Министерство образования Ставропольского края
Государственное бюджетное профессиональное образовательное учреждение
«Пятигорский техникум торговли, технологий и сервиса»
(ГБПОУ ПТТТиС)

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация – техник по защите информации

2024 г.

СОДЕРЖАНИЕ

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

1.1. Область применения программы

Рабочая программа профессионального модуля (далее рабочая программа) – является частью основной профессиональной образовательной программы по специальности СПО в соответствии с ФГОС по специальности СПО образования 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» укрупненной группы 10.00.00 Информационная безопасность базовой подготовки в части освоения основного вида профессиональной деятельности (ВПД):

Защита информации техническими средствами и соответствующих профессиональных компетенций (ПК):

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.

1.2 Цель и планируемые результаты освоения профессионального модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

1.3 В результате освоения профессионального модуля студент должен:

Владеть навыками	– 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. – Корректировки конструкторской документации на изготовление средства защиты информации от несанкционированного доступа для поставки, контроля и испытаний. – Отработки конструкции средства защиты информации на технологичность с учетом стандартов ЕСТД; – Заключения договоров с поставщиками комплектующих изделий и материалов и лицензионных соглашений с правообладателями на использование объектов промышленной и интеллектуальной собственности – Сертификационных испытаний технических средств защиты информации от несанкционированного доступа на соответствие требованиям безопасности информации; – Испытания опытного образца защищенного технического средства обработки информации на соответствие техническим условиям.
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 – Оценивать защищенность ограждающих конструкций помещения от утечки информации по акустическому каналу – Оценивать защищенность ограждающих конструкций от утечки информации по виброакустическому каналу комплексом – Проводить статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении. – Проводить техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок – Устранять выявленные неисправности технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок – Проводить ремонт с привлечением производителей технических средств защиты информации – Оценивать защищенность телефонных каналов – Оценивать защищенность помещения от утечки информации по каналам акустоэлектрических преобразований технических средств

	– Обнаруживать ПЭМИ по электрической составляющей электромагнитного поля – Оценивать состояние трассы наблюдения – Проводить испытания защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами – Организовывать технический контроль эффективности мер защиты информации – Проводить оценку разведдоступности – Проводить комплекс работ по проверке возможности утечки информации по техническим каналам – Проводить оценку защищенности объекта информатизации – Разрабатывать проект системы видеонаблюдения для торговой организации – Настраивать системы телевизионного наблюдения с учетом специфики деятельности организации – Определять состав ССОИ для образовательной организации – Испытывать на устойчивость технические средства охраны – Разрабатывать проекты применения технических средств воздействия для образовательной организации – Изготовлять технические средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок – Отрабатывать конструкции технического средства защиты информации на технологичность с учетом стандартов ЕСТД – Проверять работоспособность средств защиты информации от несанкционированного доступа и специальных воздействий, выполнение правил их эксплуатации – Выполнять правила их эксплуатации средств защиты информации
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. – Технические каналы утечки информации при передаче ее по каналам связи – Демаскирующие признаки объектов – Средства выявления каналов утечки информации – Техническая разведка: определение, классификация, возможности. Формы разведывательной деятельности. – Основные этапы и процедуры добывания информации технической разведкой – Нормативные документы по противодействию технической разведке – Задачи систем защиты информации – Способы защиты технических средств обработки информации от утечки по техническим каналам – Возможности средств акустической речевой разведки – Особенности реализации пассивных мер защиты в виброакустических каналах утечки речевой информации – Средства контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок. – Порядок устранения неисправностей средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок – Организации ремонта средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок – Возможности приборов видеонаблюдения. Использование длиннофокусных фотоаппаратов – Защита информации в оптическом диапазоне частот. – Средства оценки и анализа оптического канала утечки информации – Способы уничтожения информации – Специальные средства для экспресс-копирования информации (или ее уничтожения) с магнитных носителей – Специальные технические средства для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи – Нормативные документы, регламентирующие применение технических средств защиты информации – Скрытие и защита информации от утечки по техническим каналам – Методы и средства инженерной защиты и технической охраны объектов – Порядок эксплуатации программных и технических средств и систем защиты секретной информации от НСД – Порядок приемки СЗСИ перед сдачей в эксплуатацию в составе АС – Типовой вариант КПП – Быстроразвертываемые комплексы ТСО: состав, отличительные особенности, преимущества от внедрения – Номенклатура применяемых средств обнаружения (вибрационные, комбинированные, магнитометрические, объектовые) – Сравнительный анализ применения шлюзового турникета и маятниковой двери-шлюза

	– Дополнительное оборудование систем телевизионного наблюдения. – Организация охраны объектов с примснением технических средств воздействия – Нормативная документация использования технических средств физической защиты. Единая система конструкторской документации. Единая система технологической документации Особенности выбора инженерно-технических средств физической защиты периметров протяженных объектов. Особенности монтажа

1.4. Количество часов на освоение программы профессионального модуля:

Всего часов – 812 часов

В том числе в форме практической подготовки – 480 часов

Из них на освоение МДК 03.01 – 222 часов

В том числе самостоятельная работа – 4 часа

Промежуточная аттестация в форме экзамена – 3 часа

Из них на освоение МДК 03.02 –178 часов

В том числе самостоятельная работа – 4 часа

Промежуточная аттестация в формс экзамена – 3 часа

Практики, в том числе учебная – 144 часа

производственная – 144 часа

Промежуточная аттестация в форме экзамена по модулю – 6 часов

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД) Защита информации техническими средствами, в том числе профессиональными (ПК) и общими (ОК) компетенциями и личностными результатами (ЛР).

Код	Наименование результата обучения
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.
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.
ЛР 1.	Осознающий себя гражданином и защитником великой страны
ЛР 2.	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости,

	экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций
ЛР 3.	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих
ЛР 4.	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР 5.	Демонстрирующий приверженность к родной культуре, исторической памяти на основе любви к Родине, родному народу, малой родине, принятию традиционных ценностей многонационального народа России
ЛР.6	Проявляющий уважение к людям старшего поколения и готовность к участию в социальной поддержке и волонтерских движениях
ЛР.7	Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.
ЛР.8	Проявляющий и демонстрирующий уважение к представителям различных этнокультурных, социальных, конфессиональных и иных групп. Сопричастный к сохранению, преумножению и трансляции культурных традиций и ценностей многонационального российского государства
ЛР.9.	Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях
ЛР 10.	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой
ЛР 11.	Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры
ЛР 12.	Принимающий семейные ценности, готовый к созданию семьи и воспитанию детей; демонстрирующий неприятие насилия в семье, ухода от родительской ответственности, отказа от отношений со своими детьми и их финансового содержания
ЛР КК 1.	Признающий ценность непрерывного образования, ориентирующийся в изменяющемся рынке труда, избегающий безработицы, управляющий собственным профессиональным развитием, рефлексивно оценивающий собственный жизненный опыт, критерии успешности
ЛР КК 2.	Экономически активный, предприимчивый, готовый к самозанятости

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Структура профессионального модуля

Коды профессиональных и общих компетенций, личностных результатов	Наименования разделов профессионального модуля			Объем профессионального модуля, ак.час.					
				Работа обучающихся во взаимодействии с преподавателем					
					Обучение по МДК		Практики		Самостоятельная работа
		Всего, час.	В т.ч. в форме практ. подготовки	Всего	В том числе				
					Лаборат и практ. занятий	Курсовых работ (проектов)	Учебная	Производственная	
1	2	3	4	5	6	8	9	10	12
ПК 3.1- ПК.3.4 ОК 1-10 ЛР 1-11, КК1, КК 2	МДК 03.01 Техническая защита информации	**301**	142	**221**	70	-	**72**	-	**4**
ПК 3.5 ОК 1-10 ЛР 1-11, КК1, КК 2	МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации	**257**	132	**177**	60	30	**72**	-	**4**
	Производственная практика (по профилю специальности), часов	**144**	144					144	-
	Промежуточная аттестация	**6**	6					-	-
	Всего	**708**	424	398	130	30	144	144	8

3.2. 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, ак. ч / в том числе в форме практической подготовки, ак. ч
1	2	3
Раздел 1 модуля. Применение технической защиты информации		
МДК.03.01 Техническая защита информации		***301/142***
В том числе промежуточная аттестация		***6***
Раздел 1. Концепция инженерно-технической защиты информации		
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	***4***
	Тема 1.1.1. Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности.	2
	Тема 1.1.2. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	2
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание**	**4**
	Тема 1.2.1. Задачи и требования к способам и средствам защиты информации техническими средствами.	2
	Тема 1.2.2. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.	2

Раздел 2. Теоретические основы инженерно-технической защиты информации		
Тема 2.1. Информация как предмет защиты	**Содержание**	**10**
	Тема 2.1.1. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации.	2
	Тема 2.1.2. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов.	2
	Тема 2.1.3. Основные и вспомогательные технические средства и системы.	2
	Тема 2.1.4. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	2
	Тематика практических занятий и лабораторных работ	**2**
	Тема 2.1.5. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	2
Тема 2.2. Технические каналы утечки информации	**Содержание**	**14**
	Тема 2.2.1. Понятие и особенности утечки информации. Структура канала утечки информации.	2
	Тема 2.2.2. Классификация существующих физических полей и технических каналов утечки информации.	2
	Тема 2.2.3. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	2
	Тема 2.2.4. *Технические каналы утечки информации при передаче ее по каналам связи*	*2*
	Тема 2.2.5. *Демаскирующие признаки объектов*	*2*
	Тема 2.2.6. *Средства выявления каналов утечки информации*	*2*
	Тематика практических занятий и лабораторных работ	**2**
	Тема 2.2.7. Определение канала утечки информации. Проведение сравнительного анализа каналов.	2
Тема 2.3. Методы и средства технической разведки	**Содержание**	**16**
	Тема 2.3.1. *Техническая разведка: определение, классификация, возможности. Формы разведывательной деятельности.*	*2*
	Тема 2.3.2. *Основные этапы и процедуры добывания информации технической разведкой*	*2*

	Тема 2.3.3. Классификация технических средств разведки. Методы и средства технической разведки.	2
	Тема 2.3.4. *Нормативные документы по противодействию технической разведке*	*2*
	Тема 2.3.5. Средства несанкционированного доступа к информации.	2
	Тема 2.3.6. Средства и возможности оптической разведки. Средства дистанционного съема информации.	2
	Тема 2.3.7. *Задачи систем защиты информации*	*2*
	Тематика практических занятий и лабораторных работ	**2**
	Тема 2.3.8. Планирование мероприятий по определению возможных средств организации технической разведки	2
Раздел 3. Физические основы технической защиты информации		
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**10**
	Тема 3.1.1. Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования.	2
	Тема 3.1.2. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.	2
	Тема 3.1.3. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.	2
	Тема 3.1.4. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	2
	Тематика практических занятий и лабораторных работ	**2**
	Тема 3.1.5. Измерение параметров физических полей	2
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание**	**8**
	Тема 3.2.1. Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований.	2
	Тема 3.2.2. Скрытие речевой информации в каналах связи. Экранирование. Зашумление.	2
	Тема 3.2.3. *Способы защиты технических средств обработки информации от утечки по*	*2*

	техническим каналам	
	Тематика практических занятий и лабораторных работ	**2**
	Тема 3.2.4. Организация мероприятий по скрытию речевой информации в каналах связи	2
Раздел 4. Системы защиты от утечки информации		
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**	**20**
	Тема 4.1.1. Технические средства акустической разведки. Непосредственное подслушивание звуковой информации.	2
	Тема 4.1.2. *Возможности средств акустической речевой разведки*	*2*
	Тема 4.1.3. *Особенности реализации пассивных мер защиты в виброакустических каналах утечки речевой информации*	*2*
	Тема 4.1.4. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу.	2
	Тема 4.1.5. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	2
	Тема 4.1.6. *Средства контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок.*	*2*
	Тема 4.1.7. *Порядок устранения неисправностей средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок*	*2*
	Тема 4.1.8. *Организации ремонта средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок*	*2*
	Тематика практических занятий и лабораторных работ	**4**
	Тема 4.1.9. Защита от утечки по акустическому каналу	2
	Тема 4.1.10. *Оценка защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу*	*2*
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**	**8**
	Тема 4.2.1. Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов.	2
	Тема 4.2.2. Негласная запись информации на диктофоны. Системы защиты от диктофонов.	2
	Тема 4.2.3. Номенклатура применяемых средств защиты информации от несанкционированной	2

	утечки по проводному каналу.	
	Тематика практических занятий и лабораторных работ	**2**
	Тема 4.2.4. Организация системы защиты информации от несанкционированной утечки по проводному каналу.	2
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**10**
	Тема 4.3.1. Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи.	2
	Тема 4.3.2. Системы защиты информации от утечки по вибрационному каналу.	2
	Тема 4.3.3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	2
	Тематика практических занятий и лабораторных работ	**4**
	Тема 4.3.4. *Оценка защищенности ограждающих конструкций от утечки информации по виброакустическому каналу комплексом*	*2*
	Тема 4.3.5. Защита от утечки по виброакустическому каналу	2
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	**20**
	Тема 4.4.1. Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок.	2
	Тема 4.4.2. Приемники информации с радиозакладок. Прослушивание информации с пассивных закладок.	2
	Тема 4.4.3. Системы защиты от утечки по электромагнитному каналу.	2
	Тема 4.4.4. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	2
	Тематика практических занятий и лабораторных работ	**12**
	Тема 4.4.5. Определение каналов утечки ПЭМИН	2
	Тема 4.4.6. Защита от утечки по цепям электропитания и заземления	2
	Тема 4.4.7. *Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении.*	*2*
	Тема 4.4.8. *Проведение технического обслуживания технических средств за щиты информации от утечки за счет побочных электромагнитных излучений и наводок*	*2*

	Тема 4.4.9. *Устранение выявленных неисправностей технических средств за щиты информации от утечки за счет побочных электромагнитных излучений и наводок*	*2*
	Тема 4.4.10. *Проведение ремонта с привлечением производителей технических средств защиты информации*	*2*
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**10**
	Тема 4.5.1. Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.	2
	Тема 4.5.2. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи.	2
	Тема 4.5.3. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	2
	Тематика практических занятий и лабораторных работ	**4**
	Тема 4.5.4. Защита от утечки информации по телефонному каналу	2
	Тема 4.5.5. *Оценка защищенности телефонных каналов*	2
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**10**
	Тема 4.6.1. Низкочастотное устройство съема информации. Высокочастотное устройство съема информации.	2
	Тема 4.6.2. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	2
	Тематика практических занятий и лабораторных работ	**6**
	Тема 4.6.3. *Оценка защищенности помещения от утечки информации по каналам акустоэлектрических преобразований технических средств*	2
	Тема 4.6.4. Организация защиты информации от несанкционированной утечки по электросетевому каналу.	2
	Тема 4.6.5. *Обнаружение ПЭМИ по электрической составляющей электромагнитного поля*	*2*
Тема 4.7. Системы защиты от утечки информации по	**Содержание**	**14**
	Тема 4.7.1. Телевизионные системы наблюдения. Приборы ночного видения.	2
	Тема 4.7.2. *Возможности приборов видеонаблюдения. Использование длиннофокусных*	*2*

оптическому каналу	*фотоаппаратов*	
	Тема 4.7.3. *Защита информации в оптическом диапазоне частот.*	*2*
	Тема 4.7.4. Системы защиты информации по оптическому каналу.	2
	Тема 4.7.5. *Средства оценки и анализа оптического канала утечки информации*	*2*
	Тематика практических занятий и лабораторных работ	**4**
	Тема 4.7.6. *Оценка состояния трассы наблюдения*	*2*
	Тема 4.7.7. Организация защиты информации по оптическому каналу.	2
Раздел 5. Применение и эксплуатация технических средств защиты информации		
Тема 5.1. Применение технических средств защиты информации	**Содержание**	**30**
	Тема 5.1.1. *Способы уничтожения информации*	*2*
	Тема 5.1.2. Технические средства для уничтожения информации и носителей информации, порядок применения.	2
	Тема 5.1.3. *Специальные средства для экспресс-копирования информации (или ее уничтожения) с магнитных носителей*	*2*
	Тема 5.1.4. *Специальные технические средства для негласного получения (изменения, уничтожения) информации с технических средств ее хранения, обработки и передачи*	*2*
	Тема 5.1.5. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.	2
	Тема 5.1.6. *Нормативные документы, регламентирующие применение технических средств защиты информации*	*2*
	Тема 5.1.7. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.	2
	Тема 5.1.8. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	2
	Тема 5.1.9. *Скрытие и защита информации от утечки по техническим каналам*	*2*
	Тема 5.1.10. *Методы и средства инженерной защиты и технической охраны объектов*	*2*
	Тематика практических занятий и лабораторных работ	**10**
	Тема 5.1.11. Организация защиты информации в условиях применения мобильных устройств	2

	обработки и передачи данных.	
	Тема 5.1.12. Измерение параметров побочных электромагнитных излучений и наводок при проведении аттестации объектов	2
	Тема 5.1.13. *Проведение испытаний защищенных технических средств обработки информации в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами*	*2*
	Тема 5.1.14. Проведение измерений параметров фоновых шумов при использовании технических средств защиты информации	2
	Тема 5.1.15. *Организация технического контроля эффективности мер защиты информации*	*2*
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**	**30**
	Тема 5.2.1. *Порядок эксплуатации программных и технических средств и систем защиты секретной информации от НСД*	*2*
	Тема 5.2.2. Этапы эксплуатации технических средств защиты информации.	2
	Тема 5.2.3. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.	2
	Тема 5.2.4. Установка и настройка технических средств защиты информации.	2
	Тема 5.2.5. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.	2
	Тема 5.2.6. Организация ремонта технических средств защиты информации.	2
	Тема 5.2.7. *Порядок приемки СЗСИ перед сдачей в эксплуатацию в составе АС*	*2*
	Тема 5.2.8. Проведение аттестации объектов информатизации.	2
	Тематика практических занятий и лабораторных работ	**14**
	Тема 5.2.9. Проведение технического обслуживания телефонных аппаратов	2
	Тема 5.2.10. Проведение технического обслуживания шредеров	2
	Тема 5.2.11. Проведение первичного осмотра помещений при аттестации объекта информатизации.	2
	Тема 5.2.12. *Проведение оценки разведдоступности*	*2*
	Тема 5.2.13. *Комплекс работ по проверке возможности утечки информации по техническим каналам*	*2*

	Тема 5.2.14. Оценка защищенности объекта информатизации	*2*
	Тема 5.2.15. Подготовка пакета документов для проведения аттестации объекта информатизации.	2
Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации		
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		*257/132*
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**10**
	Тема 1.1.1. Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации.	4
	Тема 1.1.2. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.	2
	Тематика практических занятий и лабораторных работ	**4**
	Тема 1.1.3. Построение модели нарушителя, определение способов его проникновения на объект, на примере образовательной организации	2
	Тема 1.1.4. Построение модели нарушителя, определение способов его проникновения на объект, на примере производственной организации	2
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**20**
	Тема 1.2.1. Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны.	6
	Тема 1.2.2. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты.	4
	Тема 1.2.3. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	2
	Тема 1.2.4. Типовой вариант КПП	*2*
	Тема 1.2.5. *Быстроразвертываемые комплексы ТСО: состав, отличительные особенности, преимущества от внедрения*	*2*
	Тематика практических занятий и лабораторных работ	**4**
	Тема 1.2.6. Определение состава инженерных конструкций, необходимых для предотвращения	2

	проникновения злоумышленника	
	Тема 1.2.7. Разработка проекта монтажа инженерных конструкций на территории организации	2
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 2.1. Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**	**14**
	Тема 2.1.1. Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта.	4
	Тема 2.1.2. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	4
	Тема 2.1.3. *Номенклатура применяемых средств обнаружения (вибрационные, комбинированные, магнитометрические, объектовые)*	2
	Тематика практических занятий и лабораторных работ	**4**
	Тема 2.1.4. Монтаж датчиков пожарной сигнализации	2
	Тема 2.1.5. Монтаж датчиков охранной сигнализации	2
Тема 2.2. Система контроля и управления доступом	**Содержание**	**22**
	Тема 2.2.1. Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД.	4
	Тема 2.2.2. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД.	2
	Тема 2.2.3. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	6
	Тема 2.2.4. *Сравнительный анализ применения шлюзового турникета и маятниковой двери-шлюза*	2
	Тематика практических занятий и лабораторных работ	**8**
	Тема 2.2.5. Рассмотрение принципов устройства и работы аппаратных средств аутентификации пользователя	2
	Тема 2.2.6. Рассмотрение принципов применения аппаратных средств аутентификации	2

	пользователя	
	Тема 2.2.7. Рассмотрение принципов устройства и работы средств контроля доступа	2
	Тема 2.2.8. Рассмотрение принципов применения средств контроля доступа	2
Тема 2.3. Система телевизионного наблюдения	**Содержание**	**20**
	Тема 2.3.1. Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения.	2
	Тема 2.3.2. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	6
	Тема 2.3.3. *Дополнительное оборудование систем телевизионного наблюдения.*	2
	Тематика практических занятий и лабораторных работ	**10**
	Тема 2.3.4. Рассмотрение принципов устройства средств видеонаблюдения.	2
	Тема 2.3.5. Рассмотрение принципов работы средств видеонаблюдения.	2
	Тема 2.3.6. Рассмотрение принципов применения средств видеонаблюдения.	2
	Тема 2.3.7. *Разработка проекта системы видеонаблюдения для торговой организации*	*2*
	Тема 2.3.8. *Настройка систем телевизионного наблюдения с учетом специфики деятельности организации*	*2*
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание**	**12**
	Тема 2.4.1. Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации.	2
	Тема 2.4.2. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	2
	Тематика практических занятий и лабораторных работ	**8**
	Тема 2.4.3. Рассмотрение принципов устройства системы сбора и обработки информации.	2
	Тема 2.4.4. Рассмотрение принципов работы системы сбора и обработки информации.	2
	Тема 2.4.5. Рассмотрение применения системы сбора и обработки информации.	2
	Тема 2.4.6. *Определение состава ССОИ для образовательной организации*	2
Тема 2.5. Система воздействия	**Содержание**	**12**
	Тема 2.5.1. Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	2

	Тема 2.5.2. *Организация охраны объектов с применением технических средств воздействия*	*2*
	Тематика практических занятий и лабораторных работ	**8**
	Тема 2.5.3. Мониторинг эффективности технических средств воздействия для гражданских организаций	2
	Тема 2.5.4. Определение эффективности технических средств воздействия для гражданских организаций	2
	Тема 2.5.5. *Испытание на устойчивость технических средств охраны*	*2*
	Тема 2.5.6. *Разработка проекта применения технических средств воздействия для образовательной организации*	*2*
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		
Тема 3.1. Применение инженерно-технических средств физической защиты	**Содержание**	**16**
	Тема 3.1.1. *Нормативная документация использования технических средств физической защиты. Единая система конструкторской документации. Единая система технологической документации*	*2*
	Тема 3.1.2. Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом.	2
	Тема 3.1.3. *Особенности выбора инженерно-технических средств физической защиты периметров протяженных объектов. Особенности монтажа*	*2*
	Тема 3.1.4. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места.	4
	Тема 3.1.5. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	2
	Тематика практических занятий и лабораторных работ	**4**
	Тема 3.1.6. Определение эффективности применения сигнально-охранных пиротехнических устройств для гражданских организаций	2
	Тема 3.1.7. *Изготовление технического средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок*	2
Тема 3.2. Эксплуатация инженерно-технических	**Содержание**	**18**
	Тема 3.2.1. Этапы эксплуатации. Виды, содержание и порядок проведения технического	2

средств физической защиты	обслуживания инженерно-технических средств физической защиты.	
	Тема 3.2.2. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	2
	Тема 3.2.3. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.	4
	Тематика практических занятий и лабораторных работ	**10**
	Тема 3.2.4. Проведение диагностики систем видеонаблюдения	2
	Тема 3.2.5. Настройка межсетевого экрана для защиты информации, не составляющей государственную тайну по 4 классу (Cisco ASA)	2
	Тема 3.2.6. *Отработка конструкции технического средства защиты информации на технологичность с учетом стандартов ЕСТД*	*2*
	Тема 3.2.7. *Проверка работоспособности средств защиты информации от несанкционированного доступа и специальных воздействий, выполнение правил их эксплуатации*	*2*
	Тема 3.2.8. *Выполнение правил их эксплуатации средств защиты информации*	*2*
Курсовой проект (работа)		**30**
Примерная тематика курсового проекта (работы) 1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества. 4. Разработка проекта системы обеспечения безопасности для образовательной организации 5. Разработка проекта системы обеспечения безопасности для торговой организации 6. Разработка проекта системы обеспечения безопасности для промышленного предприятия 7. Разработка проекта системы обеспечения безопасности для банковской организации 8. Разработка проекта КПП для гражданской организации 9. Разработка проекта систем телевизионного наблюдения для образовательной организации 10. Разработка мероприятий применения пассивных методов защиты акустической информации. 11. Разработка мероприятий применения активных методов защиты акустической информации.		

12. Подготовка пакета документов для проведения аттестации объекта информатизации на примере организации.	
Промежуточная аттестация по ПМ 03 в форме экзамена	**6**
Примерная тематика самостоятельной работы	**8**
1. Обзор современных технических средств защиты информации *2. Статистика и анализ крупных атак технической разведки* *3. Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты.* *4. Размещение периметровых средств обнаружения на местности.*	
Тематика домашних заданий	
1. Изучение аналитических обзоров в области построения систем защиты от утечки информации 2. Выполнение индивидуального задания по теме «Комплекс мер по защите от утечки информации для автономного объекта». 3. Выполнение индивидуального задания по теме «Анализ уязвимости каналов передачи информации объекта защиты» 4. Изучение аналитических обзоров в области построения систем защиты информации 5. Оценка защищенности беспроводной линии связи 6. Выполнение индивидуального задания по теме «Анализ уязвимости акустического канала передачи информации объекта защиты» 7. Выполнение индивидуального задания по теме «Анализ уязвимости проводного канала передачи информации объекта защиты» 8. Выполнение индивидуального задания по теме «Анализ уязвимости вибрационного канала передачи информации объекта защиты» 9. Выполнение индивидуального задания по теме «Анализ уязвимости электромагнитного канала передачи информации объекта защиты» 10. Выполнение индивидуального задания по теме «Анализ уязвимости телефонного канала передачи информации объекта защиты» 11. Выполнение индивидуального задания по теме «Анализ уязвимости электросетевого канала передачи информации объекта защиты» 12. Выполнение индивидуального задания по теме «Анализ уязвимости оптического канала передачи информации объекта защиты» 13. Обзор существующих средств принудительной остановки транспорта	

14. Разработка проекта применения комбинированных средств обнаружения 15. Обзор IP-камер 16. Компьютерная система синхронного стенографирования 17. Заграждение пассивное «Зверобой» 18. Система газового подавления «Армагеддон» 19. Система газового подавления «Смерч» 20. Средства обнаружения проноса/провоза запрещенных предметов и веществ 21. Системы автономного электропитания на основе альтернативных источников энергии 22. Настройка межсетевого экрана с внутренним интерфейсом Ethernet0/1.10 23. Настройка маршрута по умолчанию для межсетевого экрана 24. Настройка DHCP сервера для межсетевого экрана	
Учебная практика	**144**
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. 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. 17. *Корректировка конструкторской документации на изготовление средства защиты информации от несанкционированного доступа для поставки, контроля и испытаний.* 18. *Отработка конструкции средства защиты информации на технологичность с учетом стандартов ЕСТД;* 19. *Заключение договоров с поставщиками комплектующих изделий и материалов и лицензионных соглашений с правообладателями на использование объектов промышленной и интеллектуальной собственности*	
Производственная практика	***144***
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. 5. *Корректировка конструкторской документации на изготовление средства защиты информации от несанкционированного доступа для поставки, контроля и испытаний.* 6. *Отработка конструкции средства защиты информации на технологичность с учетом стандартов ЕСТД;* 7. *Заключение договоров с поставщиками комплектующих изделий и материалов и лицензионных соглашений с правообладателями на использование объектов промышленной и интеллектуальной собственности;* 8. *Сертификационные испытания технических средств защиты информации от несанкционированного доступа на соответствие требованиям безопасности информации;* 9. *Испытания опытного образца защищенного технического средства обработки информации на соответствие техническим условиям.*	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 - ознакомительный (узнавание ранее изученных объектов, свойств);

2 - репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 - продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

4.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Кабинет № 21 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.

Аппаратные средства аутентификации пользователя, средства защиты информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок

- глушилка мобильных телефонов GPS 600- С;

средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических колебаний, стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, система видеонаблюдения и охраны объектов

Подавитель Скорпион GSM+CPS,

Фильтр сетевой и помехоподавляющий ФП – 6,

Система видеонаблюдения ISON TOR –SE -1.

4.2. Информационное обеспечение обучения

4.2.1. Основные печатные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации.:/ А.П. Зайцев, Р.В.Мещеряков, А.А.Шелупанов 7-е изд., испр. 2014. - ISBN 654-8-4468-7764-5 Текст : непосредственный.

2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. :/ Т.С. Пеньков— М. 2015. —ISBN 852-4-5691-7764-5 _ Текст : непосредственный.

3. Новиков В.К. Организационное и правовое обеспечение информационной

безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. :/ В.К. Новиков – М.: МИЭТ, 2013. – 172 с. – ISBN 852-8-4468-3258-5 - Текст : непосредственный.

4. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. Образования :/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с – ISBN 357-8-4468-3258-5 - Текст : непосредственный.

5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие :/ М.А. Иванов , И.В. Чугунков - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений. – ISBN 128-8-4468-3258-9 - Текст : непосредственный.

6. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации :/ В.П. Мельников, С.А. Клейменов, А.М. Петраков М.: Академия, - 336 с. – 2012 – ISBN 258-8-4468-3668-9 - Текст : непосредственный.

7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012 – ISBN 658-8-4558-3258-3 - Текст : непосредственный.

8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с. – ISBN 567-8-4558-3258-2 - Текст : непосредственный.

4.2.2. Дополнительные печатные источники:

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

10. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

11. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

12. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

13. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

14. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

15. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

16. 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».

17. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

18. 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.

19. 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.

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

21. 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.

22. 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.

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

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

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

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

27. Руководящий документ. Геоинформационные системы. Защита

информации от несанкционированного доступа. Трсбования по защите информации. Утвержден ФСТЭК России, 2008.

28. 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.

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

30. 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

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

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

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

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

35. 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

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

37. 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

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

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

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

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

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

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

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

45. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
Номенклатура показателей качества. Ростехрегулирование, 2005.

46. 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.

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

48. 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.

49. 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.

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

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

52. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден

Гостехкомиссией России, 2002.

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

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

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

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

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

58. 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.

4.2.3 Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru – Текст : электронный.
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru – Текст : электронный.
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/ – Текст : электронный.
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru – Текст : электронный.
5. Справочно-правовая система «Гарант» » www.garant.ru – Текст : электронный.
6. Федеральный портал «Российское образование www.edu.ru – Текст : электронный.
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/ – Текст : электронный.

8. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru – Текст : электронный.

9. Сайт Научной электронной библиотеки www.elibrary.ru – Текст : электронный.

5. 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 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- участие в профориентационной работе; - участие в профессиональных конкурсах; - участие в научно-исследовательской работе.	-отчеты по итогам производственной (по профилю специальности) практики. - создание портфолио обучающихся. - отзывы научных руководителей.
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- планирование информационного поиска из широкого набора источников, необходимого для выполнения профессиональных задач; - проведение анализа полученной информации, выделяет в ней главные аспекты; структурировать отобранную информацию в соответствии с параметрами поиска; - интерпретация полученной информации в контексте профессиональной	Наблюдение и экспертная оценка на практических занятиях и при выполнении работ на учебной практике

	деятельности	
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.	- использование актуальной нормативно-правовой документацию по специальности; - применение современной научной профессиональной терминологии; - определение траектории профессионального развития и самообразования	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках
ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- участие в деловом общении для эффективного решения деловых задач; - планирование профессиональной деятельности; - организация работы коллектива и команды; - взаимодействие с коллегами, руководством, клиентами в ходе профессиональной деятельности.	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- использование вербальных и невербальных способов коммуникации на государственном языке с учетом особенностей и различий социального и культурного контекста; - соблюдение норм публичной речи и регламента; - самостоятельный выбор стиля монологического высказывания (служебный доклад, выступление на совещании, презентация проекта и т.п.) в зависимости от его цели и целевой аудитории и с учетом особенностей и различий социального и культурного контекста; - создание продукта письменной коммуникации определенной структуры на государственном языке; - самостоятельный выбор стиля (жанра) письменной	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках

	коммуникации на государственном языке в зависимости от цели, содержания и адресата.	
ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- осознание конституционных прав и обязанностей; - соблюдение закона и правопорядка. - участие в мероприятиях гражданско-патриотического характера, волонтерском движении. - аргументированное представление и отстаивание свое мнение с соблюдением этических норм и общечеловеческих ценностей. - осуществление своей деятельности на основе соблюдения этических норм и общечеловеческих ценностей; - демонстрирование сформированности российской гражданской идентичности, патриотизма, уважения к своему народу, уважения к государственным символам (гербу, флагу, гимну).	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- обладание нормами экологической чистоты и безопасности. - осуществление деятельности по сбережению ресурсов и сохранению окружающей среды. - прогнозирование техногенные последствия для окружающей среды, бытовой и производственной деятельности человека; - прогнозирование возникновений опасных ситуаций по характерным признакам их появления, а также на основе анализа специальной информации,	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках

	получаемой из различных источников; - владение приемами эффективных действий в опасных и чрезвычайных ситуациях природного, техногенного и социального характера.	
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- классифицирование оздоровительных систем физического воспитания, направленных на укрепление здоровья, профилактику профессиональных заболеваний, вредных привычек и увеличения продолжительности жизни; - соблюдение норм здорового образа жизни, осознанное выполнение правил безопасности жизнедеятельности; - составление своего индивидуального комплекса физических упражнений для поддержания необходимого уровня физической подготовленности; - организация собственной деятельности по укреплению здоровья и физической выносливости	Наблюдение и экспертная оценка на практических занятиях и при выполнении работ на учебной практике
ОК 9. Использовать информационные технологии в профессиональной деятельности.	- планирование информационного поиска; - принятие решения о завершении (продолжении) информационного поиска на основе оценки достоверности (противоречивости) полученной информации для решения профессиональных задач; - осуществление обмена информации с использованием современного оборудования и программного обеспечения,	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках

	в том числе на основе сетевого взаимодействия; - анализ информации, выделение в ней главных аспектов, структурирование, презентация.	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- изучение нормативно-правовой документации, технической профессиональной документации на государственном и иностранном языке, литературы и современных научных разработок в области будущей профессиональной деятельности на государственном языке; - применение необходимого лексического и грамматического минимума для чтения и перевода иностранных текстов профессиональной направленности; - владение современной научной и профессиональной терминологией; - самостоятельное совершенствование устной и письменной речи и пополнение словарного запаса; - владение навыками технического перевода текста, понимание содержания инструкций и графической документации на иностранном языке в области профессиональной деятельности.	Наблюдение и экспертная оценка на учебных занятиях и на учебной и производственной (по профилю специальности) практиках