.1995 № 608.

- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.22

- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

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

- Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

- Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

- Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

Электронные издания (электронные ресурсы):

- Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

- Федеральный портал «Информационно - коммуникационные технологии в образовании» http://oso.rcsz.ru/info/kompas/edu.htm

- Всероссийский образовательный портал https://edu-ikt.ru/

- www.dedal.ru.

- www.neurophotonica.ru.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки**
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в ИТКС.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в ИТКС.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение

ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями.	- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; - проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение
ПК 3.4. Проводить отдельные работы по физической защите линий связи ИТКС.	выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение Экзамен

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	Экспертное наблюдение Экзамен
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение Экзамен
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Экспертное наблюдение Экзамен

		Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю. *Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы*

		Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю. *Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы*

ПК 4.4Обеспечивать применение средств защиты информации в компьютерной системе		Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю. Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы