Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

КОЛЛЕДЖ КОСМИЧЕСКОГО МАШИНОСТРОЕНИЯ И ТЕХНОЛОГИЙ

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»

Королев, 2023 г.

Авторы: Синицын К.А., Чебышев А.Ю. Рабочая программа профессионального модуля ПМ.03 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты». – Королев МО: ТУ им. А.А. Леонова, 2023 г.

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования (далее - ФГОС СПО) и учебного плана по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Рабочая программа рассмотрена и одобрена на заседании цикловой комиссии по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем 16 мая 2023 г., протокол № 6.

Рабочая программа учебной дисциплины рекомендована к реализации в учебном процессе на заседании учебно-методического совета 17 мая 2023 г., протокол № 5.

Содержание

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Место модуля в структуре образовательной программы

Профессиональный модуль «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» принадлежит к профессиональному циклу.

1.2. Цель и планируемые результаты освоения профессионального модуля

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

1.2.1. Перечень общих компетенций

Код	Наименование общих компетенций
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 решение.
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 09.	Использовать информационные технологии в профессиональной деятельности.

1.2.2. Перечень профессиональных 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

Код	Наименование видов деятельности и профессиональных компетенций
	информационно-телекоммуникационных систем и сетей.

1.2.3. В результате освоения профессионального модуля обучающийся должен:

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

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

1.3. Количество часов, отводимое на освоение профессионального модуля:

Всего часов 924

Из них на освоение МДК 510 часов

в том числе самостоятельная работа 10 часов

практики, в том числе учебная 252 часа

производственная 144 часа

Консультации 4 часа

Промежуточная аттестация 36 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Тематический план профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля		Объем профессионального модуля, ак. час.							
		Суммарный объем нагрузки, час.	Работа обучающихся во взаимодействии с преподавателем							Самостоятельная работа
			Обучение по МДК				Практики		Консультации	
			Всего	В том числе			Учебная	Производственная		
				Промежут. аттест.	Лаборат. и практ. занятий	Курсовых работ (проектов)				
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
ПК 3.1 – ПК 3.4 ОК 01- ОК 07, ОК 09	Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	**290**	**284**	**18**	**74**	**-**	**-**	**-**	**-**	**6**
	Раздел 2. Физическая защита линий связи информационно-телекоммуникационных систем	**220**	**194**		**70**	**30**	**-**	**-**	4	**4**
	Учебная практика	**252**					**252**			
	Производственная практика (по профилю специальности), часов	**144**						**144**		
	Промежуточная аттестация (экзамен квалификационный)	**18**		**18**						
	Всего:	924	478	36	144	30	252	144	4	10

2.2. Содержание профессионального модуля

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		**290**
МДК.03.01.Защита информации в ИТКС с использованием технических средств защиты		284
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	**12**
	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**	**8**
	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.	
	Практические и лабораторные работы	**4**
	Принципы построения систем защиты информационной безопасности объектов информатизации. Классификация АИС и средств защиты информации.	
Тема 2.1. Информация как предмет защиты	**Содержание**	**16**
	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	**4**
	Демаскирующие признаки объектов наблюдения, сигналов и веществ. Источники опасных сигналов. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	
Тема 2.2. Технические каналы утечки	**Содержание**	**10**
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация	

информации	существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	
	Практические и лабораторные работы	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 2.3. Методы и средства технической разведки	**Содержание**	**14**
	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	**6**
	. Понятие и особенности утечки информации. Технические каналы утечки информации. Методы и средства технической разведки	
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**14**
	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	**6**
	Виды паразитных связей и наводок. Утечки информации по каналам побочных электромагнитных излучений и наводок. Измерение параметров физических полей	
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание**	**14**
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	
	Практические и лабораторные работы	**6**
	Методы защиты информации в канале связи. Пассивные методы защиты акустической информации. Активные методы защиты акустической информации.	
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**	**16**
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	
	Практические и лабораторные работы	**4**
	Защита речевой информации. Средства защиты информации от утечки по акустическому каналу.	

Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**	**14**
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	
	Практические и лабораторные работы	**4**
	Средств защиты информации от несанкционированной утечки по проводному каналу. Системы защиты от диктофонов.	
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**14**
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	
	Практические и лабораторные работы	**4**
	Защита от утечки по виброакустическому каналу	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	**16**
	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	**8**
	Системы защиты от утечки информации по электромагнитному каналу. Защита от утечки по цепям электропитания и заземления	
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**10**
	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**
	Защита от утечки информации по телефонному каналу.	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**8**
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
	Практические и лабораторные работы	**6**

	Низкочастотные и высокочастотные устройства съема информации. Средства защиты информации от несанкционированной утечки по электросетевому каналу.	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**	**12**
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	
	Практические и лабораторные работы	**4**
	Системы защиты информации по оптическому каналу.	
Тема 5.1. Применение технических средств защиты информации	**Содержание**	**8**
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	
	Практические и лабораторные работы	**6**
	Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок. Проведение измерений параметров фоновых шумов и физических полей.	
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**	**14**
	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	**6**
	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.	
Самостоятельная учебная работа при изучении раздела 1 ПМ		**6**

Рекомендуемая тематика самостоятельной работы: 1. Классификация способов и средств защиты информации. 2. Основные и вспомогательные технические средства и системы. 3. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. 4. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика. 5. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу. 6. . Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу. 7. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу. 8. Технические средства для уничтожения информации и носителей информации, порядок применения.		
Раздел 2. Физическая защита линий связи информационно-телекоммуникационных систем и сетей		**220**
МДК.03.02. Физическая защита линий связи информационно-телекоммуникационных систем и сетей		**194**
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**12**
	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**
	Цели и задачи физической защиты объектов информатизации. Методы и средства инженерной защиты и технической охраны объектов информатизации	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**10**
	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	**10**
	Принципы обеспечения безопасности объектов информатизации, жизненный цикл СОИБ Принципы построения интегрированных систем охраны объектов информатизации. Классификация и состав интегрированных систем охраны объектов информатизации. Требования к инженерным средствам физической защиты объектов информатизации. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к объектам информатизации	

Тема 2.1. Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**	**16**
	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	**12**
	Основы построения системы охранной сигнализации. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения. Объектовые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения.	
Тема 2.2. Система контроля и управления доступом	**Содержание**	**22**
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	
	Практические и лабораторные работы	**8**
	Структура и состав СКУД. Основы построения и принципы функционирования СКУД. Методы удостоверения личности, применяемые в СКУД. Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Тема 2.3. Система телевизионного наблюдения	**Содержание**	**18**
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	
	Практические и лабораторные работы	**6**
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание**	**6**
	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**	**2**
	Назначение и классификация технических средств воздействия. Основные показатели технических	

	средств воздействия.	
	Практические и лабораторные работы	**4**
	Рассмотрение структуры и построение системы сбора и обработки информации.	
Тема 3.1. Применение инженерно-технических средств физической защиты	**Содержание**	**4**
	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	**12**
	Работа с периферийным оборудованием системы контроля и управления доступом. Организация пропускного режима. Управление системой телевизионного наблюдения. Эксплуатация устройств отображения и документирования информации. Применение инженерно-технических средств физической защиты.	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**4**
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.	
	Практические и лабораторные работы	**10**
	Порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка инженерно-технических средств физической защиты. Диагностика и восстановление работоспособности технических средств физической защиты.	
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.		**4**
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.		***252***

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.	**144**
Тематика курсовых проектов: 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).	**30**
Внеаудиторная (самостоятельная) учебная работа обучающегося над курсовым проектом	

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. 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 (экзамен квалификационный)	**36**
Всего по профессиональному модулю	**924**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация профессионального модуля требует наличия учебной мастерской «Анализ защищенности информационных систем от внешних угроз».

Оборудование мастерской:

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

Технические средства обучения:

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

Оборудование мастерской:

№	Наименование оборудования	Кол-во
1	Автоматизированное рабочее место: Системный блок: - Intel Core i7-9700; - базовая тактовая частота 3.0 ГГц; - количество физических ядер 8; - количество потоков 8; ОЗУ: - 16 Гб; ПЗУ: - SSD объемом 500 Гб, HDD объемом 1000 Гб; сетевой адаптер: - технология Ethernet стандарта 1000BASE-T. Монитор: - ЖКД Dell p2419h с диагональю 24" (2 шт.) Клавиатура Logitech без клавиши Power, подключение по USB Компьютерная мышь: Logitech, подключение по USB	20
2	Экран с проектором Panasonic PT-VW360	1
3	Телекоммуникационный шкаф 42U	2

4	Автоматизированное рабочее место: Системный блок: - Intel Core i7-9700; - базовая тактовая частота 3.0 ГГц; - количество физических ядер 8; - количество потоков 8; ОЗУ: - 16 Гб; ПЗУ: - SSD объемом 500 Гб, HDD объемом 1000 Гб; сетевой адаптер: - технология Ethernet стандарта 1000BASE-T. Монитор: - ЖКД Dell p2419h с диагональю 24" (2 шт.)	4
5	Маршрутизатор Cisco ISR 4300 Series	10
6	Коммутатор Cisco 2960 plus	20
7	Межсетевой экран ASA 5506-X	10
8	Платформа RouterBoard MikroTik (Маршрутизатор, коммутатор, PoE)	20
9	Комплексный стенд по защите информации	1

Перечень программных средств:

№	Наименование	Количество лицензий
1	MS Windows 10	20
2	MS Office 2013 Pro Plus	20
3	Adobe reader	20
4	7-zip	20
5	Libre Office	20
6	Notepad++	20
7	Sublime Text 3	20
8	Visual Studio 2019	20
9	Visual Studio Code	20
10	WebStorm	20
11	VirtualBox	20
12	Putty	20
13	OpenServer (Ultimate)	20
14	Linux Debian / Linux Centos	20
15	Cisco Packet Tracer	20
16	Autodesk DWG TrueView	20
17	MS SQL Server Express	20
18	SQL Server Management Studio	20
19	MySQL Community Edition	20

3.2. Информационное обеспечение обучения

Основные источники:

1. Технические средства автоматизации и управления: Учебное пособие / Шишов О. В. - М.: НИЦ ИНФРА-М, 2021. - 396 с.: 60х90 1/16. - (Высшее образование: Бакалавриат) (Переплёт) ISBN 978-5-16-010325-9 https://znanium.com/read?id=361160

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

3. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2020. - 352 с.: ил.; 60х90 1/16. - (Высшее образование). (переплет) ISBN 978-5-00091-557-8. https://znanium.com/catalog/document?id=364477

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

Дополнительные источники:

1. Технические средства автоматизации и управления: Учебное пособие / Шишов О. В. - М.: НИЦ ИНФРА-М, 2020. - 396 с.: 60х90 1/16. - ISBN 978-5-16-010325-9 https://znanium.com/read?id=361160

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

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

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

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

6. Технические средства автоматизации и управления: Учебное пособие / Шишов О. В. - М.: НИЦ ИНФРА-М, 2021. - 396 с.: 60х90 1/16. - https://znanium.com/read?id=361160

7. Программно-аппаратная защита информации: Учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - М.: Форум: НИЦ ИНФРА-М, 2021. - 352 с.: ил.; 60x90 1/16. - (Высшее образование). (переплет) ISBN 978-5-00091-557-8.https://znanium.com/catalog/document?id=364477

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

9. Ворона В. А., Тихонов В. А. В83 Комплексные (интегрированные) системы обеспечения безопасности. – М.: Горячая линия–Телеком, 2020. – 160 с.: ил. ISBN 978-5-9912-0238-1.

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

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

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

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

– Доктрина информационной безопасности Российской Федерации

– Положение «О государственной системе защиты информации в российской федерации от иностранных технических разведок и от ее утечки по техническим каналам» (извлечения). Утверждено Постановлением Совета Министров Правительства Российской Федерации от 15.09.1993 № 912-51.

– Указ Президента Российской Федерации от 12 мая 2009 года № 537 «О Стратегии национальной безопасности Российской Федерации» Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

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

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

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

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

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

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

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

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

– Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

– 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.

Электронные издания (электронные ресурсы):

- Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
- Федеральный портал «Информационно - коммуникационные технологии в образовании» http://oso.rcsz.ru/info/kompas/edu.htm
- Всероссийский образовательный портал https://edu-ikt.ru/
- www.dedal.ru.
- www.neurophotonica.ru.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Таблица 1

Результаты освоения профессиональных компетенций

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и 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.	Фронтальный и письменный опрос. Тестирование. Экспертное наблюдение
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты ин-формации, 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.	Фронтальный и письменный опрос. Тестирование. 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.	Фронтальный и письменный опрос. Тестирование. 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	Фронтальный и письменный опрос. Тестирование. Экспертное наблюдение.

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
	(в том числе криптографических) средств защиты информации	

Таблица 2

Результаты освоения общих компетенций

Результаты (освоенные общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ОК 01 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Оценивать уровень сложности профессиональных заданий с учетом имеющихся знаний.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 02 Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Нахождение и использование информации для эффективного выполнения профессиональных задач, профессионального и личностного развития; Эффективный поиск необходимой информации; Использование при решении профессиональных задач различных источников информации, включая электронные.	Оценка деятельности обучающегося в процессе освоения образовательной программы на практических занятиях
ОК 03 Планировать и реализовывать собственное профессиональное и личностное решение.	Умение самостоятельно определять задачи профессионального и личностного развития;	Оценка по результатам наблюдения за поведением в процессе освоения профессионального модуля и выполнения работ на практических занятиях, учебной практике, экзамене
ОК 04 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Взаимодействие с обучающимися, преподавателями руководителями в ходе обучения;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Демонстрация коммуникативных навыков в процессе освоения образовательной программы	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	Анализ ситуационных задач, демонстрация использования принципов делового общения в профессиональной деятельности	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

ОК 07 Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Демонстрация применения знаний охраны труда	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 09 Использовать информационные технологии в профессиональной деятельности.	Использование информационно-коммуникационных технологий в профессиональной деятельности	Оценка по результатам наблюдения за поведением в процессе освоения профессионального модуля и выполнения работ на практических занятиях, учебной практике, экзамене (квалификационном)

Критерии оценки ответов

При оценке ответов дополнительно должны быть учтены качество сообщения, отражающего основные моменты и ответы на вопросы, заданные по теме вопроса.

Результаты защиты определяются оценками *«отлично», «хорошо», «удовлетворительно», «неудовлетворительно».*

1. Оценки ***«отлично»*** заслуживает ответ, в котором полно и всесторонне раскрыто теоретическое содержание темы, дан глубокий критический анализ действующей практики учетно-аналитической работы. Обучающийся при ответе дал аргументированные ответы на все вопросы преподавателя, проявил творческие способности в понимании и изложении ответов на вопросы.

2. Оценка ***«хорошо»*** выставляется за ответ, который имеет убедительный ответ. При его этом обучающийся показывает знания вопросов темы, оперирует данными, вносит предложения по теме ответа, во время ответа использует наглядные пособия, без особых затруднений отвечает на поставленные вопросы.

3. Оценка ***«удовлетворительно»*** выставляется за ответ, в котором имеются замечания по содержанию ответа и методике анализа. В теоретических, выводы в основном правильные, предложения представляют интерес, но недостаточно убедительно аргументированы и не на все вопросы обучающийся дал правильные ответы.

4. Оценка ***«неудовлетворительно»*** выставляется за ответ, который в основном отвечает предъявляемым вопросам, но обучающийся не дал правильных ответов на большинство заданных вопросов, т.е. обнаружил серьезные пробелы в профессиональных знаниях.