



МИНОБРНАУКИ РОССИИ

Старооскольский геологоразведочный институт

(филиал) Федерального государственного бюджетного образовательного учреждения  
высшего образования

«Российский государственный геологоразведочный университет  
имени Серго Орджоникидзе»  
(СГИ МГРИ)



УТВЕРЖДАЮ:

Директор СГИ МГРИ

И. Двоглазов

2024 г.

СОГЛАСОВАНО

Заместитель директора по СПО

Е. А. Мищенко

«06» 03 2024 г.

## РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

### ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

г. Старый Оскол  
2024 г.

Рабочая программа профессионального модуля. ПМ 03. Защита информации техническими средствами разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного Приказом Минпросвещения России от 9 декабря 2016 года № 1553.

Организация-разработчик: Старооскольский геологоразведочный институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный геологоразведочный университет имени Серго Орджоникидзе»

Разработчик:

преподаватель СГИ МГРИ

РАССМОТРЕНА И ОДОБРЕНА

Протокол № 2 от «28» февраля 2024 г.

На заседании учебно-методического отдела СГИ МГРИ

## СОДЕРЖАНИЕ

	Стр.
1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2. СТРУКТУРА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	7
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	18
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	21

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

## 1.1. Область применения программы

Рабочая программа профессионального модуля является частью основной образовательной программы в соответствии с ФГОС СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем входящей в состав укрупнённой группы 10.00.00 Информационная безопасность в части освоения основного вида профессиональной деятельности (ВПД): Защита информации техническими средствами.

## 1.2. Место дисциплины в структуре образовательной программы

Рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами, входит в профессиональный учебный цикл.

Особое значение профессиональный модуль имеет при формировании и развитии общих компетенций (ОК 01-10), профессиональных компетенций (ПК 3.1-3.5

Планируемые результаты освоения профессионального модуля

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

### 1.3.1. Перечень общих компетенций

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

### 1.3.2. Перечень профессиональных компетенций

<i>Код</i>	<i>Наименование видов деятельности и профессиональных компетенций</i>
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 (ПЭМИН), 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.

1.3.4. В результате освоения профессионального модуля обучающийся должен:

<b>Иметь практический опыт</b>	<ul style="list-style-type: none"> <li>– установки, монтажа и настройки технических средств защиты информации;</li> <li>– технического обслуживания технических средств защиты информации;</li> <li>– применения основных типов технических средств защиты информации;</li> <li>– выявления технических каналов утечки информации;</li> <li>– участия в мониторинге эффективности технических средств защиты информации;</li> <li>– диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;</li> <li>– 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;</li> </ul>
	<ul style="list-style-type: none"> <li>– проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;</li> <li>– установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.</li> </ul>
<b>Уметь</b>	<ul style="list-style-type: none"> <li>– применять технические средства для криптографической защиты информации конфиденциального характера;</li> <li>– применять технические средства для уничтожения информации и носителей информации;</li> <li>– 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;</li> </ul>

	<ul style="list-style-type: none"> <li>– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;</li> <li>– применять инженерно-технические средства физической защиты объектов информатизации</li> </ul>
<b>Знать</b>	<ul style="list-style-type: none"> <li>– порядок технического обслуживания технических средств защиты информации;</li> <li>– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;</li> <li>– 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;</li> <li>– порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;</li> <li>– методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;</li> <li>– 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;</li> <li>– основные способы физической защиты объектов информатизации; – номенклатуру применяемых средств физической защиты объектов информатизации.</li> </ul>

### **1.3. Количество часов, отводимое на освоение профессионального модуля**

Объем часов: 784 ч., в том числе в форме практической

подготовки 656 ч. из них

на освоение: - МДК 292 ч.;

практики:

- учебная практика 108 ч.;

- производственная практика 360 ч.;

промежуточная аттестация, в форме экзамена по модулю – 18 ч.

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Коды профессиональных общих компетенций и личностных результатов, формированию которых способствует элемент программы	Объем профессионального модуля, ак. час.									
	Наименования разделов профессионального модуля	Всего, час.	В том ч. Форме практической подготовки	Обучение по МДК					Практики	
				В том числе					Учебная	Производственная
				Всего	Лабораторных, и практических, занятий	Курсовых работ (проектов)	Самостоятельная работа	Промежуточная аттестация		
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>	<b>11</b>
ПК 3.1- ПК.3.4 ОК 1 – ОК10	МДК.03.01 Техническая защита информации	112	78	112	78					
ПК 3.5 ОК 01 –ОК10	МДК.03.02 Инженернотехнические средства физической защиты объектов информатизации	90	60	90	30	30		дз		
ПК 3.1- ПК.3.4 ОК 1 – ОК10	МДК.03.03 Техническое обслуживание информационно-коммуникационных систем и сетей	90	50	90	50			дз		
	Учебная практика, часов	108	108						108	
	Производственная практика, часов	360	360							360
	Промежуточная аттестация	18								
	<i>Всего:</i>	784	656	292	158	30		18		360

## 2.2. Тематический план и содержание учебного материала профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, акад. ч / в том числе в форме практической подготовки, ак. ч
1	2	3
<b>МДК.03.01</b> Техническая защита информации		112
<b>Раздел 1.</b> Характеристика технических каналов утечки информации		32
<b>Тема 1.1.</b> Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.	<b>Содержание учебного материала</b>	4
основы утечки информации по	1. Физические основы побочных электромагнитных излучений и наводок. Акустозлектрометрические преобразования.	2
каналам побочных электромагнитных	Средства обнаружения каналов утечки информации	2
излучений и наводок.	<b>В том числе лабораторных и практических занятий</b>	28
	Практическое занятие №1. Измерение параметров физических полей	2
	Практическое занятие №2. Акустозлектрометрические преобразования	2
	Практическое занятие №3. Паразитная генерация радиоэлектронных средств	2
	Практическое занятие №4. Виды паразитных связей и наводок	2
	Практическое занятие №5. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.	2
	Практическое занятие №6. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических	2
	Практическое занятие №7. Индикаторы электромагнитных излучений	2
	Практическое занятие №8. Радиочастотометры.	2
	Практическое занятие №9. Сканирующие приемники, селективные вольтметры, анализаторы спектра	2

	Практическое занятие №10. Автоматизированные поисковые комплексы	2
	Практическое занятие №11. Оценка защищенности речевой информации на базе аппаратно-программного комплекса «VNC-012GL».	2
	Практическое занятие №12. Локация полупроводниковых приборов	2
	Практическое занятие №13. Радиомониторинг несанкционированных излучений на базе многоканального комплекса радиоконтроля «Квадрат».	2
	Практическое занятие №14. Видеонаблюдение	2
	<b>Раздел 2. Применение и эксплуатация технических средств защиты информации</b>	<b>80</b>
	<b>Тема 2.1.</b>	<b>12</b>
Применение технических средств защиты информации	<b>Содержание учебного материала</b>	
	. Особенности информации, как предмета защиты. Понятие об опасном сигнале.	2
	Классификация физических полей и технических каналов утечки информации.	2
	Технические средства для уничтожения информации и носителей информации, порядок применения.	2
	Характеристика каналов утечки информации.	2
	Методы и средства защиты информации.	2
	Мероприятия по выявлению каналов утечки информации	2
	<b>В том числе лабораторных и практических занятий</b>	<b>30</b>
	Практическое занятие №15. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных	2
	Практическое занятие №16. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.	2
	Практическое занятие №17. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	2
	Практическое занятие №18. Организация защиты речевой информации.	2
	Практическое занятие №19. Пассивные средства защиты выделенных помещений.	2
	Практическое занятие №20. Аппаратура и способы активной защиты помещений от утечки речевой информации.	2
	Практическое занятие №21. Рекомендации по выбору систем виброакустической защиты.	2
	Практическое занятие №22. Подавление диктофонов.	2

	Практическое занятие №23. Нейтрализация радиомикрофонов	2
	Практическое занятие №24. Защита электросети.	2
	Практическое занятие №25. Защита оконечного оборудования слабочастотных линий	2
	Практическое занятие №26. Защита абонентского участка телефонных линий.	2
	Практическое занятие №27. Организация защиты информации от утечки возникающей при работе вычислительной техники за счет ПЭМИН	2
	Практическое занятие №28. Порядок проведения специальной проверки технических средств	2
	Практическое занятие №29. Контроль эффективности инженерно-технической защиты информации.	2
	<b>Содержание учебного материала</b>	<b>18</b>
<b>Тема 2.2 Методы и средства технической разведки и системы защиты информации</b>	9. Классификация технических средств разведки. Методы и средства.	2
	10. Средства и возможности оптической разведки. Средства дистанционного съема информации.	2
	11. Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования.	2
	12. Скрывание речевой информации в каналах связи. Экранирование. Зашумление.	2
	13. Системы защиты по акустическому каналу.	2
	14. Номенклатура применяемых средств от несанкционированной утечки информации по проводному каналу.	2
	15. Несанкционированная утечка информации по вибрационному каналу.	2
	16. Электронные стетоскопы. Лазерные системы прослушивания.	2
	17. Утечка информации по сотовым каналам связи.	2
	<b>Практические занятия</b>	<b>20</b>
	Практическое занятие №30. Измерение параметров физических полей	2
	Практическое занятие №31. Подавление опасных сигналов акустоэлектрических преобразований.	2
	Практическое занятие №32. Средства и возможности оптической разведки	2
	Практическое занятие №33. Защита от утечки по акустическому каналу	2
	Практическое занятие №34. Негласная запись информации на диктофоны. Системы защиты от диктофонов	2
	Практическое занятие №35. Защита от утечки по виброакустическому каналу	2
	Практическое занятие №36. Определение каналов утечки ПЭМИН	2
Практическое занятие №37. Защита от утечки по цепям электропитания и заземления	2	

	Практическое занятие №38. Системы защиты информации по электромагнитному каналу.	2
	Практическое занятие №39. Дифференцированный зачет	2
<b>МДК.03.02</b>	Инженерно-технические средства физической защиты объектов информатизации	
Тема 1.1. Цели и задачи физической защиты объектов информатизации	<p><b>Содержание учебного материала</b></p> <p>Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации.</p> <p>Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.</p> <p><b>В том числе лабораторных и практических занятий</b></p> <p><b>Практическое занятие № 1.</b> Анализ основных нормативно-правовых актов, регламентирующих потенциально опасные объекты</p> <p><b>Практическое занятие № 2.</b> Анализ основных нормативно-правовых актов, регламентирующих инженернотехническую защиту информации потенциально опасных объектов</p>	90 2
Тема 1.2. Общие сведения о комплексах инженернотехнических средств физической защиты	<p><b>Содержание учебного материала</b></p> <p>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.</p> <p><b>В том числе лабораторных и практических занятий</b></p> <p><b>Практическое занятие № 3.</b> Анализ нормативно-правовой базы физической защиты информации.</p> <p><b>Практическое занятие № 4.</b> Характеристика объекта защиты</p>	2
Тема 2.1 Система обнаружения комплекса инженернотехнических средств физической защиты	<p><b>Содержание учебного материала</b></p> <p>Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта.</p> <p>Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.</p> <p><b>В том числе лабораторных и практических занятий</b></p> <p><b>Практическое занятие № 5.</b> Монтаж датчиков пожарной и охранной сигнализации</p>	8 2 2

<p>Тема 2.2. Система контроля и управления доступом</p>	<p><b>Содержание учебного материала</b></p> <p>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.</p> <p>Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД.</p> <p>Обнаружение металлических предметов и радиоактивных веществ.</p> <p><b>В том числе лабораторных и практических занятий</b></p> <p><b>Практическое занятие № 6.</b> Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя</p> <p><b>Практическое занятие № 7.</b> Рассмотрение принципов устройства, работы и применения средств контроля доступа</p>	<p>2</p> <p>2</p> <p>2</p> <p>6</p>
<p>Тема 2.3. Система телевизионного наблюдения</p>	<p><b>Содержание учебного материала</b></p> <p>9. Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения.</p> <p>10. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.</p> <p><b>В том числе лабораторных и практических занятий</b></p> <p><b>Практическое занятие № 8.</b> Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.</p>	<p>2</p> <p>2</p> <p>6</p>
<p>Тема 2.4. Система сбора, обработки, отображения и документирования информации</p>	<p><b>Содержание учебного материала</b></p> <p>11. Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации.</p> <p>Устройства отображения и документирования информации.</p> <p><b>В том числе лабораторных и практических занятий</b></p> <p><b>Практическое занятие № 9.</b> Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.</p> <p><b>Содержание учебного материала</b></p>	<p>2</p> <p>4</p>

<b>Тема 2.5</b> Система воздействий	12. Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	1
	<b>В том числе лабораторных и практических занятий</b>	
<b>Курсовое проектирование</b>	<b>Практическое занятие № 10.</b> Основные показатели технических средств воздействия.	3
	<b>Содержание учебного материала</b>	<b>20</b>
	1. Составление плана курсовой работы	2
	2. Выявление объекта и предмета курсовой работы, цели и задач курсовой работы.	2
	3. Выявление характеристики структуры курсовой работы. Выявление обоснования актуальности темы	2
	4. Подбор нормативных источников по разделу курсовой работы. Подбор методических источников по разделу курсовой работы.	2
	5. Подбор материала для первого раздела курсовой работы	2
	6. Логичное распределение и систематизация материала внутри раздела курсовой работы	2
	7. Подбор материала для второго раздела курсовой работы	2
	8. Логичное распределение и систематизация материала внутри раздела курсовой работы	2
	9. Проверка оформления курсовой работы. Проверка оформления списка используемых источников и приложения	2
10. Оформление презентации к защите курсовой работы. Подготовка речи к защите курсовой работы	2	
Проведение презентации курсовой работы	2	
Дифференцированный зачет		
<b>МДК.03.03</b> Техническое обслуживание информационно-коммуникационных систем и сетей		90
<b>Введение в МДК</b>	<b>Содержание учебного материала</b>	
<b>Тема 1.1</b> Принципы и задачи ИКС	1. Введение в техническое обслуживание информационно-коммуникационных систем и сетей	2
	<b>Содержание учебного материала</b>	
	2. Основы технического обслуживания ИКС и сетей	2
	3. Методология определения проблем с ПК и серверами	2
	4. Администрирование информационных систем	2
	5. Технологии локальной вычислительной сети	2
<b>В том числе лабораторных и практических занятий</b>		
<b>Практическое занятие №1.</b> Обжим кабеля 8P8C		2

<b>Тема 1.2</b> Технологии передачи и обработки и сохранности данных	<b>Практическое занятие №2.</b> Подключение устройств с помощью витой пары	2
	<b>Практическое занятие №3.</b> Исследование протоколов сетевого взаимодействия устройств	2
	<b>Практическое занятие №4.</b> Работа с программным обеспечением “GNS3”	2
	<b>Практическое занятие №5.</b> Создание модели ИКС	2
	<b>Практическое занятие №6.</b> Диагностика функционирования узлов ПК	2
	<b>Практическое занятие №7.</b> Организация удаленного доступа к ПК по сети	2
	<b>Содержание учебного материала</b>	
	6. VPN-сети. Методы реализации VPN-сетей	2
	7. Архитектура и стандарты IEEE 802.11	2
	8. Технологии безопасности, протоколы авторизации, конфиденциальность и безопасность при работе в Web.	2
	<b>В том числе лабораторных и практических занятий</b>	
	<b>Практическое занятие №8.</b> Автоматическая настройка локальной сети.	2
	<b>Практическое занятие №9.</b> Знакомство с локальными политиками безопасности.	2
	<b>Практическое занятие №10.</b> Настройка виртуальной сети Интернет	2
	<b>Практическое занятие №11.</b> Установка и настройка операционной системы сервера и рабочих станций как Windows Server	2
	<b>Практическое занятие №12.</b> Настройка DNS и DHCP	2
<b>Тема 1.3</b> Разработка ЛВС	<b>Содержание учебного материала</b>	
	9. Проектирование сетевой инфраструктуры	2
	10. Общий доступ через протокол SMB	2
	11. Создание кластерной архитектуры	2
	12. Взаимодействие сетевых устройств	2
	13. Модель OSI	2
	14. Сетевая инкапсуляция и деинкапсуляция данных	2
	15. Протокол OSPF (динамической маршрутизации)	2
	16. Восстановление ИКС после сбоя	2
	<b>В том числе лабораторных и практических занятий</b>	
<b>Практическое занятие №13</b> Настройка коммутационного оборудования.	2	
<b>Практическое занятие №14</b> Мониторинг функционирования сети	2	

	Практическое занятие №15 Организация общего доступа к ресурсам сети	2
	Практическое занятие №16 Передача файлов с помощью технологии ЛВС	2
	Практическое занятие №17 Настройка и установка общих пользователей ИКС	2
	Практическое занятие №18 Работа с Active Directory	2
	Практическое занятие №19 Анализ основных сетевых протоколов и их предназначение	2
	Практическое занятие №20. Проведение мониторинга пакетов сети	2
	Практическое занятие №21. Эксплуатация средств защиты информации для обеспечения безопасности ИКС	2
	Практическое занятие №22. Создание таблицы маршрутизации сети	2
	<b>Содержание учебного материала</b>	
<b>Тема 1.4</b> Защита информации в ИКС	17. Работа средств защиты информации в ИКС	2
	18. Реализация ИКС на предприятии	2
	19. Задачи “толстого” и “тонкого” клиента	2
	<b>В том числе лабораторных и практических занятий</b>	
	Практическое занятие №23 Резервное копирование настроек	2
	Практическое занятие №24 Применение виртуализации для создания сети предприятия	2
	Практическое занятие №25 Работа с “толстым” и “тонким” клиентом	2
	<b>Дифференцированный зачет</b>	2
		108
<b>Учебная практика</b>		
<b>Виды работ:</b>	<ul style="list-style-type: none"> <li>- Измерение параметров физических полей.</li> <li>- Определение каналов утечки ПЭМИН.</li> <li>- Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.</li> <li>- Установка и настройка технических средств защиты информации.</li> <li>- Проведение измерений параметров побочных электромагнитных излучений и наводок.</li> <li>- Проведение аттестации объектов информатизации.</li> <li>- Анализ методов проведения атак голосового преобразования в биометрических системах верификации дикторов</li> <li>- Акустические датчики и применение пьезодатчиков в задачах информационной безопасности</li> </ul>	

<ul style="list-style-type: none"> <li>- Модели комплексной защиты информации с учетом особенностей коммерческой организации</li> <li>- Выявление голосовых подделок в биометрических системах на основе CQCC и SCMC коэффициентов</li> <li>- Использование сетей Петри в математическом моделировании</li> <li>- Теория телеграфика</li> <li>- Идентификация частотно-временных особенностей сетевого трафика при создании множественных запросов на соединение</li> <li>- Протокол маршрутизации между автономными системами BGP</li> <li>- Методика обнаружения скремблированных радиосигналов средств негласного контроля</li> <li>- Принципы защиты этапа загрузки операционной системы</li> </ul> <p><b>Производственная практика</b></p> <p><b>Виды работ:</b></p> <ul style="list-style-type: none"> <li>- Оценка защищенности речевой информации на основе анализа многомерных данных</li> <li>- Усовершенствование комплекса виброакустической оценки защиты речевой информации "VNK -012GL"</li> <li>- Влияние шумоочистки на результат оценки акустической защищенности</li> <li>- Разработка модели угроз утечки информации по техническим каналам</li> <li>- Несанкционированный доступ к ЭВМ. Аспекты безопасность UEFI.</li> <li>- Анализ угроз, уязвимостей компьютерных сетей и средств защиты</li> <li>- Системы обнаружения вторжений</li> <li>- Встраивание идентификационной метки в аудиосигнал с использованием эффекта маскировки в спектре</li> <li>- Применение дискретного вейвлет-преобразования для выявления редактированных участков звуковых сигналов</li> <li>- Метод многомерного анализа данных в селективных поисковых системах</li> <li>- Применение методов многомерного анализа данных при обработке полиграмм для выявления возможного инсайдера</li> <li>- Селективный металлодетектор на микроконтроллере</li> <li>- Методика обработки сигналов металлодетекторов</li> <li>- Разработка программно-аппаратного комплекса для двухфакторной аутентификации</li> </ul>	360
Объем часов по ПМ.03	784
Из них: теория	104
Практические занятия	188

Учебная практика	108
Производственная практика	360
Промежуточная аттестация – экзамен по ПМ	18

### 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

#### 3.1. Материально-техническое обеспечение

Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

лаборатория «Технических средств защиты информации», оснащенная:

Лаборатория технических средств информатизации. Рабочее место преподавателя, рабочие места по количеству обучающихся, компьютеры с лицензионным программным обеспечением, мультимедийное оборудование, интерактивная панель, комплект учебно-наглядных пособий, презентации, комплект видеофильмов.

Кабинет самостоятельной и воспитательной работы. Рабочее место преподавателя, рабочие места по количеству обучающихся, мультимедийное оборудование, комплект учебно-наглядных пособий, презентации, комплект видеофильмов, компьютер с лицензионным программным обеспечением, с возможностью подключения к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СГИ МГРИ: <http://stud.sofmgri.ru:8081/>

#### Учебно-методическое и информационное обеспечение дисциплины

##### а) нормативные акты:

№ п/п	Источник
1.	Федеральный закон от 27 июля 2006 г. № 149-ФЗ .Об информации, информационных технологиях и о защите информации от 27 июля 2006 - docs.cntd.ru <a href="https://docs.cntd.ru/document/901990051">https://docs.cntd.ru/document/901990051</a>
2.	2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ О персональных данных от 27 июля 2006 - docs.cntd.ru <a href="https://docs.cntd.ru/document/901990046">https://docs.cntd.ru/document/901990046</a>
3.	ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий (с Поправкой) - docs.cntd.ru <a href="https://docs.cntd.ru/document/1200048398">https://docs.cntd.ru/document/1200048398</a>
4.	ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий - docs.cntd.ru <a href="https://docs.cntd.ru/document/1200051499">https://docs.cntd.ru/document/1200051499</a>
5.	ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер - docs.cntd.ru <a href="https://docs.cntd.ru/document/1200051500">https://docs.cntd.ru/document/1200051500</a>
6.	ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети - docs.cntd.ru <a href="https://docs.cntd.ru/document/1200048416">https://docs.cntd.ru/document/1200048416</a>

7.	ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология (ИТ). Практические правила управления информационной безопасностью - docs.cntd.ru <a href="https://docs.cntd.ru/document/1200044724">https://docs.cntd.ru/document/1200044724</a>
8.	ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель - docs.cntd.ru <a href="https://docs.cntd.ru/document/1200071694">https://docs.cntd.ru/document/1200071694</a>
9.	ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности - docs.cntd.ru <a href="https://docs.cntd.ru/document/1200069465">https://docs.cntd.ru/document/1200069465</a>
10.	ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности - docs.cntd.ru <a href="https://docs.cntd.ru/document/1200069464">https://docs.cntd.ru/document/1200069464</a>
11.	ГОСТ Р 34.10-2001 Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи - docs.cntd.ru <a href="https://docs.cntd.ru/document/1200026578">https://docs.cntd.ru/document/1200026578</a>
12.	ГОСТ Р 34.11-94 Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования (принят в качестве межгосударственного стандарта ГОСТ 34.311-95) - docs.cntd.ru <a href="https://docs.cntd.ru/document/1200004857">https://docs.cntd.ru/document/1200004857</a>

б) основная литература:

№ п/п	Источник
1.	Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://www.urait.ru/bcode/518005">https://www.urait.ru/bcode/518005</a> (
2.	Богатырев, В. А. Надежность информационных систем : учебное пособие для среднего профессионального образования / В. А. Богатырев. — Москва : Издательство Юрайт, 2023. — 318 с. — (Профессиональное образование). — ISBN 978-5-534-15205-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://urait.ru/bcode/520442">https://urait.ru/bcode/520442</a>
3.	Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/130184">https://e.lanbook.com/book/130184</a>
4.	Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для СПО / В. И. Петренко, И. В. Мандрица. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 108 с. — ISBN 978-5-8114-9038-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/183744">https://e.lanbook.com/book/183744</a>
5.	Тенгайкин, Е. А. Эксплуатация объектов сетевого администрирования. Безопасность функционирования информационных систем. Лабораторные работы : учебное пособие для СПО / Е. А. Тенгайкин. — Санкт-Петербург : Лань, 2022. — 80 с. — ISBN 978-5-8114-8692-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/197546">https://e.lanbook.com/book/197546</a>

6.	Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 464 с. — (Профессиональное образование). — ISBN 978-5-534-17310-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://urait.ru/bcode/532849">https://urait.ru/bcode/532849</a> .
----	--

в) дополнительная литература:

№ п/п	Источник
1.	Гвоздева, Т. В. Проектирование информационных систем. Стандартизация : учебное пособие для вузов / Т. В. Гвоздева, Б. А. Баллод. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 252 с. — ISBN 978-5-8114-7963-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/169810">https://e.lanbook.com/book/169810</a>
2.	Зараменских, Е. П. Информационные системы: управление жизненным циклом : учебник и практикум для среднего профессионального образования / Е. П. Зараменских. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 497 с. — (Профессиональное образование). — ISBN 978-5-534-16179-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://www.urait.ru/bcode/530571">https://www.urait.ru/bcode/530571</a>
3.	Гниденко, И. Г. Технология разработки программного обеспечения : учебное пособие для среднего профессионального образования / И. Г. Гниденко, Ф. Ф. Павлов, Д. Ю. Федоров. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 248 с. — (Профессиональное образование). — ISBN 978-5-534-18131-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <a href="https://www.urait.ru/bcode/534337">https://www.urait.ru/bcode/534337</a>

г) периодические издания:

№ п/п	Источник
1.	Вопросы кибербезопасности : научный журнал / учредитель : Научно-производственное объединение Эшелон. — Москва : Научный центр правовой информации 2013 — . — выходит 6 раз в год . — ISBN печатной версии 2311-3456. — Текст : электронный // ЭБС elibrary [сайт]. — URL : <a href="https://www.elibrary.ru/title_about_new.asp?id=50036">https://www.elibrary.ru/title_about_new.asp?id=50036</a> .
2. 1	Безопасность информационных технология : научный журнал / учредитель : Национальный исследовательский ядерный университет МИФИ . — Москва : Национальный исследовательский ядерный университет МИФИ 1994 — . — выходит 4 раза в год . — ISBN печатной версии 2074-7128. — Текст : электронный // ЭБС elibrary [сайт]. — URL : <a href="https://www.elibrary.ru/title_about_new.asp?id=8429">https://www.elibrary.ru/title_about_new.asp?id=8429</a>
3.	Программные продукты и системы : научный журнал / учредитель : Куприянов В. П.; Акционерное общество "Научно-исследовательский институт "Центрпрограммсистем". — Тверь : 1988 — . — Выходит 4 раза в год. — ISBN печатной версии 0236-235X. — Текст : электронный // ЭБС elibrary [сайт]. — URL: <a href="https://www.elibrary.ru/title_about_new.asp?id=9834">https://www.elibrary.ru/title_about_new.asp?id=9834</a>
4.	Естественные и технические науки: науч. журнал /гл. ред. А.Я.Хавкин. — Москва : ООО "Издательство "Спутник+", 2002— . — Выходит 12 раз в год. ISBN печатной версии 1684 – 2626. — Текст : непосредственный.

## 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в процессе проведения лабораторных, практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий.

Итоговой формой контроля является: экзамен по профессиональному модулю

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки результатов обучения
<p>ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации ПК 3.2.</p> <p>Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации ПК 3.3.</p> <p>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.</p> <p>Организовывать отдельные работы по физической защите объектов информатизации</p> <p>ОК.01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам</p> <p>ОК.02 Осуществлять поиск, анализ и интерпретацию</p>	<ul style="list-style-type: none"> <li>– установка, монтажа и настройка технических средств защиты информации;</li> <li>– технического обслуживания технических средств защиты информации;</li> <li>– применения основных типов технических средств защиты информации;</li> <li>– выявления технических каналов утечки информации;</li> <li>– участия в мониторинге эффективности технических средств защиты информации;</li> <li>– диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;</li> <li>– 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;</li> <li>– проведения</li> </ul>	<p>тестирование, экзамен квалификационный, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>

<p>информации, необходимой для выполнения задач профессиональной деятельности</p> <p>ОК.03 Планировать и реализовывать собственное профессиональное и личностное развитие.</p> <p>ОК.04 Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.</p> <p>ОК.05 Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.</p> <p>ОК.06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения</p> <p>ОК.07 Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.</p> <p>ОК.08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности</p> <p>ОК.09 Использовать информационные технологии в профессиональной деятельности</p> <p>ОК.10 Пользоваться профессиональной документацией на государственном и иностранном языках</p>	<p>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 инженернотехнических средств физической защиты.</p>	
---	---	--