МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
Северо-Кавказский филиал

СОГЛАСОВАНО

Генеральный директор ООО «Промышленные системы автоматического управления»

_____ В.Г. Потемкин

«19» января 2021 г.

УТВЕРЖДАЮ:
Директор СКФ БГТУ
им. В.Г. Шухова

_____ В.Л. Курбатов

«24» февраля 2021 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

основной профессиональной образовательной программы – программы подготовки специалистов среднего звена
Специальность
10.02.05 Обеспечение информационной безопасности автоматизированных систем
(базовой подготовки)
Квалификация выпускника
Техник по защите информации
Срок обучения
3 года 10 месяцев

Минеральные Воды, 2021 г.

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного Приказом Министерства образования и науки РФ № 1553 от 09.12.2016 г.,
- Плана учебного процесса БГТУ им. В.Г. Шухова по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного в 2021 г.

Организация разработчик: СКФ ФГБОУ ВО «БГТУ им. В.Г. Шухова», Северо-Кавказский филиал

Составитель: старший преподаватель  О.А. Митюгова

ученая степень и звание подпись инициалы, фамилия

Рабочая программа обсуждена и рекомендована на заседании кафедры Экономических и естественно-научных дисциплин

название кафедры

«_24_» _февраля_ 2021 г., протокол №_7__

Заведующий кафедрой: к.пед.н.  И.В. Черкасова

ученая степень и звание подпись инициалы, фамилия

Согласовано с работодателями:

ФИО	***Должность, место работы***
Потемкин Владимир Григорьевич	Директор ООО «Промышленные системы автоматического управления»

СОДЕРЖАНИЕ

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

1.1. Цель и планируемые результаты освоения профессионального модуля

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

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	**Защита информации техническими средствами**
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

1.1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

.

Иметь практический опыт в	− установке, монтажа и настройки технических средств защиты информации; − техническомобслуживании технических средств защиты информации; − применения основных типов технических средств защиты информации; − выявлении технических каналов утечки информации; − применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации; − проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; − проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
уметь	− применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; − применять технические средства для криптографической защиты информации конфиденциального характера; − применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; − применять инженерно-технические средства физической защиты объектов информатизации
знать	− физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; − номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; − основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации; − основные способы физической защиты объектов информатизации; − методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; − номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов:	**602**
на освоение МДК	**374**
теоретическое обучение	178
лабораторные занятия	126
Самостоятельная работа	20
Консультации	2
Промежуточная аттестация	30
Курсовой проект	30
на практики	**216**
учебную	108
производственную (по профилю специальности)	108
Экзамен по профессиональному модулю (демонстрационный экзамен)	**12**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.			Практики		Самостоятельная работа
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 3.1-ПК.3.4 ОК 1–ОК10	**Раздел 1 модуля.** Применение технической защиты информации	**172**	**150**	70	–	**–**	–	*10*
ПК 3.5 ОК 01–ОК10	**Раздел 2 модуля.** Применение инженерно-технических средств физической защиты объектов информатизации	**202**	**186**	56	30	**–**	–	*10*
ПК 3.1-ПК.3.5 ОК 1–ОК10	Учебная практика	**108**				**108**	**–**	–
ПК 3.1-ПК.3.5 ОК 1–ОК10	Производственная практика (по профилю специальности)	**108**					**108**	–
	Экзамен по профессиональному модулю	**12**	**12**	–	**–**	**–**	**–**	**–**
	Всего:	**602**	**366**	126	30	**108**	**108**	20

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов
1	2	3
Раздел 1 модуля. Применение технической защиты информации		**172**
МДК.03.01 Техническая защита информации		**172**
Раздел 1. Концепция инженерно-технической защиты информации		
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание учебного материала**	2
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание учебного материала**	4
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.	
	Тематика лабораторных занятий	2
	Определение основных показателей эффективности инженерно-технической защиты информации	
Раздел 2. Теоретические основы инженерно-технической защиты информации		
Тема 2.1. Информация как предмет защиты	**Содержание учебного материала**	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.	
	Тематика лабораторных занятий	4

	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.	
	Тематика лабораторных занятий	4
	Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения	
Тема 2.3. Методы и средства технической разведки	**Содержание учебного материала**	4
	Классификация технических средств разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	
	Тематика лабораторных занятий	8
	Методы и средства технической разведки.	
	Методы технического закрытия речевых сигналов	
Раздел 3. Физические основы технической защиты информации		
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание учебного материала**	6
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	
	Тематика лабораторных занятий	4
	Измерение параметров физических полей	
Тема 3.2. Физические процессы при подавлении опасных	**Содержание учебного материала**	2
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	

сигналов	**Тематика лабораторных занятий**	4
	Изучение физических процессов при подавлении опасных сигналов	
Раздел 4. Системы защиты от утечки информации		
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание учебного материала**	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 каналу.	
	Тематика лабораторных занятий	4
	Защита от утечки по акустическому каналу	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание учебного материала**	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.	
	Тематика лабораторных занятий	4
	Распространение сигналов в технических каналах утечки информации	
Самостоятельная работа обучающихся Подготовка к лабораторным занятиям с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.		6
Промежуточная аттестация по МДК.03.01 в форме дифференцированного зачета		2
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание учебного материала**	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.	
	Тематика лабораторных занятий	4
	Защита от утечки по виброакустическому каналу	
Тема 4.4. Системы защиты от утечки	**Содержание учебного материала**	6
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей	

информации по электромагнитному каналу	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.	
	Тематика лабораторных занятий	8
	Определение каналов утечки ПЭМИН	
	Защита от утечки по цепям электропитания и заземления	
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание учебного материала**	6
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	
	Тематика лабораторных занятий	4
	Ознакомление с номенклатурой применяемых средств защиты информации от несанкционированной утечки по телефонному каналу	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание учебного материала**	4
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
	Тематика лабораторных занятий	4
	Ознакомление с номенклатурой применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание учебного материала**	4
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	
	Тематика лабораторных занятий	2
	Изучение принципа действия системы защиты информации по оптическому каналу	
Раздел 5. Применение и эксплуатация технических средств защиты информации		
Тема 5.1. Применение	**Содержание учебного материала**	10

технических средств защиты информации	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.	
	Тематика лабораторных занятий	6
	Измерение параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации	
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание учебного материала**	10
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.	
	Тематика лабораторных занятий	8
	Установка и настройка технических средств защиты информации.	
Самостоятельная работа обучающихся Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторным занятиям с использованием методических рекомендаций преподавателя, отчетов к их защите.		4
Консультации		*6*
Промежуточная аттестация по МДК.03.01 в форме экзамена		*6*
Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации		**202**
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**202**
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание учебного материала**	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.	
	Тематика лабораторных занятий	6
	Изучение характеристик потенциально опасных объектов	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание учебного материала**	12
	Общие принципы обеспечения безопасности объектов.	
	Жизненный цикл системы физической защиты	
	Требования к инженерным средствам физической защиты.	
	Принципы построения интегрированных систем охраны.	
	Классификация и состав интегрированных систем охраны.	
	Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	
	Тематика лабораторных занятий	6
	Изучение принципа работы интегрированной систем охраны	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание учебного материала**	10
	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.	
	Тематика лабораторных занятий	6
	Монтаж датчиков пожарной и охранной сигнализации	
Тема 2.2. Система контроля и управления доступом	**Содержание учебного материала**	16
	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.	
	Тематика лабораторных занятий	8
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	
	Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Тема 2.3. Система телевизионного наблюдения	**Содержание учебного материала**	16
	Аналоговые и цифровые системы видеонаблюдения.	
	Назначение системы телевизионного наблюдения..	
	Состав системы телевизионного наблюдения.	
	Видеокамеры	
	Объективы.	
	Термокожухи.	
	Поворотные системы.	
	Инфракрасные осветители.	
	Детекторы движения.	
	Тематика лабораторных занятий	**6**
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	
Самостоятельная работа обучающихся Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к лабораторным занятиям с использованием методических рекомендаций преподавателя, отчетов к их защите.		6
Промежуточная аттестация по МДК.03.02 в форме дифференцированного зачета		2

Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание учебного материала**	8
	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.	
	Тематика лабораторных занятий	4
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	
Тема 2.5 Система воздействия	**Содержание учебного материала**	4
	Назначение и классификация технических средств воздействия.	
	Основные показатели технических средств воздействия.	
	Тематика лабораторных занятий	4
	Расчет показателей технических средств воздействия.	
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		
Тема 3.1 Применение инженерно-технических средств физической защиты	**Содержание учебного материала**	8
	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.	
	Тематика лабораторных занятий	6
	Работа с периферийным оборудованием системы контроля и управления доступом.	
	Управление системой воздействия.	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание учебного материала**	10
	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.	
	Тематика лабораторных занятий	10
	Установка и настройка периметровых и объектовых технических средств обнаружения	
	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты	
	Организация ремонта технических средств физической защиты	
Курсовая работа		34
Тематика курсовых работ 1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.		
Обязательная аудиторная учебная нагрузка по курсовому проекту Подготовить и оформить введение на курсовой проект. Изучить исходные данные курсового проекта. Составление плана и оглавления работы Подготовить теоретический раздел курсового проекта Оформить теоретический раздел курсового проекта. Изучить существующие методы решения исходной задачи и выбрать оптимальное. Оформить результаты решения индивидуальной задачи. Сделать выводы по результатам аналитического решения. Составить алгоритм решения индивидуальной задачи Реализовать решение задачи на практике		30
Самостоятельная работа по курсовому проекту Подготовить и оформить введение на курсовой проект. Изучить исходные данные курсового проекта. Подготовить и оформить теоретический раздел курсового проекта. Изучить существующие методы решения исходной задачи и выбрать оптимальное. Оформить результаты решения индивидуальной задачи. Сделать выводы по результатам аналитического решения.		4

Оформить пояснительную записку КП согласно требованиям.	
Консультации	2
Промежуточная аттестация по МДК.03.02 в форме экзамена	6
Учебная практика **Виды работ:** – Измерение параметров физических полей. – Определение каналов утечки ПЭМИН. – Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. – Установка и настройка технических средств защиты информации. – Проведение измерений параметров побочных электромагнитных излучений и наводок. – Проведение аттестации объектов информатизации. – Монтаж различных типов датчиков. – Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. – Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. – Рассмотрение системы контроля и управления доступом. – Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. – Рассмотрение датчиков периметра, их принципов работы. – Выполнение звукоизоляции помещений системы зашумления. – Реализация защиты от утечки по цепям электропитания и заземления. – Разработка организационных и технических мероприятий по заданию преподавателя; – Разработка основной документации по инженерно-технической защите информации.	**108**
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	***108***

технических средствами.	
Экзамен по профессиональному модулю	***12***
Всего	***602***

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Кабинет информатики. № 21. Лаборатория технических средств защиты информации.

Оснащена информационными стендами, по 10 компьютеров на базе процессора DualCoreIntelCore i3, оперативной памятью 4ГБ и жестким диском 500 ГБ, локальной сетью с пропускной способностью 100 Мбит/с, операционная система Windows 7 (32-bit) учебной доской, учебно-методическими пособиями, наглядными пособиями, стульями на 1 ученика 1 стул, столами 1 шт. на 2 человек,

Оснащена аппаратными средствами аутентификации пользователя; средствами защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок; средствами измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и т.д.); стендами физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов.

3.2. Информационное обеспечение обучения: перечень рекомендуемых учебных изданий, интернет-ресурсов, дополнительной литературы, периодических изданий, программного обеспечения

3.2.1. Основная литература:

1. Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю. Н. Рагозин ; под редакцией Т. С. Кулакова. — Санкт-Петербург : Интермедия, 2018. — 168 c. — ISBN 978-5-4383-0161-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/73641.html. — Режим доступа: для авторизир. Пользователей
2. Технологии защиты информации в компьютерных сетях : учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — Саратов : Профобразование, 2021. — 368 c. — ISBN 978-5-4488-1014-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102207.html. — Режим доступа: для авторизир. пользователей
3. Методы и средства инженерно-технической защиты информации : учебное пособие / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, Т. Р. Гайнулин. — Брянск : Брянский государственный технический университет, 2012. — 187 c. — ISBN 5-89838-357-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/7000.html. — Режим доступа: для авторизир. Пользователей
4. Разработка системы технической защиты информации : учебное пособие / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, Т. Р. Гайнулин. — Брянск : Брянский государственный технический университет, 2012. — 187 c. — ISBN 5-89838-358-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/7005.html. — Режим доступа: для авторизир. пользователей
5.

3.2.2. Дополнительная литература:

1. Шелухин, О. И. Системы обнаружения вторжений в компьютерные сети : учебное

пособие / О. И. Шелухин, А. Н. Руднев, А. В. Савелов. — Москва : Московский технический университет связи и информатики, 2013. — 88 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/63360.html. — Режим доступа: для авторизир. Пользователей
2. Бубнов А.А. Техническая защита информации в объектах информационной инфраструктуры : учебник для студ. Сред. Проф. Заведений / А.А. Бубнов, В.Н. Пржегорлинский, К.Ю. Фомина. - Москва : "Академия", 2019. - 272 с.
3. Технологии защиты информации в компьютерных сетях : учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — Саратов : Профобразование, 2021. — 368 с. — ISBN 978-5-4488-1014-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102207.html. — Режим доступа: для авторизир. Пользователей
4. Каторин, Ю. Ф. Защита информации техническими средствами : учебное пособие / Ю. Ф. Каторин, А. В. Разумовский, А. И. Спивак ; под редакцией Ю. Ф. Каторин. — Санкт-Петербург : Университет ИТМО, 2012. — 417 с. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/66445.html. — Режим доступа: для авторизир. пользователей

3.2.3. Официальные, справочно-библиографические издания

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

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

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

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

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

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

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

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

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

10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

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

12. Меры защиты информации в государственных информационных системах.

Утверждены ФСТЭК России 11 февраля 2014 г.

13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

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

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

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

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

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

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

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

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

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

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

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

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

27. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
28. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
29. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
30. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
31. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
33. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
34. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
35. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

3.2.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), необходимых для освоения дисциплины

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru

6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке ипроведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных заданий, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных заданий, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных заданий, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных заданий, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных заданий, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно	- взаимодействие с обучающимися, преподавателями и	

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

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