Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
(Финансовый университет)
Колледж информатики и программирования

СОГЛАСОВАНО
Акционерное общество
«Особое Конструкторское Бюро Систем
Автоматизированного Проектирования»
(АО «ОКБ САПР»)
Генеральный директор

_____ И.Г. Назаров
«__» _____ 2023 г.

УТВЕРЖДАЮ

Заместитель директора
по учебной работе

_____ Н.Ю. Долгова
«26» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

10.02.05 Обеспечение информационной безопасности
автоматизированных систем

Москва 2023 г.

Рабочая программа профессионального модуля на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Разработчики:
Маринич А.Л.., преподаватель первой квалификационной категории Колледжа информатики и программирования
Филатов А.П., преподаватель первой квалификационной категории Колледжа информатики и программирования.

Рабочая программа профессионального модуля рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии Основы информационной безопасности

Протокол от «11» мая 2023 г. № 9

Председатель предметной (цикловой) комиссии _____ А.Л. Маринич

1. Общая характеристика рабочей программы профессионального модуля

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности «Защита информации техническими средствами» и соответствующие ему общие компетенции, и профессиональные компетенции:

1.1.1. Перечень общих компетенции

Код	Общие компетенции
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК.11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

1.1.2. Перечень профессиональных компетенций

Код	Профессиональные компетенции
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.

1.1.3. В результате освоения профессионального модуля студент должен:

иметь практический опыт	– установки, монтажа и настройки технических средств защиты информации; – технического обслуживания технических средств защиты информации; – применения основных типов технических средств защиты информации; – выявления технических каналов утечки информации; – участия в мониторинге эффективности технических средств защиты информации; – диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; – проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; – проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; – установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты; – *технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты информации за счет побочных электромагнитных излучений и наводок;* * – *технического обслуживания, диагностики, устранения отказов и неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам.**
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, *технических средств защиты акустической речевой информации от утечки по техническим каналам**;

	− применять инженерно-технические средства физической защиты объектов информатизации, − *производить установку и монтаж, настройку и испытание, техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов .**
знать	− порядок технического обслуживания технических средств защиты информации; − номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; − физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; − порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; − методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; − номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; − основные принципы действия и характеристики технических средств физической защиты; − номенклатуру применяемых средств физической защиты объектов информатизации; − основные способы физической защиты объектов информатизации; − *порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации** ; − *нормативно правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации **; − *номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.** .

**вариативная часть*

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 594 часа, в том числе в форме практической подготовки 414 часов

Из них на освоение МДК 366 часов,

в том числе самостоятельная работа 14 часов.

Практики, в том числе учебная 72 часа,

производственная (по профилю специальности) 144 часа.

Курсовой проект (работа) в составе МДК 03.02 30 часов

Экзамен по модулю экзамен 12 часов

2. Структура и содержание профессионального модуля

2.1. Структура профессионального модуля пм.03 защита информации техническими средствами

Коды компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час	В т. ч. в форме практическая подготовка	Объем профессионального модуля, ак.час,						
				Работа студентов во взаимодействии с преподавателем						Самостоятельная работа
				Обучение по МДК				Практики		
				Всего	в том числе					
					Промежуточная аттестация	Лабораторных и практических занятий	Курсовых работ (проектов)	Учебная	Производственная	
1	2	3	4	5	6	7	8	9	10	11
ПК 3.1-ПК.3.4 ОК 01–ОК11	Раздел 1. Применение технической защиты информации	230	122	172	12	86	-	36	-	10
ПК 3.5 ОК 01–ОК11,	Раздел 2. Применение инженерно-технических средств физической защиты объектов информатизации	208	148	156	12	82	30	36	-	4

ПК.3.5, ОК 01–ОК11	Производственная практика (по профилю специальности)	144	144						144	
	Экзамен по модулю	12			12					
	Всего:	594	414	328	36	168	30	72	144	14

2.2. Тематический план и содержание профессионального модуля

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа студентов, курсовой проект(работа)	Объем в часах
1	2	3
Раздел 1 ПМ.03. Применение технической защиты информации		**230**
МДК.03.01 Техническая защита информации		**194**
Раздел 1. Концепция инженерно-технической защиты информации		**6**
Тема 1.1. Предмет и задачи технической защиты информации	Содержание	2
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	2
	В том числе практических и лабораторных занятий	-
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.	4
	В том числе практических и лабораторных занятий	-
Раздел 2. Теоретические основы инженерно-технической защиты информации		**24**
Тема 2.1. Информация как предмет защиты	Содержание	8
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства, и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	4
	В том числе практических и лабораторных занятий	4

	Практическое занятие «Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке».	4
Тема 2.2. Технические каналы утечки информации	Содержание	8
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	4
	В том числе практических и лабораторных занятий	4
	Практическое занятие «Угрозы информационной безопасности»	4
Тема 2.3. Методы и средства технической разведки	Содержание	8
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	4
	В том числе практических и лабораторных занятий	4
	Практическое занятие «Организация аттестации выделенного помещения по требованиям безопасности информации»	4
Раздел 3. Физические основы технической защиты информации		**32**
Тема 3.1. *Физические поля как носители информации об объектах*.*	Содержание	2
	Общая характеристика технических каналов утечки информации. Принципы классификации физических полей как носителей информации. Понятия о методиках измерения характеристик физических полей..	2
	В том числе практических и лабораторных занятий	-
Тема 3.2. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание	10
	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	6
	В том числе практических и лабораторных занятий	4
	Практическое занятие «Измерение параметров физических полей»	4

Тема 3.3. *Демаскирующие признаки объектов наблюдения и сигналов*.*	Содержание	8
	Основные сигналы и их источники. Опознавательные признаки. Признаки деятельности. Видовые демаскирующие признаки. Классификация сигналов (аналоговые, акустические, речевые, дискретные, электрические, телеграфные, регулярные, магнитные, телекодовые, случайные, электромагнитные, факсимильные, корпускулярные, телевизионные, материально−вещественные, условные). Спектр сигнала.	4
	В том числе практических и лабораторных занятий	4
	Практическое занятие «Изучение спектров сигнала»	4
Тема 3.4. Физические процессы при подавлении опасных сигналов	Содержание	6
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	2
	В том числе практических и лабораторных занятий	4
	Практическое занятие «Расчет эффективности экранирования защитных экранов»	4
Тема 3.5 *Радиоволны и их свойства*.*	Содержание	6
	Принципы радиосвязи. Понятие о радиоканале. Влияние ионосферы и Земли на распространение радиоволн. Распространение и применение электромагнитных волн. Свойства электромагнитных волн (прохождение и поглощение волн, отражение от металлической пластинки, изменение направления на границе диэлектрика (преломление), поперечность электромагнитных волн, интерференция).	4
	В том числе практических и лабораторных занятий	2
	Практическое занятие «Электромагнитные колебания и волны»	2
Раздел 4. Системы защиты от утечки информации		**58**
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	Содержание	8
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	4
	В том числе практических и лабораторных занятий	4
	Практическое занятие «Защита от утечки по акустическому каналу»	4
	Содержание	8

Тема 4.2. Системы защиты от утечки информации по проводному каналу	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	4
	В том числе практических и лабораторных занятий	4
	Практическое занятие «Системы защиты от утечки информации по проводному каналу»	4
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	Содержание	8
	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.	4
	В том числе практических и лабораторных занятий	4
	Практическое занятие «Защита от утечки по виброакустическому каналу»	4
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	Содержание	12
	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.	4
	В том числе практических и лабораторных занятий	8
	Практическое занятие «Определение каналов утечки ПЭМИН»	4
	Практическое занятие «Защита от утечки по цепям электропитания и заземления»	4
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	Содержание	8
	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.	4
	В том числе практических и лабораторных занятий	4
	Практическое занятие «Технические средства защиты информации в телефонных линиях»	4
	Содержание	8

Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	4
	В том числе практических и лабораторных занятий	4
	Практическое занятие «Системы защиты от утечки информации по электросетевому каналу»	4
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	Содержание	6
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	4
	В том числе практических и лабораторных занятий	2
	Практическое занятие «Системы защиты от утечки информации по оптическому каналу»	2
Раздел 5. Применение и эксплуатация технических средств защиты информации		**52**
Тема 5.1. Применение технических средств защиты информации	Содержание	18
	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.	8
	В том числе практических и лабораторных занятий	10
	Практическое занятие «Применение технических средств защиты информации»	10
Тема 5.2. Эксплуатация технических средств защиты информации	Содержание	20
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.	8
	В том числе практических и лабораторных занятий	12
	Практическое занятие «Эксплуатация технических средств защиты информации»	12
	Содержание	6

Тема 5.3. *Лицензирование видов деятельности в области технической защиты информации**	Понятие лицензирования. Структура системы лицензирования в области технической защиты информации. Виды лицензируемой деятельности. Законодательство и нормативная документация в области лицензирования защиты информации. Алгоритм подачи заявления на лицензирование деятельности в области технической защиты информации	2
	В том числе практических и лабораторных занятий	4
	Практическое занятие «Поиск и изучение документация в области лицензирования защиты информации»	4
Тема 5.4. *Аккредитация деятельности в области технической защиты информации**	Содержание	8
	Аккредитация деятельности в области технической защиты информации. Требования к аккредитации. Реестр аккредитованных испытательных лабораторий. Аттестация объекта оценки по требованиям безопасности. Сертификация средств защиты информации. Противодействие иностранным техническим разведкам и экспортный контроль в области технической защиты информации.	4
	В том числе практических и лабораторных занятий	4
	Практическое занятие «Аттестация объекта оценки по требованиям безопасности»	4
Примерная тематика внеаудиторной самостоятельной работы при изучении раздела 1 Знакомство с руководящими документами ФСТЭК России по СВТ, и АС от НСД. показателями защищенности средств ВТ от НСД к информации, классами, и группами защищенности СВТ от НСД. классификацией автоматизированных систем и требованиями группами защищенности АС и требованиями к ним_		10
Промежуточная аттестация в форме экзамена по МДК.03.01		**12**
Учебная практика раздела 1 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.		**36**

– Проведение измерений параметров побочных электромагнитных излучений и наводок. – Проведение аттестации объектов информатизации. – *Осуществление электромагнитного экранирования различными способами.** – *Выбор электромагнитных экранов.** – *Расчет основных параметров экрана.** – *Расчет и инструментальный контроль показателей защиты информации различными средствами измерения при инструментальном контроле.**		
Раздел 2 ПМ.02. Применение инженерно-технических средств физической защиты объектов информатизации		**208**
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**180**
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		**28**
Тема 1.1. Цели и задачи физической защиты объектов информатизации	Содержание	14
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.	6
	В том числе практических и лабораторных занятий	8
	Практическое занятие «Характеристика объекта защиты» Практическое занятие «Анализ нормативно-правовой базы физической защиты». Практическое занятие «Формирование требований к физической защите объекта»	2 2 4
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	Содержание	14
	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.	6
	В том числе практических и лабораторных занятий	8
	Практическое занятие «Изучение инженерных конструкций, применяемых для предотвращения проникновения злоумышленника к источникам информации»	8
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		**64**
	Содержание	14

Тема 2.1 Система 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.	6
	В том числе практических и лабораторных занятий	8
	Практическое занятие «Монтаж датчиков пожарной и охранной сигнализации»	8
Тема 2.2. Система контроля и управления доступом	Содержание	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.	8
	В том числе практических и лабораторных занятий	8
	Практическое занятие «Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя» Практическое занятие «Рассмотрение принципов устройства, работы и применения средств контроля доступа»	4 4
Тема 2.3. Система телевизионного наблюдения	Содержание	12
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	4
	В том числе практических и лабораторных занятий	8
	Практическое занятие «Рассмотрение принципов устройства, работы и применения средств видеонаблюдения».	8
Тема 2.4. Система сбора, обработки, отображения и документирования информации	Содержание	12
	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.	4
	В том числе практических и лабораторных занятий	8

	Практическое занятие «Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации».	8
Тема 2.5 Система воздействия	Содержание	10
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	2
	В том числе практических и лабораторных занятий	8
	Практическое занятие «Исследование технических средств воздействия»	8
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		**42**
Тема 3.1 Применение инженерно-технических средств физической защиты	Содержание	18
	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.	6
	В том числе практических и лабораторных занятий	12
	Практическое занятие «Оценка эффективности защиты информации»	6
	Практическое занятие «Разработка структурной схемы и спецификации оборудования»	6
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	Содержание	16
	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.	2
	В том числе практических и лабораторных занятий	14
	Практическое занятие «Планирование и проектирование внутренних нормативных документов по введению средств защиты информации в эксплуатацию»	6
	Практическое занятие «Изучение принципов диагностики, устранения отказов и восстановления работоспособности технических средств физической защиты»	8
Примерная тематика внеаудиторной самостоятельной работы		4

– Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты. – Размещение периметровых средств обнаружения на местности. – Самостоятельнее изучения порядка допуска субъектов на охраняемые объекты	
Тематика курсовых проектов (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.	**30**
Консультация	**4**
Промежуточная аттестация в форме экзамена по МДК.03.02	**8**
Учебная практика раздела 2 Виды работ: 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.	36
Производственная практика Виды работ 1. *Анализ объектов информатизации предприятий, учреждений и организаций.** 2. *Анализ ресурсов обеспечения инженерно-технической защиты информации.** 3. *Изучение основных этапов проектирования системы защиты информации техническими средствами** 4. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации;	**144**

5. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; 6. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; 7. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. 8. *Оценка эффективности защиты информации**	
Промежуточная аттестация в форме экзамен по модулю	**12**
Всего	**594**

3. Условия реализации рабочей программы профессионального модуля

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:
Лаборатория технических средств защиты информации

3.2. Информационное обеспечение реализации программы

Основные печатные и электронные издания

1.Зайцев, А.П. Технические средства и методы защиты информации: учебник для студентов вузов, обучающихся по группе специальностей - "Информационная безопасность" / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов .- 7-е изд., испр. .- Москва : Горячая линия - Телеком, 2019 - 442 с. + Тираж не указан.- ISBN 978-5-9912-0233-6.

2.Шейдаков, Н. Е. Физические основы защиты информации: учебное пособие / Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. - Москва: РИОР: ИНФРА-М, 2022. - 204 с. -(Высшее образование). - DOI: https://doi.org/10.12737/21158. - ISBN 978-5-369-01603-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/1851140 (дата обращения: 07.06.2022). – Режим доступа: по подписке.

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

4. Информационный портал по безопасности www.SecurityLab.ru.

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

6. Российский биометрический портал www.biometrics.ru

7. Сайт журнала Информационная безопасность http://www.itsec.ru – Сайт Научной электронной библиотеки www.elibrary.ru

8. Справочно-правовая система «Гарант» » www.garant.ru

9. Справочно-правовая система «Консультант Плюс» www.consultant.ru

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

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

12. Федеральный портал «Российское образование www.edu.ru

Дополнительные источники

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. 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.
12. 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.
13. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
14. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных

информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
15. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
16. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
17. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
18. 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.
19. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
20. 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
21. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологи
22. 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
23. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
24. 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
25. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

26. 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
27. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
28. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
29. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
30. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
31. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
32. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
33. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
34. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
35. Номенклатура показателей качества. Ростехрегулирование, 2005.
36. 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.
37. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
38. 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.
39. 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.

40. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
41. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
42. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
43. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
44. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
45. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
46. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
47. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
48. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

4. Контроль и оценка результатов освоения профессионального модуля

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Формы и методы контроля, в том числе по учебной и производственной практике
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 и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен по модулю, экспертное наблюдение экспертное наблюдение выполнения практических занятий, 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 по модулю, экспертное наблюдение экспертное наблюдение выполнения практических занятий, 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 по модулю, экспертное наблюдение экспертное наблюдение выполнения практических занятий, 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 по модулю, экспертное наблюдение экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач,

		оценка процесса и результатов выполнения видов работ на практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экзамен по модулю, экспертное наблюдение экспертное наблюдение выполнения практических занятий, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
Код и наименование профессиональных и общих компетенций, формируемые в амках модуля	Критерии оценки	Формы и методы контроля, в том числе по учебной и производственной практике

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- выбор метода и способа решения профессиональных задач с соблюдением техники безопасности и согласно заданной ситуации; -оценка эффективности и качества выполнения согласно заданной ситуации	Наблюдение, мониторинг, оценка содержания портфолио студента.
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- эффективный поиск необходимой информации; - информация, подобранная из разных источников в соответствии с заданной ситуацией	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 03. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	- решение стандартных и нестандартных профессиональных задач в области эксплуатации компонент подсистем безопасности автоматизированных систем;	Мониторинг и рейтинг выполнения работ на учебной и производственной практике
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- демонстрация собственной деятельности в условиях коллективной и командной работы в соответствии с заданной ситуацией; - демонстрация собственной деятельности в роли руководителя команды в соответствии с заданными условиями.	Подготовка рефератов, докладов, сообщений, использование электронных источников

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- - демонстрация собственной деятельности в условиях коллективной и командной работы в соответствии с заданной ситуацией; - демонстрация собственной деятельности в роли руководителя команды в соответствии с заданными условиями.	Наблюдение за навыками работы в глобальных, корпоративных и локальных информационных сетях.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	- демонстрация интереса к будущей профессии; - демонстрация целеустремленности, самообразования и саморазвития	Наблюдение за ролью обучающегося в группе; портфолио
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- демонстрация качества принятых организационных решений - готовность к частой смене технологий в профессиональной деятельности; - анализ инноваций в области профессиональной деятельности.	Деловые игры - моделирование социальных и профессиональных ситуаций.
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	- оценка собственного продвижения, личностного развития.	Контроль графика выполнения индивидуальной самостоятельной работы обучающегося; открытые защиты творческих и проектных работ

ОК 09. Использовать информационные технологии в профессиональной деятельности.	- использование основных видов современной вычислительной техники; - эксплуатация и устранение типичных выявленных дефектов технических средств информатизации; - демонстрация результативной деятельности в области эксплуатации и технического сопровождения автоматизированных систем	Семинары учебно-практические конференции. Конкурсы профессионального мастерства. Олимпиады.
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- использование основных видов современной вычислительной техники; - эксплуатация и устранение типичных выявленных дефектов технических средств информатизации; - демонстрация результативной деятельности в области эксплуатации и технического сопровождения автоматизированных систем	Семинары учебно-практические конференции. Деловые игры-моделирование профессиональных ситуаций.
ОК.11 Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере	- эффективный поиск и применение знаний финансовой грамотности; - информация, подобранная из разных источников в соответствии с заданной ситуацией	Семинары учебно-практические конференции. Деловые игры-моделирование профессиональных ситуаций