МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования «Саратовский государственный технический
университет имени Гагарина Ю.А.»

Профессионально-педагогический колледж

УТВЕРЖДАЮ
Директор ППК СГТУ имени Гагарина Ю.А.
_____ Л.И. Рожкова
10 июня 2021 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

специальность

10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Рабочая программа рассмотрена
на заседании методической комиссии
рекламы, информационной безопасности и
компьютерных сетей
протокол № 11 от «09» июня 2021 г.
Председатель МК _____ М.А. Ястребова

Саратов 2021

Рабочая программа профессионального модуля разработана в соответствии с Федеральным государственным образовательным стандартом (далее – ФГОС) по специальности среднего профессионального образования (далее СПО)10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённого приказом Министерства образования и науки РФ от 9 декабря 2016 года № 1553.

Разработчик: Богданов В.Ю. – преподаватель ППК СГТУ имени Гагарина Ю.А

Рецензенты:
Внутренний: Ястребова М.А. – преподаватель высшей квалификационной категории ППК СГТУ имени Гагарина Ю.А.
Внешний:Жордочкин А.В. - генеральный директор ООО «Ирис»

СОДЕРЖАНИЕ

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

1.1. Область применения рабочей программы

Рабочая программа профессионального модуля является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основного вида профессиональной деятельности Защита информации техническими средствами.

1.2. Место профессионального модуля в структуре ППССЗ:

Профессиональный модуль входит в профессиональный цикл ППССЗ.

1.3. Цели и требования к результатам освоения профессионального модуля

Изучение профессионального модуля направлено на освоение основного вида деятельности 3.4.3Защита информации техническими средствами и соответствующих ему общих компетенций и профессиональных компетенций.

1.3.1. Перечень общих компетенций

Код	Наименование результата обучения
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

1.3.2. Перечень профессиональных компетенций

Код	Наименование результата обучения
ПК 3.1	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5	Организовывать отдельные работы по физической защите объектов информатизации.

1.3.3. 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 средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять инженерно-технические средства физической защиты объектов информатизации.
знать	– физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации; – основные способы физической защиты объектов информатизации; – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

	− номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.

1.4. Количество часов на освоение программы профессионального модуля:

Максимальной учебной нагрузки обучающегося – 600 часов, в том числе:
обязательной аудиторной учебной нагрузки обучающегося – 324 часа;
самостоятельной работы обучающегося – 32 часа;
консультации – 4 часа;
учебной практики – 72 часа;
производственной практики – 144 часа;
экзамен квалификационный -12 часов.

2. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

2.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	**Наименование разделов профессионального модуля**	**Суммарный объем нагрузки, час.** *(максимальная учебная нагрузка и практики)*	**Объем времени, отведенный на освоение МДК**							**Консультации**	**Промежуточная аттестация**	**Практика**		**Экзамен квалификационный**
			Обязательная аудиторная учебная нагрузка обучающегося					**Самостоятельная работа обучающегося**						
			Всего часов	**в т.ч. лаборат. занятия** *(если предусмотрено)* часов	**в т.ч. практич. занятия** *(если предусмотрено)* часов	**в т.ч., курсовая работа (проект)** *(если предусмотрено)* часов	**в т.ч. семинар. занятия** *(если предусмотрено)* часов	**Всего** часов	**в т.ч., курсовая работа (проект)** *(если предусмотрено)* часов			**Учебная** *(если предусмотрено)* часов	**Производственная (по профилю специальности)** часов	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**		**12**	**13**	
ОК 01-11, ПК 3.1-3.5	МДК 03.01 Техническая защита информации	**174**	**148**	10	36	-	-	**12**	-	**2**	-			
	МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации	**198**	**176**	10	46	30	-	**20**	-	**2**	-			
	УП 03.01 Учебная практика	**72**										**72**		
	ПП 03.01 Производственная практика	**144**											**144**	
	Экзамен квалификационный	**12**												**12**
	Всего:	**600**	**324**	**20**	**82**	**30**	**-**	**32**	**-**	**4**	**12**	**72**	**144**	**12**

2.2. Тематический план и содержание профессионального модуля

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа обучающегося, курсовая работа (проект) *(если предусмотрены)* , иные виды учебной работы в соответствии с учебным планом	Объем часов	Уровень освоения	Коды компетенций, формированию которых способствует элемент программ
1	2	3	4	5
5 семестр				
Раздел 1 модуля. Применение технической защиты информации		**174**		
МДК.03.01 Техническая защита информации		**174**		
Раздел 1. Концепция инженерно-технической защиты информации		**6**		ОК 01-10, ПК 3.1-3.4
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание учебного материала**	**2**		
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	2	1	
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание учебного материала**	**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.	4	1	
Раздел 2. Теоретические основы инженерно-технической защиты информации		**28**		
Тема 2.1. Информация как предмет защиты	**Содержание учебного материала**	**12**		
	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.	4	1	
	Практическое занятие №1 Содержательный анализ основных руководящих, нормативных и методических документов по защите информации	2	2	

	Практическое занятие №2 Содержательный анализ основных руководящих, нормативных и методических документов по противодействию технической разведке.	2	2	
	Самостоятельная работа обучающихся№1Угрозы безопасности информации и меры по их предотвращению	4	3	
Тема 2.2. Технические каналы утечки информации	**Содержание учебного материала**	**8**		
	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.	4	1	
	Практическое занятие №3 Исследование технических каналов утечки информации	4	2	
Тема 2.3. Методы и средства технической разведки	**Содержание учебного материала**	**8**		
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	4	1	
	Практическое занятие №4 Исследование средств технической разведки	4	2	
Раздел 3. Физические основы технической защиты информации		**24**		ОК 01-10, ПК 3.1-3.4
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание учебного материала**	**12**		
	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	8	1	
	Практическое занятие №5 Измерение параметров физических полей	4	2	
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание учебного материала**	**12**		
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	4	1	
	Лабораторное занятие №1 Исследование физических процессов при	6	2	

	подавлении опасных сигналов			
	Самостоятельная работа обучающихся№2 Методы добывания информации	2	3	
Раздел 4. Системы защиты от утечки информации		**74**		ОК 01-10, ПК 3.1-3.4
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание учебного материала**	**8**		
	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.	4	1	
	Практическое занятие №6 Защита от утечки по акустическому каналу	4	2	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание учебного материала**	**8**		
	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.	4	1	
	Практическое занятие №7 Системы защиты от утечки информации по проводному каналу	4	2	
Промежуточная аттестация – другие формы контроля (средний балл по текущим оценкам успеваемости)				
6 семестр				
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание учебного материала**	**10**		
	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.	6	1	
	Практическое занятие №8 Защита от утечки по виброакустическому каналу	4	2	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание учебного материала**	**14**		
	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	6	1	

	утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.			
	Лабораторное занятие №2 Определение каналов утечки ПЭМИН	4	2	
	Практическое занятие №9 Защита от утечки по цепям электропитания и заземления	4	2	
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание учебного материала**	**16**		
	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.	6	1	
	Практическое занятие №10 Системы защиты от утечки информации по телефонному каналу	4	2	
	Самостоятельная работа обучающихся №3 Утечка информации по сотовым цепям связи	6	3	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание учебного материала**	**8**		
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	4	1	
	Практическое занятие №11 Системы защиты от утечки информации по электросетевому каналу	4	2	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание учебного материала**	**10**		
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	6	1	
	Практическое занятие №12 Системы защиты от утечки информации по оптическому каналу	4	2	
Раздел 5. Применение и эксплуатация технических средств защиты информации				ОК 01-10, ПК 3.1-3.4
Тема 5.1. Применение технических средств защиты информации	**Содержание учебного материала**	**12**		
	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,	8	1	

	создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.			
	Практическое занятие №13 Применение технических средств защиты информации	4	2	
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание учебного материала**	**16**		
	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.	8	1	
	Практическое занятие №14 Система защиты информации SecretNet 4.0	2	2	
	Практическое занятие №15 Электронный замок «Соболь»	2		
	Практическое занятие №16 Программно-аппаратный комплекс «Аккорд-1.95»	2		
	Практическое занятие №17 Система защиты информации «SecretDisk»	2		
Консультация		2		
Промежуточная аттестация – экзамен		12		
6 семестр				
Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации		**198**		
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**198**		
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты				ОК 01-11, ПК 3.5
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание учебного материала**	**6**		
	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.	6	1	
	Практическое занятие №1 Характеристика объекта защиты	2	2	

Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание учебного материала**	**8**		
	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.	8	1	
	Практическое занятие №2 Анализ нормативно-правовой базы физической защиты. Формирование требований к физической защите объекта.	4	2	
	Самостоятельная работа обучающихся №1 Выполнение конспекта: Основные операции проведения технического обслуживания инженерно-технических средств физической защиты.	3	3	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты				
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание учебного материала**	**6**		ОК 01-11, ПК 3.5
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	6	1	
	Лабораторное занятие № 1 Монтаж датчиков пожарной и охранной сигнализации	6	2	
Тема 2.2. Система контроля и управления доступом	**Содержание учебного материала**	**8**		
	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.	8	1	
	Практическое занятие №3 Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	6	2	
	Практическое занятие №4 Рассмотрение принципов устройства,	6	2	

	работы и применения средств контроля доступа			
Тема 2.3. Система телевизионного наблюдения	**Содержание учебного материала**	**6**		
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	6	1	
	Практическое занятие №5 Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	6	2	
	Самостоятельная работа обучающихся № 2 Выполнение конспекта: IP-видеокамеры.	3	3	
Промежуточная аттестация – другие формы контроля (средний балл по текущим оценкам успеваемости)				
7 семестр				
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание учебного материала**			
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	10	1	
	Практическое занятие №6 Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	6	2	
	Самостоятельная работа обучающихся № 3 Выполнение конспекта: Система сбора и обработки информации ОРИОН	3	3	
Тема 2.5 Система воздействия	**Содержание учебного материала**			
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	10	1	
	Практическое занятие №7 Рассмотрение принципов устройства, работы и применения системы воздействия	4	2	
	Практическое занятие №8 Выбор и обоснование средств подсистемы задержки	4	2	
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты				
Тема 3.1 Применение инженерно-технических средств физической защиты	**Содержание учебного материала**			
	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	12	1	

	автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.			
	Лабораторное занятие № 2 Разработка структурной схемы и спецификации оборудования	4	2	
	Самостоятельная работа обучающихся № 4 Моделирование кабинета руководителя	5	3	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание учебного материала**			
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.	12	1	
	Практическое занятие №9 Порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта периметровых технических средств обнаружения	4	2	
	Практическое занятие №10 Порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы контроля и управления доступом	4	2	
	Практическое занятие №11 Порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы видеонаблюдения	4	2	
	Практическое занятие №12 Порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы пожарной сигнализации	4	2	
	Практическое занятие №13 Порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы охранной сигнализации	4	2	
	Самостоятельная работа обучающихся № 5 Выполнение конспекта: Размещение периметровых средств обнаружения на местности.	3	3	
	Самостоятельная работа обучающихся № 6 Выполнение конспекта: Порядок допуска субъектов на охраняемые объекты.	3	3	
Курсовое проектирование		30		
Примерная тематика курсовых проектов:				

Обеспечение физической защиты спортивно-развлекательного центра Обеспечение физической защиты учебного заведения Обеспечение физической защиты районного отделения полиции Обеспечение физической защиты научной библиотеки Обеспечение физической защиты супермаркета Обеспечение физической защиты рекламного агентства Обеспечение физической защиты наземной парковки Обеспечение физической защиты торгового центра Обеспечение физической защиты коттеджа Обеспечение физической защиты офиса фармацевтической фирмы Обеспечение физической защиты подземной парковки Обеспечение физической защиты птицефабрики Обеспечение физической защиты поликлиники Обеспечение физической защиты детского сада Обеспечение физической защиты склада Обеспечение физической защиты редакции научного издания Обеспечение физической защиты ювелирного магазина Обеспечение физической защиты банковского хранилища Обеспечение физической защиты районного суда Обеспечение физической защиты серверной Обеспечение физической защиты музея изобразительных искусств			
Консультация	2		
Промежуточная аттестация - дифференцированный зачет	2		
Учебная практика УП.03.01 **Примерные виды работ:** Выявление технических каналов утечки информации Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации Проведение измерений параметров побочных электромагнитных излучений и наводок Рассмотрение принципов работы системы инженерно-технической защиты и ее проектирование	**72**		
Производственная практика ПП.03.01 **Примерные виды работ:** Выявление технических каналов утечки информации	**144**		

Применение технических средств защиты информации Участие в обслуживании и эксплуатации технических средств защиты информации, в том числе средств защиты информации от несанкционированного съёма и утечки по техническим каналам Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок (ПЭМИН) Оценка защищенности информации от утечки по техническим каналам Участие в обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения Организация отдельных работ по физической защите объектов информатизации Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами			
Всего:	**600**		
Промежуточная аттестация (всего):			
Промежуточная аттестация по МДК.03.01-экзамен			
Промежуточная аттестация по МДК.03.02- дифференцированный зачет			
Промежуточная аттестация по ПМ - экзамен квалификационный			

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению профессионального модуля

Реализация программы профессионального модуля требует наличия лабораториитехнических средств защиты информациидля проведения занятий лекционного типа, лабораторных занятий, практических занятий, в том числе групповых, индивидуальных, письменных, устных консультаций, текущего контроля и промежуточной аттестации.

Оборудование:

- рабочее место преподавателя;
- специализированная мебель (столы, стулья по количеству обучающихся);
- доска ученическая.

Технические средства обучения:

- компьютер (ноутбук);
- мультимедийный проектор, экран.

Учебно-наглядные пособия: плакаты, учебно-наглядные пособия, обеспечивающие тематические иллюстрации по рабочей программе дисциплины, в том числе, видео-аудио материалы, компьютерные презентации.

Компьютер имеет доступ к электронно-библиотечным системам, выход в глобальную сеть Интернет, оснащен лицензионным программным обеспечением.

3.2. Учебно-методическое и информационное обеспечение реализации профессионального модуля

Нормативно-правовые акты

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». - Режим доступа: http://www.consultant.ru/

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». - Режим доступа: http://www.consultant.ru/

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». - Режим доступа: http://www.consultant.ru/

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». - Режим доступа: http://www.consultant.ru/

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях». - Режим доступа: http://www.consultant.ru/

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю». - Режим доступа: http://www.consultant.ru/

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». - Режим доступа: http://www.consultant.ru/

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». - Режим доступа: http://www.consultant.ru/

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608. - Режим доступа: http://www.consultant.ru/

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. - Режим доступа: http://www.consultant.ru/

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. - Режим доступа: http://www.consultant.ru/

12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. - Режим доступа: http://www.consultant.ru/

13. Приказ ФСТЭК России от 17.07.2017 N 134 (ред. от 17.12.2019) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации" (Зарегистрировано в Минюсте России 09.08.2017 N 47722) - Режим доступа: http://www.consultant.ru/

14. Приказ ФСТЭК России от 12.07.2012 N 84 (ред. от 20.05.2015) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации" (Зарегистрировано в Минюсте России 20.08.2012 N 25220) - Режим доступа: http://www.consultant.ru/

15. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». - Режим доступа: http://www.consultant.ru/

16. 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. – Режим доступа: http://docs.cntd.ru/

17. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности – Режим доступа: http://docs.cntd.ru/

18. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер – Режим доступа: http://docs.cntd.ru/

19. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. – Режим доступа: http://docs.cntd.ru/

20. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Практические правила управления информационной безопасностью. – Режим доступа: http://docs.cntd.ru/

21. 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. – Режим доступа: http://docs.cntd.ru/

22. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – Режим доступа: http://docs.cntd.ru/

23. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – Режим доступа: http://docs.cntd.ru/

24. ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи". – Режим доступа: http://docs.cntd.ru/

25. ГОСТ 34.311-95 Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования (аутентичен ГОСТ Р 34.11-94). – Режим доступа: http://docs.cntd.ru/

26. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

27. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013. – Режим доступа: http://docs.cntd.ru/

28. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

29. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000. – Режим доступа: http://docs.cntd.ru/

30. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

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

Номенклатура показателей качества. Ростехрегулирование, 2005. – Режим доступа: http://docs.cntd.ru/

32. 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. – Режим доступа: http://docs.cntd.ru/

33. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

34. 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. – Режим доступа: http://docs.cntd.ru/

35. 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. – Режим доступа: http://docs.cntd.ru/

36. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

37. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

Основные учебные издания

38. Бубнов А.А. Техническая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / А.А. Бубнов, В.Н. Пржегорлинский, К.Ю. Фомина; под ред. В.Н. Пржегорлинского.- 1-е изд. - М. : Издательский центр «Академия», 2019. – 272 с. В пер. ISBN 978-5-4468-8718-7

39. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

40. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

41. Ильин М.Е. Криптографическая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / М.Е. Ильин, Т.И. Калинкина, В.Н. Пржегорлинский; под ред. В.Н. Пржегорлинского. - 1-е изд. - М. : Издательский центр «Академия», 2020. – 288 с. В пер. ISBN 978-5-4468-8717-0.

42. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. - Москва : ИД "ФОРУМ" : ИНФРА-М, 2021. - 416 с. - (Среднее профессиональное образование). ISBN 978-5-8199-0754-2

Дополнительные учебные издания

43. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282. http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm

44. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. – Режим доступа: http://www.consultant.ru/

45. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489. – Режим доступа: http://www.consultant.ru/

46. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638. - Режим доступа: https://fstec.ru/

47. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008. – Режим доступа: http://docs.cntd.ru/

48. 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. – Режим доступа: http://docs.cntd.ru/

49. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. - Режим доступа: http://www.consultant.ru/

50. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. - Режим доступа: http://www.consultant.ru/

51. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах

персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г. – Режим доступа: http://www.consultant.ru/

52. 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. - Режим доступа: http://www.consultant.ru/

Интернет-ресурсы

53. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) - Режим доступа: https://fstec.ru/

54. Информационно-справочная система по документам в области технической защиты информации - Режим доступа: https://fstec.ru/

55. Справочно-правовая система «Консультант Плюс» - Режим доступа: http://www.consultant.ru/

56. Справочно-правовая система «Гарант» - Режим доступа: http://www.garant.ru/

57. Федеральный портал. Российское образование. - Режим доступа:http://www.edu.ru

Сайт Научной электронной библиотеки - Режим доступа: https://www.elibrary.ru/

Методические указания для обучающихся по освоению профессионального модуля

58. Методические указания для обучающихся по выполнению практических работ.

59. Методические указания для обучающихся по выполнению заданий самостоятельной работы.

60. Методические указания для обучающихся по выполнению лабораторных работ.

61. Методические рекомендации по подготовке и защите курсовых работ (проектов).

62. Методические указания по выполнению заданий практики.

3.3. Общие требования к организации образовательного процесса

При реализации компетентностного подхода программа профессионального модуля предусматривает использование в образовательном процессе активных и интерактивных форм проведения занятий (применение электронных образовательных ресурсов, деловых игр, разбора конкретных ситуаций, психологических тренингов, групповых дискуссий) в сочетании с внеаудиторной работой для формирования и развития общих и профессиональных компетенций обучающихся.

Реализация практических занятий осуществляется непосредственно в ППК СГТУ имени Гагарина Ю.А.

Образовательная деятельность в форме практической подготовки организована при реализации МДК 03.01 Техническая защита информации, МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации, учебной практики, производственной практики, предусмотренных учебным планом следующим образом:

– при реализации МДК 03.01 Техническая защита информации, МДК 03.02 Инженерно-технические средства физической защиты объектов информатизациипрактическая подготовка организуется путем проведения практических занятий, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью;

– при проведении практики практическая подготовка организуется путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью.

Учебная практика проводится на базе ППК СГТУ имени Гагарина Ю.А.

Производственная практика проводится в организациях, направление деятельности которых соответствует профилю подготовки обучающихся. Производственная практика проводится концентрировано по завершении освоения МДК 03.01 Техническая защита информации, МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации

Формы проведения консультаций для обучающихся: групповые, индивидуальные, письменные, устные.

Программа профессионального модуля реализуется в 5-7 семестрах 3-4 курса обучения. Освоению профессионального модуля должно предшествовать изучение учебных дисциплин: ЕН.01 Математика, ЕН.02 Информатика, ОП.01 Основыинформационной безопасности, ОП.02 Организационно-правовое обеспечение информационной безопасности, ОП.03 Основы алгоритмизации и программирования, ОП.04 Электроника и схемотехника, ОП.07Технические средства информатизации, ОП.08 Инженерная графика, ОП.09 Технологии программирования.

3.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по междисциплинарным курсам, учебной практике, производственной практике:

- наличие высшего профессионального образования, соответствующего профилю преподаваемого модуля;
- наличие опыта деятельности в организациях соответствующей профессиональной сферы;
- получение дополнительного профессионального образования по программам повышения квалификации, в том числе в форме стажировки в профильных организациях не реже 1 раза в 3 года.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Критерии оценки, формы и методы контроля и оценки результатов обучения

Код, наименование профессиональных компетенций	Критерии оценки	Формы и методы контроля и оценки результатов обучения
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	– применение, техническое обслуживание, диагностика, устранение отказов, восстановление работоспособности, установка, монтаж и настройка инженерно-технических средств физической защиты и технических средств защиты информации;	Текущий контроль успеваемости: - опрос устный (фронтальный); - выполнение практической работы (индивидуальная форма работы); - защита рефератов - собеседование по результатам выполненной работы; - наблюдение за процессом выполнения заданий; - демонстрация выполнения видов работ практики; - выполнение письменной работы "Отчет по практике". Межсессионная аттестация – тестирование. Промежуточная аттестация по МДК.03.01 в форме экзамена, МДК.03.02в форме дифференцированного зачета. Промежуточная аттестация по УП.03.01 в форме дифференцированного зачета. Промежуточная аттестация по ПП.03.01в форме
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	– применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;	
ПК 3.3 Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.	– проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	

ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	– проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;	дифференцированного зачета. Промежуточная аттестация по ПМ.03 в форме экзамена квалификационного.
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации.	– выявление технических каналов утечки информации; – применение средств охранной сигнализации, охранного телевидения и систем контроля и управления доступом;	

Код, наименование общих компетенций	**Критерии оценки**	**Формы и методы контроля и оценки результатов обучения**
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- распознавание задач в профессиональном и/или социальном контексте; - распознавание проблем в профессиональном и/или социальном контексте; - анализ задачи и/или проблемы; - выделение составных частей задачи и/или проблемы; - определение этапов решения задачи; - выявление информации, необходимой для решения задачи и/или проблемы; - осуществление эффективного поиска информации, необходимой для решения задачи и/или проблемы; - разработка плана действия решения задачи и/или проблемы; - определение необходимых ресурсов для решения задачи и/или проблемы; - владение актуальными методами работы в профессиональной и смежных сферах; - реализация составленного плана; - оценка результата и	Текущий контроль успеваемости: - опрос устный (фронтальный); - выполнение практической работы (индивидуальная форма работы); - защита рефератов - собеседование по результатам выполненной работы; - наблюдение за процессом выполнения заданий; - демонстрация выполнения видов работ практики; - выполнение письменной работы "Отчет по практике". Межсессионная аттестация – тестирование. Промежуточная аттестация по МДК.03.01 в форме экзамена, МДК.03.02в форме дифференцированного зачета. Промежуточная аттестация по УП.03.01 в форме дифференцированного зачета. Промежуточная

	последствий своих действий (самостоятельно или с помощью наставника).	аттестация по ПП.03.01в форме дифференцированного зачета. Промежуточная аттестация по ПМ.03 в форме экзамена квалификационного.
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- определение задач поиска информации, необходимых источников информации; - планирование процесса поиска необходимой информации; - осуществление поиска информациинеобходимойдля выполнения задач профессиональной деятельности; - проведение анализа информации, необходимой для выполнения задач профессиональной деятельности; - осуществление интерпретации информации, необходимой для выполнения задач профессиональной деятельности; - структурирование получаемой информации; - выделение наиболее значимой в перечне информации; - оценка практической значимости результатов поиска; - оформление результатов поиска.	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- планирование собственного профессионального развития; - построение траектории собственного профессионального и личностного развития; - реализация собственного профессионального и личностного развития; - определение актуальности нормативно-правовой документации в профессиональной деятельности.	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с	- организация работы коллектива и команды; - эффективное взаимодействие с коллегами, руководством;	

коллегами, руководством, клиентами.	- эффективное взаимодействие с клиентами.	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- грамотное изложение своих мыслей на государственном языке с учетом особенностей социального и культурного контекста; - правильное оформление документов по профессиональной тематике на государственном языке.	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	- понимание значимость своей специальности; - описание значимости своей специальности; - презентация структуры профессиональной деятельности по специальности; - проявление гражданско-патриотической позиции; - демонстрация осознанного поведения на основе традиционных общечеловеческих ценностей; - применение стандартов антикоррупционного поведения.	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- содействие сохранению окружающей среды; - содействие ресурсосбережению; - осуществление эффективных действий в чрезвычайных ситуациях; - соблюдение норм экологической безопасности; - определение направлений ресурсосбережения в рамках профессиональной деятельности по специальности	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической	- использование физкультурно-оздоровительной деятельности для укрепления здоровья, достижения жизненных и профессиональных целей; - применение рациональных приемов двигательных функций в профессиональной деятельности;	

подготовленности.	- использование средств профилактики перенапряжения характерными для данной специальности	
ОК 09.Использовать информационные технологии в профессиональной деятельности.	- применение средств информационных технологий для решения профессиональных задач; - использование современного программного обеспечения	
ОК 10.Пользоваться профессиональной документацией на государственном и иностранном языках.	- понимание общего смысла четко произнесенных высказываний на известные темы (профессиональные и бытовые); - понимание текста на базовые профессиональные темы; - участие в диалогах на знакомые общие и профессиональные темы; - построение простых высказываний о себе и о своей профессиональной деятельности; - краткое обоснование и объяснение своих действий (текущих и планируемых); - написание простых связных сообщений на знакомые или интересующие профессиональные темы	
ОК.11 Использовать знания финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере	- выявление достоинств и недостатков коммерческой идеи; - презентация идеи открытия собственного дела в профессиональной деятельности; - оформление бизнес-плана; - расчет размера выплат по процентным ставкам кредитования; - определение инвестиционной привлекательности коммерческих идей в рамках профессиональной деятельности; - презентация бизнес - идеи; - определение источников финансирования	

4.2. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по профессиональному модулю

Показатели и критерии оценивания компетенций

Показатели и критерии оценивания компетенций, описание шкал оценивания содержатся в приложении 1.

Контрольные и тестовые задания

Контрольные задания содержатся в приложении 1.

Методические материалы

Методические материалы, определяющие процедуры оценивания знаний, умений, характеризующих формирование компетенций, содержатся в приложении 1.

Приложение 1

Контрольно-оценочные средства

для проведения промежуточной аттестации по профессиональному модулю
ПМ.03 Защита информации техническими средствами

1.1. Форма промежуточной аттестации: Экзамен квалификационный (8 семестр).

1.2. Система оценивания результатов выполнения заданий

Оценивание результатов выполнения заданий промежуточной аттестации осуществляется на основе следующих принципов:

достоверности оценки – оценивается уровень сформированности знаний, умений, практического опыта, общих и профессиональных компетенций, продемонстрированных обучающимися в ходе выполнения задания;

адекватности оценки – оценка выполнения заданий должна проводиться в отношении тех компетенций, которые необходимы для эффективного выполнения задания;

надежности оценки – система оценивания выполнения заданий должна обладать высокой степенью устойчивости при неоднократных оценках уровня сформированности знаний, умений, практического опыта, общих и профессиональных компетенций обучающихся;

комплексности оценки – система оценивания выполнения заданий должна позволять интегративно оценивать общие и профессиональные компетенции обучающихся;

объективности оценки – оценка выполнения конкурсных заданий должна быть независимой от особенностей профессиональной ориентации или предпочтений преподавателей, осуществляющих контроль или аттестацию.

При выполнении процедур оценки заданий используются следующие основные методы:

- метод экспертной оценки;
- метод расчета первичных баллов;
- метод расчета сводных баллов;
- метод агрегирования.

Результаты выполнения заданий оцениваются в соответствии с разработанными критериями оценки.

Используется сто бальная шкала оценки для оценивания результатов обучения.

Перевод сто бальной шкалы учета результатов в пяти бальную оценочную шкалу:

Оценка	**Количество баллов, набранных за выполнение теоретического и практического задания**
Оценка 5 «отлично»	90-100
Оценка 4 «хорошо»	76-89
Оценка 3 «удовлетворительно»	50-75
Оценка 2 «неудовлетворительно»	≤ 49

1.3. Контрольно-оценочные средства

1.3.1Задание:

1. Тестирование
2. Практическое задание

Примерное задание «Тестирование»

1) Основной целью защиты информации является

а) обеспечение заданного уровня безопасности
б) обеспечение невозможности кражи
в) обеспечение сохранности вида

2) В защите информации выделены следующие направления: организационно-правовое, программно-аппаратное, _____ (укажите название).

3) Чем определяется уровень безопасности информации?
а) стоимостью затрат на создание системы безопасности
б) величиной потенциального ущерба от реализации угроз
в) вероятностью реализации угроз

4) Почему защита информации должна производиться скрытно?
а) чтобы обеспечить большую неопределенность данных у злоумышленника
б) чтобы исключить возможные угрозы
в) чтобы уменьшить затраты на защиту

5) Что понимают под каналом утечки информации ?
а) некий физический путь несанкционированного распространения носителей информации от ее источника к несанкционированному потребителю
б) несанкционированное распространение носителя с защищаемой информацией за пределы контролируемой зоны
в) несанкционированное распространение носителя с защищаемой информацией к потребителю

6) Чем отличается технический канал утечки информации от канала связи?
а) у канала связи носитель информации санкционированный, у канала утечки – несанкционированный
б) у канала связи получатель информации санкционированный , у канала утечки – несанкционированный
в) у канала связи источник информации санкционированный , у канала утечки – несанкционированный

7) Приведите в соответствие каналы утечки информации и носители информации:
А) оптический, Б) акустический, В) радиоэлектронный, Г) вещественный
1) частицы вещества, 2) фотоны, 3) акустические волны, 4) электромагнитное поле
Ответ:

А	Б	В	Г

8) Пироэлектрический преобразователь используется в извещателях:
а) акустических
б) оптико-электронных
в) радиоволновых

9) Емкостные извещатели могут быть использованы для
а) обнаружения пожара
б) защиты металлических шкафов
в) контроля целостности остеклённых конструкций

10) Какой канал утечки информации основан на использовании электромагнитной энергии видимого и инфракрасного диапазона?

а) визуально-оптический канал
б) электромагнитный канал
в) виброакустический канал
г) материально-вещественный канал

11) Методы инженерно-технической защиты информации должны обеспечивать следующие направления защиты: скрытие информации, нейтрализацию источников опасных сигналов, _____защиту (укажите название).

12) Что не включает в себя физическая защита информации?
а) техническую охрану объектов
б) инженерную защиту
в) маскировку

13) В чем заключается метод энергетического скрытия информации?
а) увеличение отношения сигнал/помеха
б) уменьшение отношения сигнал/помеха
в) созданием искусственных помех

14) В интересах защиты применяют три вида освещения: дежурное, охранное и _____ (укажите название).

15) Закладное устройство представляет собой
а) ретранслятор
б) передатчик
в) приемник

16) Чем принципиально отличаются проводные и излучающие закладные устройства?
а) частотным диапазоном работы
б) видом носителя информации
в) мощностью сигнала

17) Какие функции не характерны для подразделения инженерно-технической защиты информации?
а) выявление потенциальных угроз
б) разработка мер по предотвращению угроз
в) охрана объектов организации
г)контроль уровней опасных сигналов

18) Приведите в соответствие нормативно-правовые документы по защите информации с уровнем действия
А) Нормативно-методические документы Федеральной службы по техническому и экспортному контролю РФ
Б) Инструкция по защите информации на предприятии
В) Законы Российской Федерации (РФ)
1) Уровень государства
2) Уровень организации
3) Уровень ведомства
Ответ

А	Б	В

19) Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется
а) системой угроз;
б) системой защиты;
в) системой безопасности;

20) Как оценивается угроза утечки информации:
а) величиной ущерба от её реализации
б) уровнем секретности информации
в) значением для собственника информации

21) Выделите угрозы утечки информации (укажите все правильные ответы)
а) утеря документов;
б) действия помех;
в) побочные излучения и наводки

22) Последовательность проектирования (модернизации) системы защиты информации включает три основных этапа:
а) выбор мер защиты;
б) моделирование объектов защиты;
в) моделирование угроз информации.
Установите правильную последовательность действий
Ответ:

1	2	3

23) Виды моделей, применяемые при проектировании системы защиты информации
а) вербальные, физические и математические
б) структурные, пространственные, линейные
в) функциональные, нелинейные, детальные

24) Алгоритм проектирования (модернизации) системы защиты информации является итерационным процессом?
а) нет;
б) да;
в) частично

25) Какой закон лежит в основе принципа действия электродинамического микрофона?
а) закон Ома;
б) закон электромагнитной индукции;
в) закон Фарадея

26) К основным группам технических средств ведения разведки не относятся
а) радиомикрофоны
б) фотоаппараты
в) электронные "уши"
г) дистанционное прослушивание разговоров

27) Сигналы по форме бывают
А – аналоговые и дискретные

В – импульсные и цифровые
С – электрические и электромагнитные

28) Чувствительность оптического средства наблюдения
а) оценивается минимальным уровнем световой энергии, при котором обеспечивается требуемое качество изображения объекта наблюдения
б) характеризуется минимальными линейными или угловыми размерами между двумя соседними точками изображения, которые наблюдаются как отдельные
в) определяет интервал силы света на входе оптического приемника, при котором обеспечивается заданное качество изображения

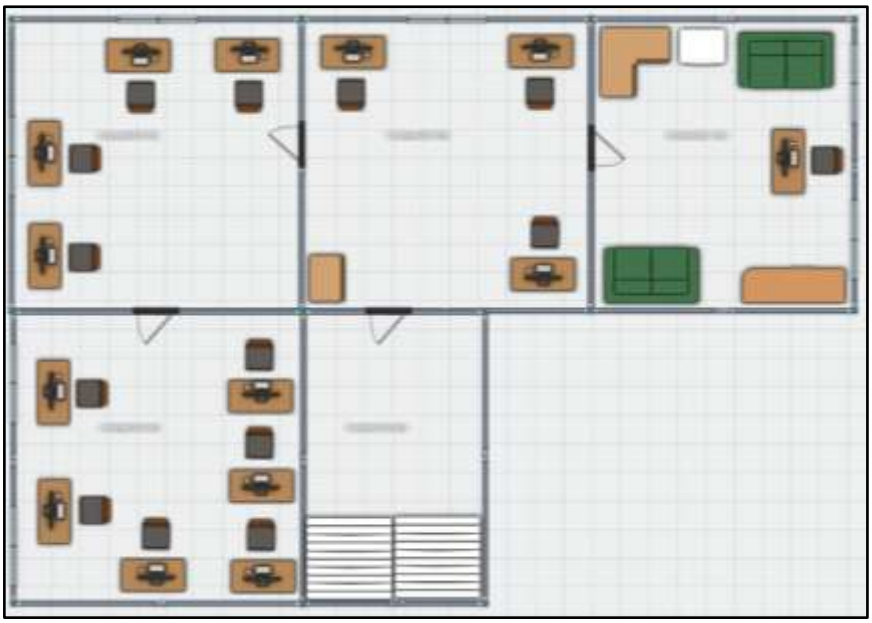
29) Что входит в организационную составляющую ИТЗИ?
а) подбор и расстановка персонала
б) регламентация деятельности сотрудников и технических средств защиты
в) выявление технических каналов утечки информации

30) Электропитание извещателя ИП212-45 осуществляется:
а) от источника постоянного тока напряжением от 7,5 до 30 В.
б) по шлейфу сигнализации постоянным напряжением от 12 до 24 В.
в) от источника постоянного тока напряжением от12 до 24 В.
г) по шлейфу сигнализации постоянным напряжением от 7,5 до 30 В.

Примерное практическое задание:

Ситуация 1

План помещений 1 этажа организации и расположенное в помещениях оборудование представлены на рисунке.



Задание.
1. Провести анализ признаков утечки информации (по оптическому каналу, по акустическому каналу, по радиоэлектронному каналу, по вещественному каналу) и определить возможные каналы утечки информации.

2. Составить перечень оборудования, необходимого для обеспечения предотвращения утечки информации.
3. Разработать структурную схему системы инженерно-технической защиты информации.
4. Описать алгоритм работы системы инженерно-технической защиты информации.
5. Описать работу оптико-электронного инфракрасного извещателя.

1.3.2. Критерии оценки

Критерии оценки задания «Тестирование»
Максимальное количество баллов за выполнение задания «тестирование» – **30 баллов.**

Оценка за задание «Тестирование» определяется простым суммированием баллов за правильные ответы на вопросы. Один верный ответ равен 1 баллу.

Ответ считается правильным, если:

- при ответе на вопрос закрытой формы с выбором ответа выбран правильный ответ;
- при ответе на вопрос открытой формы дан правильный ответ;
-при ответе на вопрос на установление правильной последовательности установлена правильная последовательность;
-при ответе на вопрос на установление соответствия, если сопоставление произведено верно для всех пар.

Критерии оценки практического задания

№	Критерии оценки	Баллы за критерии оценки
Задание 1		
	Провести анализ признаков утечки информации (по оптическому каналу, по акустическому каналу, по радиоэлектронному каналу, по вещественному каналу) и определить возможные каналы утечки информации.	**Максимальный балл – 19 баллов**
	Критерии оценки:	
1	Проведен анализ признаков утечки информации по оптическому каналу	2
2	Проведен анализ признаков утечки информации по акустическому каналу	2
3	Проведен анализ признаков утечки информации по радиоэлектронному каналу	2
4	Проведен анализ признаков утечки информации по вещественному каналу	2
5	Верно указаны признаки утечки информации по оптическому каналу	2
6	Верно указаны признаки утечки информации по акустическому каналу	2
7	Верно указаны признаки утечки информации по радиоэлектронному каналу	2
8	Верно указаны признаки утечки информации по вещественному каналу	2
9	Верно определены каналы утечки информации	3
Задание 2		

	Составить перечень оборудования, необходимого для обеспечения предотвращения утечки информации	**Максимальный балл – 8 баллов**
	Критерии оценки:	
1	Верно составлен перечень оборудования, необходимого для обеспечения предотвращения утечки информации	5
2	Приведено обоснование выбора оборудования	3
	Задание 3	
	Разработать структурную схему системы инженерно-технической защиты информации	**Максимальный балл – 15 баллов**
	Критерии оценки:	
1	Указаны средства охранной сигнализации	3
2	Указаны средства охранного телевидения	3
3	Указаны средства систем контроля и управления доступом	3
4	Меры защиты обоснованы исходя из рода деятельности предприятия	2
5	Разработана общая схема системы инженерно-технической защиты информации	4
	Задание 4	
	Описать алгоритм работы системы инженерно-технической защиты информации	**Максимальный балл – 17 баллов**
	Критерии оценки:	
1	Описан принцип работы средств охранной сигнализации	4
2	Описан принцип работы средств охранного телевидения	4
3	Описан принцип работы средств систем контроля и управления доступом	4
4	Описан общий алгоритм работы системы инженерно-технической защиты информации	5
	Задание 5	
	Описать работу подсистемы/датчика/извещателя	**Максимальный балл – 11 баллов**
	Критерии оценки:	
1	Верно указано функциональное назначение подсистемы/датчика/извещателя	4
2	Верно указано место установки подсистемы/датчика/извещателя	2
3	Верно описан принцип работы подсистемы/датчика/извещателя	5
	ИТОГО	**70**

1.4. Материально-техническое обеспечение для проведения промежуточной аттестации

Аттестация проводится в лаборатории технических средств защиты информации

1.5. Учебно-методическое и информационное обеспечение для проведения промежуточной аттестации

Нормативно-правовые акты

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». - Режим доступа: http://www.consultant.ru/

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». - Режим доступа: http://www.consultant.ru/

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». - Режим доступа: http://www.consultant.ru/

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». - Режим доступа: http://www.consultant.ru/

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях». - Режим доступа: http://www.consultant.ru/

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю». - Режим доступа: http://www.consultant.ru/

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера». - Режим доступа: http://www.consultant.ru/

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». - Режим доступа: http://www.consultant.ru/

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608. - Режим доступа: http://www.consultant.ru/

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. - Режим доступа: http://www.consultant.ru/

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. - Режим доступа: http://www.consultant.ru/

12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. - Режим доступа: http://www.consultant.ru/

13. Приказ ФСТЭК России от 17.07.2017 N 134 (ред. от 17.12.2019) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации" (Зарегистрировано в Минюсте России 09.08.2017 N 47722) - Режим доступа: http://www.consultant.ru/

14. Приказ ФСТЭК России от 12.07.2012 N 84 (ред. от 20.05.2015) "Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации" (Зарегистрировано в Минюсте России 20.08.2012 N 25220) - Режим доступа: http://www.consultant.ru/

15. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации». - Режим доступа: http://www.consultant.ru/

16. 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. – Режим доступа: http://docs.cntd.ru/

17. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности – Режим доступа: http://docs.cntd.ru/

18. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер – Режим доступа: http://docs.cntd.ru/

19. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети. – Режим доступа: http://docs.cntd.ru/

20. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Практические правила управления информационной безопасностью. – Режим доступа: http://docs.cntd.ru/

21. 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. – Режим доступа: http://docs.cntd.ru/

22. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – Режим доступа: http://docs.cntd.ru/

23. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – Режим доступа: http://docs.cntd.ru/

24. ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи". – Режим доступа: http://docs.cntd.ru/

25. ГОСТ 34.311-95 Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования (аутентичен ГОСТ Р 34.11-94). – Режим доступа: http://docs.cntd.ru/

26. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

27. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013. – Режим доступа: http://docs.cntd.ru/

28. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

29. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000. – Режим доступа: http://docs.cntd.ru/

30. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

31. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005. – Режим доступа: http://docs.cntd.ru/

32. 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. – Режим доступа: http://docs.cntd.ru/

33. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных

воздействий. Общие требования. Росстандарт, 2014. – Режим доступа: http://docs.cntd.ru/

34. 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. – Режим доступа: http://docs.cntd.ru/

35. 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. – Режим доступа: http://docs.cntd.ru/

36. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

37. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006. – Режим доступа: http://docs.cntd.ru/

Основные учебные издания

38. Бубнов А.А. Техническая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / А.А. Бубнов, В.Н. Пржегорлинский, К.Ю. Фомина; под ред. В.Н. Пржегорлинского.- 1-е изд. - М. : Издательский центр «Академия», 2019. – 272 с. В пер. ISBN 978-5-4468-8718-7

39. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

40. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru

41. Ильин М.Е. Криптографическая защита информации в объектах информационной инфраструктуры : учебник для студ. учреждений сред. проф. образования / М.Е. Ильин, Т.И. Калинкина, В.Н. Пржегорлинский; под ред. В.Н. Пржегорлинского. - 1-е изд. - М. : Издательский центр «Академия», 2020. – 288 с. В пер. ISBN 978-5-4468-8717-0.

42. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. - Москва : ИД "ФОРУМ" : ИНФРА-М, 2021. - 416 с. - (Среднее профессиональное образование). ISBN 978-5-8199-0754-2

Дополнительные учебные издания

43. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282. http://www.rfcmd.ru/sphider/docs/InfoSec/RD_FSTEK_requirements.htm

44. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. – Режим доступа: http://www.consultant.ru/

45. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489. – Режим доступа: http://www.consultant.ru/

46. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638. - Режим доступа: https://fstec.ru/

47. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008. – Режим доступа: http://docs.cntd.ru/

48. 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. – Режим доступа: http://docs.cntd.ru/

49. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17. - Режим доступа: http://www.consultant.ru/

50. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г. - Режим доступа: http://www.consultant.ru/

51. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г. – Режим доступа: http://www.consultant.ru/

52. 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. - Режим доступа: http://www.consultant.ru/

Интернет-ресурсы

53. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) - Режим доступа: https://fstec.ru/

54. Информационно-справочная система по документам в области технической защиты информации - Режим доступа: https://fstec.ru/

55. Справочно-правовая система «Консультант Плюс» - Режим доступа: http://www.consultant.ru/

56. Справочно-правовая система «Гарант» - Режим доступа: http://www.garant.ru/

57. Федеральный портал. Российское образование. - Режим доступа:http://www.edu.ru

Сайт Научной электронной библиотеки - Режим доступа: https://www.elibrary.ru/

Методические указания для обучающихся по освоению профессионального модуля

58. Методические указания для обучающихся по выполнению практических работ.

59. Методические указания для обучающихся по выполнению заданий самостоятельной работы.

60. Методические указания для обучающихся по выполнению лабораторных работ.

61. Методические рекомендации по подготовке и защите курсовых работ (проектов).

62. Методические указания по выполнению заданий практики.