Воронежский колледж робототехники и компьютерных технологий

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01D72D329BBD7B20000000072C4B0002
Владелец: Лукина Виктория Борисовна
Действителен: с 09.04.2021 до 09.04.2022

УТВЕРЖДАЮ
Директор колледжа
_____ Лукина В.Б.
«_____» _____ 2019г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«ПМ.03. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ»

для специальности среднего профессионального образования **10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»**

Квалификация выпускника: **техник по защите информации**

Воронеж
2019

Рабочая программа составлена на основании требований:

— Федерального государственного образовательного стандарта среднего профессионального образования №1551, утвержденного приказом Министерства образования и науки Российской Федерации от 09 декабря 2016 г.;

— учебного плана Воронежского колледжа робототехники и компьютерных технологий по специальности 10.02.04 — "Обеспечение информационной безопасности телекоммуникационных систем", утвержденного Педагогическим советом от 16.12.2019 г. протокол №1

Индекс — 10.02.04 ИБ

Составитель: преподаватель _____С.С. Куликов

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ПМ.03. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ»

1.1. Цель и планируемые результаты освоения профессионального модуля

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

1.1.1. Перечень общих компетенций

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

1.1.2. Перечень общих компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государ-

	ственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации; проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты.
Уметь	применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации
Знать	порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; физические основы формирования технических каналов утеч-

	ки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; структуру и условия формирования технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты информации; номенклатуру применяемых средств физической защиты объектов информатизации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов: **572 часа.**

Из них на освоение МДК **291 часов:**

МДК.03.01Защита информации в ИТКС с использованием технических средств защиты–**148 час;**

МДК.03.02Физическая защита линий связи ИТКС – **124 часов.**

МДК.03.03 Технические средства охраны и видео наблюдения –**144 часов**

На практики учебную и производственную –**144 часов.**

1. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа[1]
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Учебная, часов	Производственная (по профилю специальности), часов	
ПК 3.1- ПК.3.4 ОК 1 – ОК 7, ОК 9	**Раздел 1.** Защита информации в ИТКС с использованием технических средств защиты	**148**	**102**	**40**				**46**
ПК 3.5 ОК 1 – ОК 7, ОК 9	**Раздел 2.**Физическая защита линий связи ИТКС	**124**	**90**	**36**				**34**

*1*Примерная тематика самостоятельных работв рамках образовательной программы планируется образовательной организацией с соответствии с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины.

ПК 3.5 ОК 1 – ОК 7, ОК 9	**Раздел 3.**Технические средства охраны и видео наблюдения	**144**	**99**	**36**				**33**
Учебная практика		**72**				**72**		
Производственная практика		**72**					**72**	
	Промежуточная аттестация	**12**						
	Всего:	**572**	**291**	**116**				**113**

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

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	**Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)**	**Объем часов**
1	2	3
Раздел 1. Защита информации в ИТКС с использованием технических средств защиты		**148**
МДК.03.01.Защита информации в ИТКС с использованием технических средств защиты		**148**
Тема 1.1. Предмет и	**Содержание**	**4**

задачи технической защиты информации	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание**	**4**
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.	
Тема 2.1. Информация как предмет защиты	**Содержание**	**4**
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	
	Практические и лабораторные работы	**3**
	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	
Тема 2.2. Технические каналы утечки информации	**Содержание**	**4**
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	
	Практические и лабораторные работы	**3**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	

Тема 2.3. Методы и средства технической разведки	**Содержание**	**4**
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	
	Тематика практических занятий и лабораторных работ	**3**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**4**
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	
	Тематика практических занятий и лабораторных работ	**3**
	Измерение параметров физических полей	
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание**	**4**
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	
	Практические и лабораторные работы	**3**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**	**4**
	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 кана-	

	лу.	
	Практические и лабораторные работы	**3**
	Защита от утечки по акустическому каналу	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**	**4**
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	
	Практические и лабораторные работы	**3**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**4**
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	
	Практические и лабораторные работы	**3**
	Защита от утечки по виброакустическому каналу	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	**4**
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	
	Практические и лабораторные работы	**6**
	Определение каналов утечки ПЭМИН	**3**

	Защита от утечки по цепям электропитания и заземления	**3**
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**4**
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	
	Практические и лабораторные работы	**2**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**4**
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
	Практические и лабораторные работы	**2**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**	**4**
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	
	Практические и лабораторные работы	**3**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 5.1. Применение технических средств защиты информации	**Содержание**	**4**
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведе-	

	ние измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	
	Практические и лабораторные работы	**2**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**	**4**
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.	
	Практические и лабораторные работы	**3**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Самостоятельная учебная работа при изучении раздела 1 ПМ		**46**
Рекомендуемая тематика самостоятельной работы: 1. Классификация способов и средств защиты информации. 2. Основные и вспомогательные технические средства и системы. 3. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. 4. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика. 5. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информа-		

ции от несанкционированной утечки по акустическому каналу. 6. . Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу. 7. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу. 8. Технические средства для уничтожения информации и носителей информации, порядок применения.		
Раздел 2. Физическая защита линий связи ИТКС		**124**
МДК.03.02. Физическая защита линий связи ИТКС		**124**
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**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.	
	Практические и лабораторные работы	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**6**
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	
	Практические и лабораторные работы	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 2.1. Система	**Содержание**	**5**

обнаружения комплекса инженерно-технических средств физической защиты	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	
	Практические и лабораторные работы	**4**
	Монтаж датчиков пожарной и охранной сигнализации	
Тема 2.2. Система контроля и управления доступом	**Содержание**	
	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.	**6**
	Практические и лабораторные работы	**8**
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	4
	Рассмотрение принципов устройства, работы и применения средств контроля доступа	4
Тема 2.3. Система телевизионного наблюдения	**Содержание**	
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	**5**
	Практические и лабораторные работы	**4**
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	

Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание**	**5**
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	
	Практические и лабораторные работы	**4**
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	
Тема 2.5. Система воздействия	**Содержание**	**5**
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	
	Практические и лабораторные работы	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 3.1. Применение инженерно-технических средств физической защиты	**Содержание**	**6**
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	
	Практические и лабораторные работы	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**6**
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного обо-	

	рудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.	
	Практические и лабораторные работы	
	Тематика учебных занятий формируется образовательной организацией самостоятельно	**4**
Самостоятельная учебная работа при изучении раздела модуля 2 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.		**34**
Раздел 3. Технические средства охраны и видео наблюдения		**144**
МДК.03.03.Технические средства охраны и видео наблюдения		**144**
Тема 1.1 Современная концепция защиты и охраны объекта	**Содержание**	**9**
	Система защиты. Оценка угроз. Принципы построения системы охраны объекта. Технические средства охраны (охранные сигнализация и освещение объекта и его составных частей, системы телевизионного наблюдения и тревожно-вызывной сигнализации, системы сбора, обработки, представления и регистрации информации, получаемой от средств охраны, средства служебной связи). Зоны безопасности объекта, их расположение. Требования к охране зон безопасности объекта.	
Тема 1.2 Извещатели системы охраны	**Содержание**	**9**
	Электромеханические. Емкостные. Радиолокационные. Трибоэлектрические. Акустические. Сейсмические. Вибрационные. Оптические. Ольфактонные. Магнитометрические. Радиационные. Электроконтактные. Магнитоконтактные. Пассивные инфракрасные детекторы. Активные инфракрасные приборы охраны. Ультразвуковые и радиотехнические системы охраны.	
	Практические и лабораторные работы	**6**

	Изучение оптических каналов	
	Утечка информации (атака и защита)	
Тема 1.3 Системы и средства охранного видеонаблюдения	**Содержание**	**8**
	Средства видеонаблюдения. Типовые структуры систем охранного видеонаблюдения. Функции, характеристики и комплектация систем видеонаблюдения.	
	Практические и лабораторные работы	**9**
	АналоговыеCCTV-системы с кассетными видеорекордерами.	
	Аналоговые CCTV-системы с цифровыми видеорегистраторами.	
	Аналоговые CCTV-системы с сетевыми видеорегистраторами.	
Тема 2.1 Цифровые системы видеонаблюдения.	**Содержание**	**8**
	Основные возможности систем цифрового видеонаблюдения. Преимущества цифровой системы видеонаблюдения над аналоговой.	
	Практические и лабораторные работы	**6**
	Сетевые видеосистемы с видеосерверами.	
	Сетевые видеосистемы с сетевыми камерами.	
Тема 2.2 Компьютерное видеонаблюдение.	**Содержание**	**8**
	Особенности и преимущество компьютерного видеонаблюдения. Организация компьютерного видеонаблюдения. Работа по локальной сети.	
	Практические и лабораторные работы	**6**
	Беспроводные системы видеонаблюдения.	
	Режимы работы видеонаблюдения.	
Тема 3.1 Беспроводные системы видеонаблюдения	**Содержание**	**9**
	Основные элементы беспроводной системы видеонаблюдения. Организация беспроводной системы видеонаблюдения. Функции, характеристики передатчиков и приемников. Скрытое видеонаблюдение.	

	Практические и лабораторные работы	**13**
	Видеонаблюдение через интернет.	
	Платы видеозахвата и их функции.	
	Видеокоммутаторы, видеоквадраторы, видеомультиплексоры.	
	Видеозащита в интегрированном комплексе охраны и защиты	
Тема 3.2 Видеонаблюдение через Интернет	**Содержание**	**9**
	Принципы построения систем видеонаблюдения через Интернет. Классификация систем видеонаблюдения. Разбор рекомендаций ГУВО МВД России. Режимы работы видеосистем.	
Учебная практика по профессиональному модулю 1. Монтаж различных типов датчиков. 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. 4. Рассмотрение системы контроля и управления доступом. 5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 6. Рассмотрение датчиков периметра, их принципов работы. 7. Выполнение звукоизоляции помещений системы зашумления. 8. Реализация защиты от утечки по цепям электропитания и заземления. 9. Разработка организационных и технических мероприятий по заданию преподавателя; 10. Разработка основной документации по инженерно-технической защите информации.		
Производственная практика профессионального модуля **Виды работ** 1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;		

3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	
Тематика курсовых проектов (работ): 1. Модель угроз НСД на предприятии 2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии 3. Проведение классификации ПО по требованиям ФСТЭК на предприятии 4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии 5. Построение модели нарушителя по требованиям ФСТЭК на предприятии 6. Построение модели нарушителя по требованиям ФСБ на предприятии 7. Модель угроз безопасности ИС персональных данных на предприятии 8. Комплексная модель защиты информации на предприятии. 9. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) 10. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 11. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание).	
Рекомендуемая тематика внеаудиторной (самостоятельной) работы: 1. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов. 2. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. 3. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. 4. Объектовые средства обнаружения: назначение, устройство, принцип действия.	**33**

5. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. 6. Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. 7. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. 8.Управление системой воздействия.	
Промежуточная аттестация	**12**
Всего по ПМ	**572**

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Лаборатория«Защиты информации от утечки по техническим каналам».

Лаборатория должна быть оснащена средствами защиты информации от утечки по акустическому (виброакустическому) каналу; средствами защиты информации от утечки по каналам, формируемым за счет побочных электромагнитных излучений и наводок; средствами контроля эффективности защиты информации от утечки по акустическому (виброакустическому) каналу и каналам побочных электромагнитных излучений и наводок;

шумогенераторы;

комплексный поисковый прибор;

прожигатели телефонных линий;

устройство обнаружения скрытых видеокамер;

виброакустические генераторы;

подавители диктофонов;

подавители устройств сотовой связи;

устройство защиты аналоговых сигналов;

устройство защиты цифровых сигналов;

стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения, охранно-пожарной сигнализации и охраны объектов;

комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

3.2.1. Печатные издания

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.

2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2013. – 184 с.

4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2013. – 172 с.

5. Е.Б. Белов, В.Н. Пржегорлинский Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/. – М.: Издательский центр «Академия», 2017. – 336с

6. Ю.Ю. Коваленко. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / – М.: Горячая линия – Телеком, 2012.

7. Электронный конспект лекций «Инженерно-техническая защита информации». Составитель: И.Н. Драч, преподаватель ГБОУ СПО РО «РКСИ»

8. Электронный конспект лекций «Криптографическая защита информации». Составитель: Шигаева С.В., преподаватель ГБОУ СПО РО «РКСИ»

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

10. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

11. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012

12. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности: учебник: Рекомендовано УМО, 2009. - 192с.

13. 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. http://www.iprbookshop.ru/66445.html

3.2.2. Электронные издания (электронные ресурсы)

Интернет-ресурсы:

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

Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

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

http://www.morion.ru/
http://www.nateks.ru/
http://www.iskratel.com/
http://www.ps-ufa.ru/
http://3m.com/
http://www.rusgates.ru/index/php - Материалы сайта завода «Ферроприбор»

3.2.3. Дополнительные источники

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
- Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
- Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
- Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
- Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
- Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
- 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.
- Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25

ноября 1994 г.

- 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.
- Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
- 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.
- 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.
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России
  от 30 августа 2002 г. № 282.
- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
- Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России
  от 31 августа 2010 г. № 416/489.
- Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
- Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
- 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.
- Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шиф-

ровальных (криптографических) средств защиты информации».

- 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
- ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
- ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
- ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
- ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
- 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
- ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
- 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
- ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
- ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
- ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
- ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
- ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

Росстандарт, 2014.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
- ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
  Номенклатура показателей качества. Ростехрегулирование, 2005.
- 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.
- ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
- 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.
- 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.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
- Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
- Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

– Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Отечественные журналы:

"InformationSecurity/ Информационная безопасность"
Системный администратор
Компьютер ПРЕСС
Системы безопасности. Журнал для руководителей и специалистов в области
безопасности
Сети и системы связи
Интернет Ресурсы
http://cryptogrof.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями.	- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; - проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение
ПК 3.4. Проводить отдельные работы по физической защите линий связи ИТКС.	выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	Экспертное наблюдение Экзамен

ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение Экзамен
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	Экспертное наблюдение Экзамен
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение Экзамен
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Экспертное наблюдение Экзамен

ПРИЛОЖЕНИЕ 1

Воронежский колледж робототехники и компьютерных технологий

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01D72D329BBD7B20000000072C4B0002
Владелец: Лукина Виктория Борисовна
Действителен: с 09.04.2021 до 09.04.2022

УТВЕРЖДАЮ

Директор колледжа

_____ Лукина В.Б.

«_____» _____ 2019 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

дисциплины

«ПМ.03. ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ»

для специальности среднего профессионального образования **10.02.04" Обеспечение информационной безопасности телекоммуникационных систем "**

Квалификация выпускника: **техник по защите информации**.

Воронеж
2019

Цель фонда оценочных средств. Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты». Перечень видов оценочных средств соответствует Рабочей программе дисциплины.

Фонд оценочных средств включает контрольные материалы для проведения текущего контроля в форме индивидуальных заданий при выполнении цикла лабораторных работ и промежуточной аттестации в форме вопросов и заданий (могут быть заданы как в форме билета, так и экзаменационного теста) к экзамену.

Структура и содержание заданий - задания разработаны в соответствии с рабочей программой дисциплины «защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты».

1. Паспорт фонда оценочных средств

Результатом освоения учебной дисциплины являются предусмотренные ФГОС по специальности умения и знания, направленные на формирование общих и профессиональных компетенций.

Таблица 1

№ п/п	Код компетенции	Содержание компетенции	Планируемые результаты обучения	Наименование оценочного средства
1	ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	**Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (само- **Знания:** актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности	**Задание** на выполнение индивидуального варианта лабораторной работы
2	ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	**Умения:** определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска **Знания:** номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации	**Задание** на выполнение индивидуального варианта лабораторной работы
3	ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.	**Умения:** определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования **Знания:** содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования	**Задание** на выполнение индивидуального варианта лабораторной работы

4	ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	**Умения:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности **Знания:** психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности	**Задание** на выполнение индивидуального варианта лабораторной работы
5	ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	**Умения:** грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе **Знания:** особенности социального и культурного контекста; правила оформления документов и построения устных сообщений.	**Задание** на выполнение индивидуального варианта лабораторной работы
6	ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.	**Умения:** описывать значимость своей специальности **Знания:** сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности	**Задание** на выполнение индивидуального варианта лабораторной работы
7	ОК 09	Использовать информационные технологии в профессиональной деятельности.	**Умения:** применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение **Знания:** современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности	**Задание** на выполнение индивидуального варианта лабораторной работы
8	ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.	**Умения:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы **Знания:** правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности	**Задание** на выполнение индивидуального варианта лабораторной работы

9	ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно-телекоммуникационных системах и сетях	**Умения:** проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации; **Знания:** способов защиты информации от утечки по техническим каналам с использованием технических средств защиты; основных типов технических средств защиты информации от утечки по техническим каналам; законодательства в области информационной безопасности, структуру государственной системы защиты информации, нормативных актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;	**Задание** на выполнение индивидуального варианта лабораторной работы
10	ПК 3.2.	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях	**Умения:** проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации; **Знания:** основных типов технических средств защиты информации от утечки по техническим каналам; организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам; порядка и правил ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;	**Задание** на выполнение индивидуального варианта лабораторной работы
11	ПК 3.3.	Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требовани-	**Умения:** проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации;	**Задание** на выполнение индивидуального варианта лабораторной работы

		ями	**Знания:** способов защиты информации от утечки по техническим каналам с использованием технических средств защиты; основных типов технических средств защиты информации от утечки по техническим каналам; методик измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам; порядка и правил ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;	
12	ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.	**Умения:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных. **Знания:** номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам.	**Задание** на выполнение индивидуального варианта лабораторной работы
13	ВД 3	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты	**Умения:** 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 **Знания:** порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; физические основы формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; структуру и условия формирования технических каналов утечки информации; порядок устранения неисправностей техни-	**Задание** на выполнение индивидуального варианта лабораторной работы

			ческих средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты информации; номенклатуру применяемых средств физической защиты объектов информатизации.	

Формой промежуточной аттестации по учебной дисциплине является

экзамен

указать форму аттестации, предусмотренную учебным планом

2. Формы контроля и оценивания элементов учебной дисциплины

В результате текущей аттестации по учебной дисциплине осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования общих и профессиональных компетенций.

Таблица 2

Раздел / тема дисциплины	**Проверяемые У, З, ОК, ПК**	**Форма текущего контроля и оценивания**
Раздел 1. Защита информации в ИТКС с использованием технических средств защиты	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Самостоятельная работа
Тема 1.1. Предмет и задачи технической защиты информации	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Самостоятельная работа

Тема 1.2. Общие положения защиты информации техническими средствами	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Самостоятельная работа
Тема 1.3. Информация как предмет защиты	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 1
Тема 1.4. Технические каналы утечки информации	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 2
Тема 1.5. Методы и средства технической разведки	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 3
Тема 1.6. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 4
Тема 1.7. Физические процессы при подавлении опасных сигналов	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 5
Тема 1.8. Системы защиты от утечки информации по акустическому каналу	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 6

Тема 1.9. Системы защиты от утечки информации по проводному каналу	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 7
Тема 1.10. Системы защиты от утечки информации по вибрационному каналу	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 8
Тема 1.11. Системы защиты от утечки информации по электромагнитному каналу	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 9
Тема 1.12. Системы защиты от утечки информации по телефонному каналу	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 10
Тема 1.13. Системы защиты от утечки информации по электросетевому каналу	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 11
Тема 1.14. Системы защиты от утечки информации по оптическому каналу	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 12
Тема 1.15. Применение технических средств защиты информации	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 13

Тема 1.16. Эксплуатация технических средств защиты информации	ПК 3.1- ПК.3.4 ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 14
Раздел 2. Физическая защита линий связи ИТКС	ОК 01, 02, 03, 04, 09, 10	Самостоятельная работа
Тема 2.1. Цели и задачи физической защиты объектов информатизации	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 1
Тема 2.2. Общие сведения о комплексах инженерно-технических средств физической защиты	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 2

Тема 2.3. Система обнаружения комплекса инженерно-технических средств физической защиты	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 3
Тема 2.4. Система контроля и управления доступом	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 4-5
Тема 2.5. Система телевизионного наблюдения	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 6
Тема 2.6. Система сбора, обработки, отображения и документирования информации	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 7

Тема 2.7. Система воздействия	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 8
Тема 2.8. Применение инженерно-технических средств физической защиты	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 9
Тема 2.9. Эксплуатация инженерно-технических средств физической защиты	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 10
Раздел 3. Технические средства охраны и видео наблюдения	ОК 01, 02, 03, 04, 09, 10	Самостоятельная работа

Тема 3.1 Современная концепция защиты и охраны объекта	ОК 01, 02, 03, 04, 09, 10	Самостоятельная работа
Тема 3.2 Извещатели системы охраны	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 1-2
Тема 3.3 Системы и средства охранного видеонаблюдения	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 3-5
Тема 3.4 Цифровые системы видеонаблюдения.	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 6-7
Тема 3.5 Компьютерное видеонаблюдение.	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 8-9

Тема 3.6 Беспроводные системы видеонаблюдения	ОК 01, 02, 03, 04, 09, 10	Практическое занятие №№ 10-14
Тема 3.7 Видеонаблюдение через Интернет	ОК 01, 02, 03, 04, 09, 10	Самостоятельная работа

3. Оценка освоения учебной дисциплины

3.1 Тематика курсовых работ

1. Модель угроз НСД на предприятии
2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии
3. Проведение классификации ПО по требованиям ФСТЭК на предприятии
4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии
5. Построение модели нарушителя по требованиям ФСТЭК на предприятии
6. Построение модели нарушителя по требованиям ФСБ на предприятии
7. Модель угроз безопасности ИС персональных данных на предприятии
8. Комплексная модель защиты информации на предприятии.
9. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание)
10. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание)
11. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание).

4. Контрольно-оценочные материалы для промежуточной аттестации по учебной дисциплине

Оценка освоения дисциплины предусматривает проведение экзамена

указать форму аттестации, предусмотренную учебным планом

4.1. Вопросы (задания) к экзамену по дисциплине:

1. Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности.
2. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.
3. 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. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ.
5. 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.
6. Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации.
7. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.
8. Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации
9. 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.
10. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей
11. Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.
12. 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.
13. Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов.
14. Номенклатура применяемых средств защиты информации от несанкцио-

нированной утечки по проводному каналу.

15. 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.
16. Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок.
17. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.
18. Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке
19. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.
20. Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.

5. Критерии и шкалы для интегрированной оценки уровня сформированности компетенций

Индикаторы компетенции	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**отлично**
Полнота знаний	Уровень знаний ниже минимальных требований. Лабораторные работы выполнены не в полном объеме	Минимально допустимый уровень знаний. Лабораторные работы выполнены в полном объеме	Уровень знаний в объеме, соответствующем программе подготовки. Лабораторные работы выполнены в полном объеме	Уровень знаний в объеме, соответствующем программе подготовки, лабораторные работы выполнены в полном объеме
Наличие умений	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи. Индивидуальные задачи решены по типовому шаблону.	Продемонстрированы все основные умения. Решены типовые задачи. Выполнены индивидуальные задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения, решены все основные задачи, выполнены все индивидуальные задания в полном объеме.
Характеристика сформированности компетенции	Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. Требуется повторное обучение	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по большинству практических задач.	Сформированность компетенции в целом соответствует требованиям, но есть недочеты. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по некоторым профессиональным задачам.	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач.
Уровень сформированности компетенций	Низкий	Ниже среднего	Средний	Высокий