Департамент образования Ярославской области
Государственное профессиональное образовательное учреждение Ярославской области
Переславский колледж им. А. Невского

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

по специальности **10.02.05**

Обеспечение информационной безопасности автоматизированных систем

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта по специальности СПО10.02.05 Обеспечение информационной безопасности автоматизированных систем

Организация-разработчик: ГПОУ ЯО Переславский колледж им. А. Невского

Разработчики: Шендрик А.Е., преподаватель ГПОУ ЯО Переславский колледж им. А. Невского

СОДЕРЖАНИЕ

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

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить вид деятельности *Защита информации техническими средствами* и соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	**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.

1.1.2. 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 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.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт в:	– выявлении технических каналов утечки информации; – применении, техническом обслуживании диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации; – проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
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 743 часа, из них:

- на освоение МДК – 453 час, в том числе на экзамены по МДК – 12 часов,
- на самостоятельную работу: по МДК - 44 часа, подготовка к экзамену по модулю - 4;
- на учебную практику – 126 часов;
- на производственную практику – 108 часов;
- экзамен по модулю - 8 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля ПМ.03 Защита информации техническими средствами

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 3.1-ПК.3.4 ОК 1–ОК10	**Раздел 1 модуля.** Техническая защита информации	**193**	**187**	98	–	90	–	**6**
ПК 3.5 ОК 01–ОК10	**Раздел 2 модуля.** Инженерно-технические средства физической защиты объектов информатизации	**304**	**266**	114	32	36	-	**38**
	Учебная практика УП.03	**126**						
ПК 3.1-ПК.3.5 ОК 1–ОК10	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	**108**					**108**	–
	Экзамен по профессиональному модулю	**12**	**8**	–	–	–	–	**4**
	Всего:	**743**	**461**	212	32	**126**	**108**	**48**

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов
1	2	3
Раздел 1 модуля. Применение технической защиты информации		**193**
МДК.03.01 Техническая защита информации		**187**
Раздел 1. Концепция инженерно-технической защиты информации		**5**
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	**1**
	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**	**4**
	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.	
Раздел 2. Теоретические основы инженерно-технической защиты информации		**32**
Тема 2.1. Информация как предмет защиты	**Содержание**	**6**
	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 занятия	**4**
	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	

Тема 2.2. Технические каналы утечки информации	**Содержание**	**6**
	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 занятия	**6**
	Определение и выявление каналов утечки информации с использованием приборов инженерно-технической защиты	
Тема 2.3. Методы и средства технической разведки	**Содержание**	**4**
	Классификация технических средств разведки. Методы и средства технической разведки.	
	Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	
	Практические и лабораторные занятия	**6**
	Проведение мероприятий средствами технической разведки по установленным методикам	
Раздел 3. Физические основы технической защиты информации		**22**
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**6**
	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	
	Практические и лабораторные занятия	**6**
	Измерение параметров физических полей	
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание**	**4**
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований.	
	Экранирование. Зашумление.	

	Практические и лабораторные занятия	**6**
	Организация подавления опасных сигналов с использованием приборов инженерно-технической защиты	
Раздел 4. Системы защиты от утечки информации		**82**
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**	**6**
	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 занятия	**6**
	Защита от утечки по акустическому каналу	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**	**6**
	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 занятия	**6**
	Организация защиты информации от утечки по проводному каналу с использованием приборов инженерно-технической защиты	
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**4**
	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 занятия	**6**
	Защита от утечки по виброакустическому каналу	
Тема 4.4. Системы	**Содержание**	**6**

защиты от утечки информации по электромагнитному каналу	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.	
	Практические и лабораторные занятия	**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**	**6**
	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 занятия	**8**
	Проведение мероприятий по защите телефонного канала от утечки информации с использованием приборов инженерно-технической защиты	
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 занятия	**6**
	Организация защиты информации от утечки по электросетевому каналу	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**	**4**
	Телевизионные системы наблюдения.	
	Приборы ночного видения. Системы защиты информации по оптическому каналу.	
	Практические и лабораторные занятия	**6**
	Проведение мероприятий по защите информации от утечки по оптическому каналу с использованием приборов инженерно-технической защиты	

Раздел 5. Применение и эксплуатация технических средств защиты информации		**40**
Тема 5.1. Применение технических средств защиты информации	**Содержание**	**8**
	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 электромагнитных 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 занятия	**12**
	Определение и выявление каналов утечки информации. Организация комплексной защиты информации от утечки по различным каналам. Работа с приборами инженерно-технической защиты	
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**	**8**
	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 занятия	**12**
	Техническое обслуживания приборов инженерно-технической защиты. Диагностика, выявление и устранение неисправностей, восстановление работоспособности приборов инженерно-технической защиты	
Самостоятельная работа для подготовки к промежуточной аттестации		**6**
Промежуточная аттестация в форме экзамена		**6**

Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации		**304**
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**266**
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		**44**
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**10**
	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 занятия	**8**
	Составление модели нарушителя на объекте. Осмотр территории и выявление путей и способов проникновения нарушителя на охраняемый объект.	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**12**
	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 занятия	**14**
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	
	Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		**120**
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической	**Содержание**	**12**
	Информационные основы построения системы охранной сигнализации.	
	Назначение, классификация технических средств обнаружения.	
	Построение систем обеспечения безопасности объекта.	

защиты	Состав систем обеспечения безопасности объекта	
	Периметровые средства обнаружения: назначение, устройство, принцип действия.	
	Объектовые средства обнаружения: назначение, устройство, принцип действия.	
	Практические и лабораторные занятия	**12**
	Монтаж датчиков пожарной и охранной сигнализации Работа со стендом «Охранно-пожарная сигнализация «Астра»	
Тема 2.2. Система контроля и управления доступом	**Содержание**	**12**
	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 занятия	**12**
	Проектирование с сборка различных схем контроля доступа на стенде «Системы контроля и управления доступом»	
	Программирование контролеров – добавление и удаление различных проксикарт (брелков, ТМ-ключей) на стенде «Системы контроля и управления доступом»	
Тема 2.3. Система телевизионного наблюдения	**Содержание**	**12**
	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 занятия	**12**
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	
Тема 2.4. Система	**Содержание**	**12**

сбора, обработки, отображения и документирования информации	Классификация системы сбора и обработки информации.	
	Схема функционирования системы сбора и обработки информации.	
	Варианты структур построения системы сбора и обработки информации.	
	Варианты структур построения системы сбора и обработки информации.	
	Устройства отображения и документирования информации.	
	Устройства отображения и документирования информации.	
	Практические и лабораторные занятия	**12**
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	
Тема 2.5 Система воздействия	**Содержание**	**12**
	Назначение технических средств воздействия.	
	Классификация технических средств воздействия.	
	Основные показатели технических средств воздействия.	
	Основные показатели технических средств воздействия.	
	Вспомогательные показатели технических средств воздействия.	
	Вспомогательные показатели технических средств воздействия.	
	Практические и лабораторные занятия	**12**
	Проектирование системы защиты территории на базе технических средств воздействия	
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		**64**
Тема 3.1 Применение инженерно-технических средств физической защиты	**Содержание**	**16**
	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.	
	Управление системой телевизионного наблюдения с автоматизированного рабочего места.	
	Порядок применения устройств отображения и документирования информации.	
	Управление системой воздействия.	
	Управление системой воздействия.	
	Практические и лабораторные занятия	**16**
	Организация защиты территории объекта и моделирование средств контроля на демонстрационном	

	стенде «Инфракрасные датчики контроля»	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**16**
	Этапы эксплуатации.	
	Виды и содержание проведения технического обслуживания инженерно-технических средств физической защиты.	
	Порядок проведения технического обслуживания инженерно-технических средств физической защиты.	
	Установка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	
	Настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	
	Диагностика технических средств физической защиты.	
	Устранение отказов и восстановление работоспособности технических средств физической защиты.	
	Организация ремонта технических средств физической защиты.	
	Практические и лабораторные занятия	**16**
	Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы наблюдение с использованием стенда «Инфракрасные датчики контроля»	
Курсовой проект (работа)		**32**
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. 4. Проектирование системы контроля и управления доступом на объекте. 5. Проектирование системы видеонаблюдения на объекте. 6. Проектирование системы ограничения доступа на территорию объекта. 7. Проектирование системы охранно-пожарной сигнализации объекта. 8. Проектирование системы защиты информации от утечки по различным каналам.		
Самостоятельная работа: подготовка курсовой работы		**32**

Самостоятельная работа для подготовки к промежуточной аттестации	**6**
Промежуточная аттестация в форме экзамена	**6**
Учебная практика по разделу 2 модуля 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.	**126**
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.	***108***
Самостоятельная работа для подготовки к промежуточной аттестации	**4**
Экзамен по профессиональному модулю	***8***
Всего	***743***

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

лекционные аудитории с мультимедийным оборудованием; лаборатория «Технических средств защиты информации».

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

Оборудование лаборатории «Технических 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.

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2017.

2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2017.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2017. – 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», 2018. – 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. – 2016

7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2017

8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2017. – 416 с.

3.2.2. Дополнительные печатные источники:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
8. 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».
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
11. 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.
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
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.
18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

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

22. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

23. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

25. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

26. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

27. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

28. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

29. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

30. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

31. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

33. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

34. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

35. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.

Номенклатура показателей качества. Ростехрегулирование, 2005.

38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

40. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

41. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

42. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

43. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

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

45. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

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

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

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

50. 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.

3.2.3 Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые 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	Демонстрировать умения и практические навыки в установке, монтаже, настройке ипроведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 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	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять 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	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
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	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОП 02.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	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	

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)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной	- эффективность использования информационно-коммуникационных	

деятельности.	технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	