

**ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ  
«СТАВРОПОЛЬСКИЙ МНОГОПРОФИЛЬНЫЙ  
КОЛЛЕДЖ»**

**ПРОГРАММА  
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ  
ПМ.03 Защита информации техническими средствами  
для обучающихся специальности  
10.02.05 Обеспечение  
информационной безопасности  
автоматизированных систем**

2022 г.

## **Аннотация**

Рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами разработана на основе Федерального государственного стандарта (далее ФГОС) по специальности среднего профессионального образования (далее СПО) Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем утвержденным приказом Минобрнауки России от 09.12.2016г. № 1553. и в соответствии с учебным планом СмК специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённому директором колледжа Кандауровой Н.В. на 2022 г.

Организация-разработчик: Частное образовательное учреждение профессионального образования "Ставропольский многопрофильный колледж"

Разработчики:

1. Хвалько Леонид Александрович

Рассмотрено на заседании методического объединения укрупненных групп специальностей 09.00.00 «Информатика и вычислительная техника»; 10.00.00 «Информационная безопасность» Протокол № 6 от 26.05.2022 г.

Рекомендовано к использованию в учебном процессе Методическим советом СмК, протокол № 6 от 26.05.2022 г.

# 1. ПАСПОРТ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

## ПМ.03 Защита информации техническими средствами

### 1.1. Область применения программы

Рабочая программа профессионального модуля - является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО **10.02.05 Обеспечение информационной безопасности автоматизированных систем**

в части освоения основного вида деятельности (ВД): **ПМ.03 Защита информации техническими средствами** и соответствующие профессиональные компетенции и личностные результаты:

#### 1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное 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 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 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

#### 1.1.2. Перечень личностных результатов

Код	Наименование личностных результатов
ЛР 3	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих
ЛР 1	Осознающий себя гражданином и защитником великой страны

<b>Код</b>	<b>Наименование личностных результатов</b>
ЛР 14	Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности
ЛР 10	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой
ЛР 17	Умеющий рационально использовать время, информацию и материальные ресурсы, соблюдать порядок на рабочем месте, осуществлять коллективную работу в Компании
ЛР 3	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих
ЛР 19	Соблюдающий производственную этику, стиль общения, принятый в Компании
ЛР 16	Выработавший умения и навыки трудовой деятельности, проявляющий основы трудовой культуры по отношению к коллегам, контрагентам и клиентам Компании
ЛР 22	Выработавший принципы экологически целесообразного поведения, бережного отношения к своей жизни, жизни других людей, природы, планеты в целом
ЛР 22	Выработавший принципы экологически целесообразного поведения, бережного отношения к своей жизни, жизни других людей, природы, планеты в целом
ЛР 1	Осознающий себя гражданином и защитником великой страны
ЛР 13	Демонстрирующий готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности
ЛР 16	Выработавший умения и навыки трудовой деятельности, проявляющий основы трудовой культуры по отношению к коллегам, контрагентам и клиентам Компании
ЛР 18	Способный адаптироваться к новой ситуации и применять новые подходы к решению возникающих проблем
ЛР 20	Способный к адекватной самооценке
ЛР 21	Демонстрирующий высокую культуру труда на конкретном рабочем месте. Не использующий сам и не способствующий использованию и дальнейшему распространению пиратского контента в сети.
ЛР 24	Способствующий развитию военно-патриотического движения, активно участвующий в подобных мероприятиях
ЛР 28	Проявляющий осознанное принятие базовых национальных ценностей, традиций, особых форм культурно-исторической, социальной и духовной жизни родного села, города, района Ставропольского края

### 1.1.3. Перечень профессиональных компетенций и видов деятельности

<b>Код</b>	<b>Наименование профессиональных компетенций</b>
ВД	Защита информации техническими средствами
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.

Код	Наименование профессиональных компетенций
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

## 1.2. Цели и задачи модуля - требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями, обучающийся в ходе освоения профессионального модуля должен:

### **иметь практический опыт:**

1. выявлении технических каналов утечки информации;
2. применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;
3. проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;
4. проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

### **уметь:**

1. применять инженерно-технические средства физической защиты объектов информатизации
2. применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных

### **знать:**

1. номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации
2. методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации
3. основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации

## 1.3. Рекомендуемое количество часов на освоение программы профессионального модуля

Всего - 352 час(-а, -ов), в том числе:  
максимальной учебной нагрузки обучающегося - 352 час(-а, -ов), включая:  
обязательной аудиторной учебной нагрузки обучающегося - 352 час(-а, -ов);  
самостоятельной работы обучающегося - 0 час(-а, -ов);

## 2. Содержание обучения по профессиональному модулю ПМ.03 Защита информации техническими средствами

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём часов	Уровень освоения	Коды компетенций
МДК.03.01 Техническая защита информации		172		

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём часов	Уровень освоения	Коды компетенций
Тема №1. Лекции	Содержание учебного материала			ЛР 16, ЛР 1, ЛР 10, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.4., ПК 3.5., ЛР 22
	1 Лекция №1. Понятие информации и информационной безопасности	2	1	
	2 Лекция №2. Понятие «угроза информации». Понятие «риска информационной безопасности»	2	1	
	3 Лекция №3. Целостность, доступность и конфиденциальность информации	2	1	
	4 Лекция №4. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи Часть 1	2	1	
	5 Лекция №5. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи Часть 2	2	1	
	6 Лекция №6. Цели и задачи защиты информации. Основные понятия в области защиты информации	2	1	
	7 Лекция №7. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации	2	1	
	8 Лекция №8. Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации	2	1	
	9 Лекция №9. Каналы и методы несанкционированного доступа к информации. Уязвимости	2	1	
	10 Лекция №10. Анализ существующих методик определения требований к защите информации	2	1	
	11 Лекция №11. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации	2	1	
	12 Лекция №12. Организационная структура системы защиты информации. Законодательные акты в области защиты информации	2	1	
	13 Лекция №13. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации	2	1	
	14 Лекция №14. Основные механизмы защиты информации	2	1	
	15 Лекция №15. Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Часть 1	2	1	
	16 Лекция №16. Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Часть 2	2	1	
	17 Лекция №17. Цели и задачи защиты информации от утечки информации по техническим каналам	2	1	
	18 Лекция №18. Технические каналы утечки информации с СВТ и ИС.	2	1	
	19 Лекция №19. Технические каналы утечки акустической (речевой) и видовой информации.	2	1	
	20 Лекция №20. Технические средства защиты информации в акустических и вибрационных полях.	2	1	
	21 Лекция №21. Характеристика каналов утечки информации от средств связи и ПЭМИН. Средства технической защиты для этих каналов. Часть 1.	2	1	
	22 Лекция №22. Характеристика каналов утечки информации от средств связи и ПЭМИН. Средства технической защиты для этих каналов. Часть 2.	2	1	
	23 Лекция №23. Технические средства защиты от наблюдения и линий связи от утечки конфиденциальной информации. Часть 1.	2	1	
	24 Лекция №24. Технические средства защиты от наблюдения и линий связи от утечки конфиденциальной информации. Часть 2.	2	1	
	25 Лекция №25. Лицензирование деятельности и сертификация средств защиты информации. Часть 1.	2	1	
	26 Лекция №26. Лицензирование деятельности и сертификация средств защиты информации. Часть 2.	2	1	
	27 Лекция №27. Способы и средства оценки эффективности инженерно-технической защиты информации. Часть 1.	2	1	
	28 Лекция №28. Способы и средства оценки эффективности инженерно-технической защиты информации. Часть 2.	2	1	
	29 Лекция №29. Система технической защиты информации. Часть 1	2	1	
	30 Лекция №30. Система технической защиты информации. Часть 2	2	1	
	31 Лекция №31. правовые основы защиты информации и информационной безопасности (Федеральный закон РФ «Об информации, информационных технологиях и о защите информации»)	2	1	
	32 Лекция №32. Аппаратно-программные средства контроля доступа	2	1	
	33 Лекция №33. Настройка аутентификации пользователей с помощью электронного замка	2	1	
	34 Лекция №34. Управление ключами криптографической защиты электронной почты в комплексе программных средств	2	1	
	35 Лекция №35. Изменение политики контроля устройств	2	1	
	36 Лекция №36. Настройка средств криптографической защиты сетевого трафика стандартного протокола IPSec	2	1	
	37 Лекция №37. Управление средствами информационной безопасности сервера	2	1	
38 Лекция №38. Настройка средств защиты информации сервера	2	1		

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём часов	Уровень освоения	Коды компетенций
Тема №2. Практические занятия	Содержание учебного материала			ЛР 1, ЛР 10, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.4., ПК 3.5., ЛР 16, ЛР 22
	1 Практическое занятие №1. Автономный регистратор сотовых разговоров SpRecord SpGate MR	2	2	
	2 Практическое занятие №2. Видеоглазок беспроводной Radio DVR	2	2	
	3 Практическое занятие №3. Видеоэндоскоп MaxiVideo MV208	2	2	
	4 Практическое занятие №4. Микрофон усиливающий «Супер Ухо SD»	2	2	
	5 Практическое занятие №5. Видеорегистратор LawMate PV-550SE с камерой 618CA	2	2	
	6 Практическое занятие №6. Подавитель диктофонов Бубен-ультра	2	2	
	7 Практическое занятие №7. Беспроводная IP-камера для помещений Link 128 МИНИ	2	2	
	8 Практическое занятие №8. Адаптер записи с телефонной линии ICON TRX1	2	2	
	9 Практическое занятие №9. Угрозы безопасности информации на предприятии	2	2	
	10 Практическое занятие №10. Защита информации от традиционного шпионажа и диверсий	2	2	
	11 Практическое занятие №11. Защита информации от случайных угроз	2	2	
	12 Практическое занятие №12. Основные этапы проектирования системы защиты информации	2	2	
	13 Практическое занятие №13. Специфика персонала предприятия как объекта защиты	2	2	
	14 Практическое занятие №14. Разработка моделей объектов защиты	2	2	
	15 Практическое занятие №15. Электронно-цифровая подпись	2	2	
Тема №3. Практическая подготовка	Содержание учебного материала			ЛР 1, ЛР 10, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.4., ПК 3.5., ЛР 16, ЛР 22
	1 Практическая подготовка №1. Законодательство РФ в области информационной безопасности	2	2	
	2 Практическая подготовка №2. Изучение положений о государственном лицензировании деятельности в области защиты информации	2	2	
	3 Практическая подготовка №3. Изучение положений о сертификации средств защиты информации по требованиям безопасности информации	2	2	
	4 Практическая подготовка №4. Система сертификации средств криптографической защиты информации	2	2	
	5 Практическая подготовка №5. Изучение положения о сертификации средств вычислительной техники и связи. Изучение положения по аттестации объектов информатизации по требованиям безопасности информации	4	2	
	6 Практическая подготовка №6. Изучение особенностей аттестации помещений по требованиям безопасности информации. Изучение положения об аккредитации испытательных лабораторий и органов сертификации средств защиты информации по требованиям безопасности информации	4	2	
	7 Практическая подготовка №7. Методы аутентификации и способы управления доступом	4	2	
	8 Практическая подготовка №8. Защита информации от электромагнитных излучений и наводок	4	2	
	9 Практическая подготовка №9. Исследование протокола IPsec	4	2	
	10 Практическая подготовка №10. Изучение средств IP-безопасности, обеспечиваемых протоколом Ipsec	4	2	
	11 Практическая подготовка №11. Организация комплексной системы защиты информации объекта	4	2	
	12 Практическая подготовка №12. Защита информации правовыми и организационными методами	4	2	
	13 Практическая подготовка №13. Моделирование технических каналов утечки информации. Анализ рисков безопасности информации.	4	2	
	14 Практическая подготовка №14. Изучение правовых основ защиты информации и информационной безопасности (Федеральный закон РФ «Об информации, информационных технологиях и о защите информации»). Аппаратно-программные средства контроля доступа	2	2	
	15 Практическая подготовка №15. Настройка аутентификации пользователей помощью электронного замка «СОБОЛЬ-PCI. Управление ключами криптографической защиты электронной почты в комплексе программных средств	2	2	
Тема №4. Промежуточная аттестация	Содержание учебного материала			ЛР 1, ЛР 10, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.4., ПК 3.5., ЛР 16, ЛР 22
	1 Промежуточная аттестация. Промежуточная аттестация	18	2	
Форма контроля - Дифференцированный зачет				
Всего по МДК.03.01 Техническая защита информации		172		
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		100/180		

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём часов	Уровень освоения	Коды компетенций
<b>Тема №1.</b> Лекции	<b>Содержание учебного материала</b>			ЛР 20, ЛР 14, ЛР 17, ЛР 19, ЛР 22, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.4., ПК 3.5., ЛР 1, ЛР 13, ЛР 16, ЛР 18, ЛР 21, ЛР 24, ЛР 28
	1 <b>Лекция №1.</b> Предмет и задачи технической защиты информации.	2	1	
	2 <b>Лекция №2.</b> Характеристика инженерно-технической защиты информации как области информационной безопасности	2	1	
	3 <b>Лекция №3.</b> Системный подход при решении задач инженерно-технической защиты информации.	2	1	
	4 <b>Лекция №4.</b> Основные параметры системы защиты информации.	2	1	
	5 <b>Лекция №5.</b> Задачи и требования к способам и средствам защиты информации техническими средствами.	2	1	
	6 <b>Лекция №6.</b> Принципы системного анализа проблем инженерно-технической защиты информации.	2	1	
	7 <b>Лекция №7.</b> Классификация способов и средств защиты информации.	2	1	
	8 <b>Лекция №8.</b> Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации.	2	1	
	9 <b>Лекция №9.</b> Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов.	2	1	
	10 <b>Лекция №10.</b> Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	2	1	
	11 <b>Лекция №11.</b> Понятие и особенности утечки информации. Структура канала утечки информации.	2	1	
	12 <b>Лекция №12.</b> Классификация существующих физических полей и технических каналов утечки информации	2	1	
	13 <b>Лекция №13.</b> Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика	2	1	
	14 <b>Лекция №14.</b> Классификация технических средств разведки	2	1	
	15 <b>Лекция №15.</b> Методы и средства технической разведки. Средства несанкционированного доступа к информации.	2	1	
16 <b>Лекция №16.</b> Средства и возможности оптической разведки. Средства дистанционного съема информации.	2	1		
<b>Тема №2.</b> Практические занятия	<b>Содержание учебного материала</b>			ЛР 18, ЛР 14, ЛР 17, ЛР 19, ЛР 22, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.4., ПК 3.5., ЛР 1, ЛР 13, ЛР 16, ЛР 20, ЛР 21, ЛР 24, ЛР 28
	1 <b>Практическое занятие №1.</b> Исследование типов вредоносного ПО	2	2	
	2 <b>Практическое занятие №2.</b> Пути заражения ПК вредоносным ПО	2	2	
	3 <b>Практическое занятие №3.</b> Изучение форм проявления компьютерных вирусов	2	2	
	4 <b>Практическое занятие №4.</b> Изучение работы СОМ-вируса	2	2	
	5 <b>Практическое занятие №5.</b> Изучение работы вируса, замещающего программный код	2	2	
	6 <b>Практическое занятие №6.</b> Профилактика проникновения вредоносного программного обеспечения посредством исследования Реестра ОС Windows	2	2	
	7 <b>Практическое занятие №7.</b> Профилактика проникновения вредоносного программного обеспечения посредством организации защиты от макровирусов средствами Microsoft Word	2	2	
8 <b>Практическое занятие №8.</b> Исследование уязвимостей Интернет браузеров в контексте новых веб технологий	2	2		
<b>Тема №3.</b> Практическая подготовка	<b>Содержание учебного материала</b>			ЛР 14, ЛР 17, ЛР 19, ЛР 22, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.4., ПК 3.5., ЛР 18, ЛР 1, ЛР 13, ЛР 16, ЛР 20, ЛР 21, ЛР 24, ЛР 28
	1 <b>Практическая подготовка №1.</b> Шифрование информации методом простой подстановки	4	2	
	2 <b>Практическая подготовка №2.</b> Шифрование информации методом «Решетки Кардано»	4	2	
	3 <b>Практическая подготовка №3.</b> Шифрование информации методом усложненной перестановки по таблице	4	2	
4 <b>Практическая подготовка №4.</b> Шифрование информации методом сложной подстановки	4	2		
<b>Тема №4.</b> Курсовая работа	<b>Содержание учебного материала</b>			ЛР 1, ЛР 22, ЛР 14, ЛР 17, ЛР 19, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.4., ПК 3.5., ЛР 20, ЛР 21, ЛР 24, ЛР 28, ЛР 13, ЛР 16, ЛР 18
1 <b>Курсовая работа.</b> Курсовая работа	30	2		
<b>Тема №5.</b> Промежуточная аттестация	<b>Содержание учебного материала</b>			ЛР 1, ЛР 14, ЛР 17, ЛР 19, ЛР 22, ЛР 3, ОК 01., ОК 02., ОК 03., ОК 04., ОК 05., ОК 06., ОК 07., ОК 08., ОК 09., ОК 10., ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.4., ПК 3.5., ЛР 18, ЛР 20, ЛР 21, ЛР 24, ЛР 28, ЛР 13, ЛР 16
1 <b>Промежуточная аттестация.</b> Промежуточная аттестация	6	2		
<b>Курсовая работа</b>				

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём часов	Уровень освоения	Коды компетенций
	Форма контроля - Дифференцированный зачет			
	Всего по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	100/180		
	Всего по ПМ.03 Защита информации техническими средствами:			

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 - ознакомительный (узнавание ранее изученных объектов, свойств);

2 - репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);

3 - продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

### **3. Условия реализации профессионального модуля**

#### **3.1 Требования к минимальному материально-техническому обеспечению профессионального модуля ПМ.03 Защита информации техническими средствами**

Реализация **МДК.03.01 Техническая защита информации** предполагает наличие:

1. Доска 1;
2. Robobuilder RQ – HVNO (Многофункциональный робот-андроид) 1;
3. Автоматизированные рабочие места на 12 обучающихся;;
4. Автоматизированное рабочее место преподавателя -1 шт;;
5. 12 комплектов компьютерных комплектующих для производства сборки, разборки и сервисного обслуживания ПК и оргтехники;;
6. Специализированная мебель для сервисного обслуживания ПК с заземлением и защитой от статического напряжения -1;;
7. Проектор и экран-1; ;
8. Маркерная доска-1;;
9. Многофункциональное устройство (МФУ) формата А4 -1;
10. Стенды – 4;
11. Плакаты – 20;
12. Матрешка – Z (набор – конструктор) - 4;
13. Структурированная кабельная система -1; ;
14. Эмулятор (эмуляторы) активного сетевого оборудования Cisco Packet Tracer -1;;

Реализация **МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации** предполагает наличие:

- Учебное оборудование:;
- Монитор - 16 шт., ;
  - Системный блок - 16 шт., ;
  - Клавиатура - 16 шт., ;
  - Мышь компьютерная - 16 шт.,;

### **3.2. Учебно-методическое и информационное обеспечение профессионального модуля**

Перечень рекомендуемых учебных изданий и дополнительной литературы для **МДК.03.01 Техническая защита информации:**

Основная литература:

Козьминых, С. И. Организационное и правовое обеспечение информационной безопасности : учебное пособие / С. И. Козьминых. - Тбилиси : Справедливая Грузия, 2020. - 309 с. - ISBN 978-9941-9663-2-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1359091>

Дополнительная литература:

Ищейнов, В. Я. Основные положения информационной безопасности : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ФОРУМ : ИНФРА-М, 2021. — 208 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-489-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189337> (дата обращения: 18.09.2022).

Информационные справочно-правовые системы и ресурсы:

Электронно-библиотечная система Znanium.com

Электронно- библиотечная система BOOK.RU

Перечень рекомендуемых учебных изданий и дополнительной литературы для **МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации:**

Основная литература:

Аполлонский, С.М., Защита техносферы от воздействия физических полей и излучений. Т.2 Защитные материалы от физических полей и излучений : монография / С.М. Аполлонский. — Москва : Русайнс, 2020. — 340 с. — ISBN 978-5-4365-0769-9. — URL:<https://book.ru/book/934705> (дата обращения: 16.10.2022)

Дополнительная литература:

Аполлонский, С.М., Защита техносферы от воздействия физических полей и излучений. Т.1 Виды физических полей и излучений. Нормативно-правовые документы : монография / С.М. Аполлонский. — Москва : Русайнс, 2020. — 332 с. — ISBN 978-5-4365-0778-1. — URL:<https://book.ru/book/934706> (дата обращения: 16.10.2022)

Информационные справочно-правовые системы и ресурсы:

Электронно-библиотечная система Znanium.com



## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

### 4.1. Таблица соответствия компетенций показателям оценки результата

Результаты	Основные показатели оценки результата	Формы и методы контроля и оценки
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Экспертная оценка решения ситуационных задач
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Экспертная оценка решения ситуационных задач
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Планировать и реализовывать собственное профессиональное и личностное развитие.	Экспертная оценка решения ситуационных задач
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Экспертная оценка решения ситуационных задач
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Экспертная оценка решения ситуационных задач
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	Экспертная оценка решения ситуационных задач
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Экспертная оценка решения ситуационных задач
ОК 09. Использовать информационные технологии в профессиональной деятельности.	Использовать информационные технологии в профессиональной деятельности.	Экспертная оценка решения ситуационных задач
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	Пользоваться профессиональной документацией на государственном и иностранном языках.	Экспертная оценка решения ситуационных задач

<b>Результаты</b>	<b>Основные показатели оценки результата</b>	<b>Формы и методы контроля и оценки</b>
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Экспертная оценка решения ситуационных задач
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Экспертная оценка решения ситуационных задач
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.	Экспертная оценка решения ситуационных задач
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Экспертная оценка решения ситуационных задач
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	Организовывать отдельные работы по физической защите объектов информатизации.	Экспертная оценка решения ситуационных задач
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Экспертная оценка решения ситуационных задач

4.2. Образовательные результаты освоения образовательной программы учебной дисциплины, подлежащие проверке

Наименование образовательного результата	Показатели оценки результата	Формы и методы контроля и оценки результата
Иметь практический опыт:		
выявлении технических каналов утечки информации;	владеть навыками выявления технических каналов утечки информации;	– выявлении технических каналов утечки информации;
применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;	владеть навыками применения, технического обслуживания, диагностики, устранения отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;	– применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;
проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	владеть навыками проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	– проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;
проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	владеть навыками проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	– проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
Умения:		
применять инженерно-технические средства физической защиты объектов информатизации	уметь применять инженерно-технические средства физической защиты объектов информатизации	Тестирование
применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных	уметь применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных	
Знания:		

Наименование образовательного результата	Показатели оценки результата	Формы и методы контроля и оценки результата
номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации	знать номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации	Коллоквиум
методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации	знать методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации	
основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации	знать основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации	

#### 4.3. Матрица соответствия контрольно-оценочных средств образовательным результатам учебной дисциплины

Наименование образовательного результата	Код ОК, ПК, ЛР	Формы и методы контроля и оценки результатов обучения, фонды оценочных средств
Иметь практический опыт:		
выявлении технических каналов утечки информации;	ОК 05., ОК 10., ПК 3.2., ПК 3.4.	Вопросы к дифференцированному зачёту №38-50
применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации;	ОК 04., ОК 06., ОК 10., ПК 3.1.	Вопросы к дифференцированному зачёту №25-37
проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	ОК 02., ОК 07., ПК 3.3., ПК 3.1.	Вопросы к дифференцированному зачёту №13-24

Наименование образовательного результата	Код ОК, ПК, ЛР	Формы и методы контроля и оценки результатов обучения, фонды оценочных средств
проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	ОК 01., ОК 04., ОК 07., ПК 3.5.	Вопросы к дифференцированному зачёту №1-12
Умения:		
применять инженерно-технические средства физической защиты объектов информатизации	ПК 3.5., ПК 3.4., ПК 3.3., ПК 3.2., ПК 3.1., ОК 10., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01., ЛР 3, ЛР 28, ЛР 24, ЛР 22, ЛР 22, ЛР 21, ЛР 20, ЛР 19, ЛР 18, ЛР 17, ЛР 16, ЛР 14, ЛР 13, ЛР 1	Вопросы к дифференцированному зачёту №41-50
применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных	ПК 3.5., ПК 3.4., ПК 3.3., ПК 3.2., ПК 3.1., ОК 10., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01., ЛР 3, ЛР 28, ЛР 24, ЛР 22, ЛР 22, ЛР 21, ЛР 20, ЛР 19, ЛР 18, ЛР 17, ЛР 16, ЛР 14, ЛР 13, ЛР 1	Вопросы к дифференцированному зачёту №31-40
Знания:		
номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации	ПК 3.5., ПК 3.4., ПК 3.3., ПК 3.2., ПК 3.1., ОК 10., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01., ЛР 3, ЛР 28, ЛР 24, ЛР 22, ЛР 22, ЛР 21, ЛР 20, ЛР 19, ЛР 18, ЛР 17, ЛР 16, ЛР 14, ЛР 13, ЛР 1	Вопросы к дифференцированному зачёту №21-30
методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации	ПК 3.5., ПК 3.4., ПК 3.3., ПК 3.2., ПК 3.1., ОК 10., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01., ЛР 3, ЛР 28, ЛР 24, ЛР 22, ЛР 22, ЛР 21, ЛР 20, ЛР 19, ЛР 18, ЛР 17, ЛР 16, ЛР 14, ЛР 13, ЛР 1	Вопросы к дифференцированному зачёту №11-20
основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации	ПК 3.5., ПК 3.4., ПК 3.3., ПК 3.2., ПК 3.1., ОК 10., ОК 09., ОК 08., ОК 07., ОК 06., ОК 05., ОК 04., ОК 03., ОК 02., ОК 01., ЛР 3, ЛР 28, ЛР 24, ЛР 22, ЛР 22, ЛР 21, ЛР 20, ЛР 19, ЛР 18, ЛР 17, ЛР 16, ЛР 14, ЛР 13, ЛР 1	Вопросы к дифференцированному зачёту №1-10

## СПИСОК ИСПОЛЬЗОВАННЫХ РПД ПРИ ФОРМИРОВАНИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код	Название РПД	Дисциплина	Активность
15855	[КБАС-2019] Техническая защита информации 2022-2023	МДК.03.01 Техническая защита информации	<b>Нет</b>
15903	[КБАС-2019] МДК.03.02. Инженерно-технические средства физической защиты объектов информатизации 2022-2023	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	<b>Нет</b>

**ИСКЛЮЧИТЕ ЭТУ СТРАНИЦУ ИЗ ПЕЧАТИ!**