Федеральное государственное образовательное бюджетное

учреждение высшего образования

«Финансовый университет при Правительстве Российской Федерации»

(Финансовый университет)

Колледж информатики и программирования

СОГЛАСОВАНО

Общество с ограниченной ответственностью «Русбитех-Астра»
Директор департамента регионального развития

_____ А.Б. Солдатов

«28» июня 2024 г.

УТВЕРЖДАЮ

Заместитель директора по учебной работе

_____ Н.Ю. Долгова

«10» июня 2024 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Москва 2024 г.

Рабочая программа профессионального модуля разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Разработчики:

Маринич А.Л., преподаватель первой квалификационной категории Колледжа информатики и программирования;

Рабочая программа профессионального модуля рассмотрена и рекомендована к утверждению на заседании предметной (цикловой) комиссии «Обеспечение информационной безопасности автоматизированных систем»

Протокол от «16» мая 2024 г. №10

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 профессиональной деятельности: защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты, соответствующие ему профессиональные и общие компетенции:

1.1.1. Перечень общих компетенций

Код	Наименование видов деятельности и профессиональных 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 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.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.

1.1.1. 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 информационно-телекоммуникационных систем и сетей.

1.1.3. В результате освоения профессионального модуля студент должен:

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

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов: 610 часов, в том числе в форме практической подготовки 610 часов.
Из них на освоение МДК – 346 часа,
в том числе самостоятельная работа -34 часов
Практики, в том числе учебная -108 час.
производственная -144 часа
Экзамен по модулю- 12 часов

2. Структура и содержание профессионального модуля

2.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.			Объем профессионального модуля, час.					
					Обучение по МДК, в час.			Практики		
			В т.ч. в форме практической подготовки	Всего	Промежуточная аттестация	лабораторные работы и практические занятия	курсовая работа (проект	Учебная, часов	Производственная (по профилю специальности), часов	Самостоятельная работа
ПК 3.1-ПК.3.4 ОК 01 ОК 07 ОК 09	Раздел 1. Защита информации в ИТКС с использованием технических средств защиты	228	228	162	18	74		48		18
ПК 3.5 ОК 01 ОК 07 ОК 09	Раздел 2. Физическая защита линий связи ИТКС	226	226	150	18	52		60		16

Производственная практика	144	144						144	
Экзамен по модулю	12	12	12						
Всего:	610	610	324	48	154	-	108	144	34

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные и практические занятия, самостоятельная работа студентов, курсовая проект (работа)	Объем часов
1	2	3
Раздел 1. ПМ.03 Защита информации в ИТКС с использованием технических средств защиты		**228**
МДК.03.01. Защита информации в ИТКС с использованием технических средств защиты		**180**
Тема 1.1. Предмет и задачи технической защиты информации	Содержание	4
	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.	4
	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	-
Тема 1.3. Информация как предмет защиты	Содержание	6
	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	4

	технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	
	В том числе практических и лабораторных занятий	2
	1.Практическое занятие «Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке».	2
Тема 1.4. 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
	1. Практическое занятие «Исследование зон покрытия городских радиостанций» 2. Практическое занятие «Поиск и наложение шумов на передаваемый сигнал»	2 2
Тема 1.5. 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
	1. Практическое занятие «Исследование активности цифровых радиопередающих устройств»	4
Тема 1.6. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание	8
	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	4

	В том числе практических и лабораторных занятий	4
	1. Практическое занятие «Измерение параметров физических полей»	4
Тема 1.7. Физические процессы при подавлении опасных сигналов	Содержание	8
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	4
	В том числе практических и лабораторных занятий	4
	1. Практическое занятие «Исследование влияния нерегулируемых генераторов шума на мобильную связь» 2. Практическое занятие «Исследование влияния регулируемых генераторов шума на мобильную связь»	2 2
Тема 1.8. 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
	1. Практическое занятие «Защита от утечки по акустическому каналу»	4
Тема 1.9. Системы защиты от утечки информации по проводному каналу	Содержание	8
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	4
	В том числе практических и лабораторных занятий	4
	1. Практическое занятие «Исследование влияния нерегулируемых генераторов шума на мобильную связь»	2

	2. Практическое занятие «Исследование влияния регулируемых генераторов шума на мобильную связь»	2
Тема 1.10. 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
	1. Практическое занятие «Защита от утечки по виброакустическому каналу»	4
Тема 1.11. 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
	1. Практическое занятие «Определение каналов утечки ПЭМИН»	4
	2. Практическое занятие «Защита от утечки по цепям электропитания и заземления»	4
Тема 1.12. 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
	1. Практическое занятие «Исследование влияния помех на мобильную связь»	2

	2. Практическое занятие «Исследование возможностей исследовательского прибора «OSCORGreen» при обнаружении радиостанций»	2
Тема 1.13. Системы защиты от утечки информации по электросетевому каналу	Содержание	10
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	6
	В том числе практических и лабораторных занятий	4
	1. Практическое занятие «Техническая сборка схемы проверки излучения исследуемого устройства» 2. Практическое занятие «Программная настройка схемы проверки излучения исследуемого устройства»	2 2
Тема 1.14. 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
	1. Практическое занятие «Анализ проводных линий связи малого тока»	2
Тема 1.15. 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
	1. Практическое занятие «Оптический поиск закладных устройств» 2. Практическое занятие «Поиск устройств несанкционированного доступа с минимальной мощностью» 3. Практическое занятие «Анализ радиоволнового спектра помещения»	2 2 2

	4. Практическое занятие «Исследование СВЧ диапазона спектра»	4
Тема 1.16. 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.	4
	В том числе практических и лабораторных занятий	16
	1. Практическое занятие «Анализ проводных линий среднего тока» 2. Практическое занятие «Анализ инфракрасного спектра помещений»	8 8
Примерная тематика внеаудиторной самостоятельной работы при изучении раздела 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.		**18**
Промежуточная аттестация в форме экзамена по МДК.03.01		**18**
Учебная практика Раздела 1 Виды работ Реализация защиты от утечки по цепям электропитания и заземления. Монтаж различных типов датчиков. Разработка организационных и технических мероприятий по заданию преподавателя;		**48**

Разработка основной документации по инженерно-технической защите информации.		
Раздел 2. ПМ 03 Физическая защита линий связи ИТКС		**226**
МДК.03.02. Физическая защита линий связи ИТКС		**166**
Тема 1.1. Цели и задачи физической защиты объектов информатизации	Содержание	8
	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.	4
	В том числе практических и лабораторных занятий	4
	1.Практическое занятие «Исследование возможностей СЗИ «Страж NT» 2. Практическое занятие «Исследование программной среды «Страж NT»	2 2
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	Содержание	18
	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	12
	1. Практическое занятие «Управление пользователями «Страж NT», учет пользователей «Страж NT» 2. Практическое занятие «Избирательное управление «Страж NT» 3. Практическое занятие «Сортировка и поиск с «Страж NT» 4. Практическое занятие «Редактирование пользователей «Страж NT» 5. Практическое занятие «Изменение настроек «Страж NT	 2 2 2 2 4
	Содержание	14

Тема 1.3. 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
	1. Практическое занятие «Монтаж датчиков пожарной и охранной сигнализации»	8
Тема 1.4. Система контроля и управления доступом	Содержание	12
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	6
	В том числе практических и лабораторных занятий	6
	1. Практическое занятие «Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя»	4
	2. Практическое занятие «Рассмотрение принципов устройства, работы и применения средств контроля доступа»	2
Тема 1.5. Система телевизионного наблюдения	Содержание	10
	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	6
	1. Практическое занятие «Рассмотрение принципов устройства, работы и применения средств видеонаблюдения».	6
	Содержание	8

Тема 1.6. Система сбора, обработки, отображения и документирования информации	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.	6
	В том числе практических и лабораторных занятий	2
	1. Практическое занятие «Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации».	2
Тема 1.7. Система воздействия	Содержание	10
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	4
	В том числе практических и лабораторных занятий	6
	1. Практическое занятие «Исследование возможностей радиолокатора NR-900EMS» 2. Практическое занятие «Исследование возможностей прибора ST 033P Пиранья» 3. Практическое занятие «Исследование возможностей анализатора спектра OSCOR Green»	2 2 2
Тема 1.8. Применение инженерно-технических средств физической защиты	Содержание	22
	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.	8
	В том числе практических и лабораторных занятий	14
	1. Практическое занятие «Исследование возможностей имитатора АВРОРА-3» 2. Практическое занятие «Исследование возможностей комплекса КРОНА-ПРО» 3. Практическое занятие «Исследование возможностей приемника СКОРПИОН-XL» 4. Практическое занятие «Исследование принципов работы индикатора поля РИЧ-8» 5. Практическое занятие «Исследование принципов работы индикатора поля MFP-8000» 6. Практическое занятие «Исследование принципов работы индикатора поля ST-107» 7. Практическое занятие «Исследование принципов работы индикатора поля PST-165»	2 2 2 2 2 2 2

Тема 1.9. Эксплуатация инженерно-технических средств физической защиты	Содержание	30
	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.	8
	В том числе практических и лабораторных занятий	22
	1. Практическое занятие «Исследование возможностей системы ТАЛИС-НЧ-ЛАЙТ» 2. Практическое занятие «Исследование возможностей системы ЛАЗУРИТ» 3. Практическое занятие «Исследование возможностей системы ШЕПОТ» 4. Практическое занятие *«Настройка работы удостоверяющего центра в аккредитованном режиме»**	4 4 4 10
Примерная тематика внеаудиторной самостоятельной работы при изучении раздела 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.		**16**
Промежуточная аттестация в форме экзамена МДК.03.02		**18**
Учебная практика Виды работ 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. Разработка организационных и технических мероприятий по заданию преподавателя; Разработка основной документации по инженерно-технической защите информации.		60
Производственная практика Виды работ		

Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам; Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	**144**
Промежуточная аттестация экзамен по модулю	**12**
Всего по ПМ	**610**

3. Условия реализации рабочей программы профессионального модуля

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

Лаборатория Защиты информации от утечки по техническим каналам

Оборудование:

-посадочные места по количеству обучающихся;
-рабочее место преподавателя;
-доска меловая;
-место хранения раздаточного и дидактического материала;
-наглядные пособия (комплекты учебных таблиц, плакатов и др.);
-дидактические материалы (раздаточные материалы, ФОС и др.).

Технические средства обучения:

-персональный компьютер с лицензионным программным обеспечением, подключенный к локальной сети и выходом в интернет;
-персональный компьютер обучающегося с лицензионным программным обеспечением, подключенный к локальной сети и выходом в интернет (по количеству обучающихся);
проектор с экраном;
-средствами защиты информации от утечки по акустическому (виброакустическому) каналу;
-средствами защиты информации от утечки по каналам, формируемым за счет побочных электромагнитных излучений и наводок;
-средствами контроля эффективности защиты информации от утечки по акустическому (виброакустическому) каналу и каналам побочных электромагнитных излучений и наводок;-шумогенераторы;
-комплексный поисковый прибор;
-прожигатели телефонных линий;
-устройство обнаружения скрытых видеокамер;
-виброакустические генераторы;
-подавители диктофонов;
-подавители устройств сотовой связи;
-устройство защиты аналоговых сигналов;
-устройство защиты цифровых сигналов.
Стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения, охранно-пожарной сигнализации и охраны объектов
комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

Помещение для самостоятельной работы

(Библиотека, читальный зал с выходом в сеть интернет)

-автоматизированные рабочие места обучающихся с выходом в Интернет и доступом в электронную информационно-образовательную среду образовательной организации (процессор Core i5, оперативная память объемом 16 Гб).

3.2. Информационное обеспечение реализации программы

Основные печатные и электронные издания

1.Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2019.

2.Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2019.

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

3.2.2. Электронные издания (электронные ресурсы)

Интернет-ресурсы:

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

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

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

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

http://www.morion.ru/

http://www.nateks.ru/

http://www.iskratel.com/

http://www.ps-ufa.ru/

http://3m.com/

http://www.rusgates.ru/index/php - Материалы сайта завода «Ферроприбор»

3.2.3. Дополнительные источники

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

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

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

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

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

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

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

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

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

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

Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

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

Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

4. Контроль и оценка результатов освоения профессионального модуля

Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в ИТКС.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	тестирование, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике, экзамен, экзамен по модулю
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в ИТКС.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в	экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения
ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями.	- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; - проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике, экзамен, экзамен

ПК 3.4. Проводить отдельные работы по физической защите линий связи ИТКС.	выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты	экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным	обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение Экзамен
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами,	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	Экспертное наблюдение Экзамен
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение Экзамен

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Экспертное наблюдение Экзамен