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

2023

Аннотация

Рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами.

Рабочая программа учебной дисциплины разработана в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем утверждённым приказом Минобрнауки России от 09.12.2016 г. №1553 и в соответствии с учебным планом СмК специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утверждённым директором колледжа Кандауровой Н.В. на 2023 - 2024 учебный год.

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

Разработчики:

1. Хвалько Леонид Александрович

Данные не найдены (Нет информации о согласовании)

Рассмотрено на заседании методического объединения ого цикла Укрупненных групп специальностей 09.00.00 «Информатика и вычислительная техника»; 10.00.00 «Информационная безопасность»

Протокол №6 от 26.05.2023

Председатель МО Хвалько Леонид Александрович

Рекомендовано к использованию в учебном процессе методическим советом

Протокол №7 от 26.05.2023

Председатель МС Шляхова Наталья Ивановна

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 **10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения основного вида деятельности (ВД) ПМ.03 Защита информации техническими средствами и соответствующие общие, профессиональные компетенции и личностные результаты.**

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
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 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2. Перечень профессиональных компетенций

Код	Наименование профессиональных компетенций
ВД	
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание 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.

1.1.3. Перечень личностных результатов

Код	Наименование личностных результатов
ЛР 1	Осознающий себя гражданином и защитником великой страны

Код	Наименование личностных результатов
ЛР 14	Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности
ЛР 20	Способный к адекватной самооценке
ЛР 28	Проявляющий осознанное принятие базовых национальных ценностей, традиций, особых форм культурно-исторической, социальной и духовной жизни родного села, города, района Ставропольского края
ЛР 10	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой
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 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

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 освоить следующие результаты:

Знание:

- основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации;
- методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;
- номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации;
- основные понятия криптографии и типовых криптографических методов и средств защиты информации;;
- методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;;
- типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.;

Умение:

- применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств

обработки и передачи данных;

- применять инженерно-технические средства физической защиты объектов информатизации;

- использовать типовые программные криптографические средства, в том числе электронную подпись;;

- проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности 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)

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 обучающихс, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	180		
Тема 1 Лекции	Содержание учебного материала			ЛР 14, ЛР 20, ЛР 28, ЛР 1, ОК 01., ОК 06., ОК 08., ПК 3.5., ПК 3.3., ОК 02., ОК 05.
	1 **Лекционные занятия №1** Предмет и задачи технической защиты информации.	2	1	
	2 **Лекционные занятия №2** Характеристика инженерно-технической защиты информации как области информационной безопасности	2	1	
	3 **Лекционные занятия №3** Системный подход при решении задач инженерно-технической защиты информации.	2	1	
	4 **Лекционные занятия №4** Основные параметры системы защиты информации.	2	1	
	5 **Лекционные занятия №5** Задачи и требования к способам и средствам защиты информации техническими средствами.	2	1	
	6 **Лекционные занятия №6** Принципы системного анализа проблем инженерно-технической защиты информации.	2	1	
	7 **Лекционные занятия №7** Классификация способов и средств защиты информации.	2	1	
	8 **Лекционные занятия №8** Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации.	2	1	
	9 **Лекционные занятия №9** Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов.	2	1	
	10 **Лекционные занятия №10** Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	2	1	
	11 **Лекционные занятия №11** Понятие и особенности утечки информации. Структура канала утечки информации.	2	1	
	12 **Лекционные занятия №12** Классификация существующих физических полей и технических каналов утечки информации	2	1	
	13 **Лекционные занятия №13** Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика	2	1	
	14 **Лекционные занятия №14** Классификация технических средств разведки	2	1	
	15 **Лекционные занятия №15** Методы и средства технической разведки. Средства несанкционированного доступа к информации.	2	1	
	16 **Лекционные занятия №16** Средства и возможности оптической разведки. Средства дистанционного съема информации.	2	1	
Тема 2 Практические занятия	Содержание учебного материала			ЛР 1, ЛР 28, ОК 02., ОК 05., ОК 01., ОК 06., ОК 08., ПК 3.5., ПК 3.3., ЛР 14, ЛР 20
	1 **Практические занятия №1** Исследование типов вредоносного ПО	2	2	
	2 **Практические занятия №2** Пути заражения ПК вредоносным ПО	2	2	
	3 **Практические занятия №3** Изучение форм проявления компьютерных вирусов	2	2	
	4 **Практические занятия №4** Изучение работы COM-вируса	2	2	
	5 **Практические занятия №5** Изучение работы вируса, замещающего программный код	2	2	
	6 **Практические занятия №6** Профилактика проникновения вредоносного программного обеспечения посредством исследования Реестра ОС Windows	2	2	
	7 **Практические занятия №7** Профилактика проникновения вредоносного программного обеспечения посредством организации защиты от макровирусов средствами Microsoft Word	2	2	
	8 **Практические занятия №8** Исследование уязвимостей Интернет браузеров в контексте новых веб технологий	2	2	
Тема 3 Практическая подготовка	Содержание учебного материала			ЛР 1, ЛР 14, ЛР 20, ОК 01., ЛР 28, ОК 06., ОК 08., ПК 3.5., ПК 3.3., ОК 02., ОК 05.
	1 **Практическая подготовка №1** Шифрование информации методом простой подстановки	4	2	
	2 **Практическая подготовка №2** Шифрование информации методом «Решетки Кардано»	4	2	
	3 **Практическая подготовка №3** Шифрование информации методом усложненной перестановки по таблице	4	2	
	4 **Практическая подготовка №4** Шифрование информации методом сложной подстановки	4	2	
Тема 4 Курсовая работа	Содержание учебного материала			ЛР 1, ЛР 14, ЛР 20, ЛР 28, ОК 02., ОК 05., ОК 01., ОК 06., ОК 08., ПК 3.5., ПК 3.3.
	1 **Курсовая работа** Курсовая работа	30	2	
Тема 5 Промежуточная аттестация	Содержание учебного материала			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 14, ЛР 20, ЛР 28
	1 **Часы на контроль** Промежуточная аттестация	6	2	

Наименование разделов ПМ, МДК и тем		Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихс, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Тема 6 Основные компоненты комплекса инженерно-технических средств физической защиты	Содержание учебного материала				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 14, ЛР 20, ЛР 28
	1	**Лекционные занятия №17** Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта.	2	1	
	2	**Лекционные занятия №18** Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	2	1	
	3	**Практические занятия №9** Категорирование объектов информатизации.	2	2	
	4	**Практические занятия №10** Тематика учебных занятий формируется образовательной организацией самостоятельно	2	2	
	5	**Практическая подготовка №5** Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты.	2	2	
	6	**Практическая подготовка №6** Принципы построения интегрированных систем охраны.	4	2	
	7	**Лекционные занятия №19** Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты.	2	1	
	8	**Практические занятия №11** Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации	2	2	
	9	**Практическая подготовка №7** Тематика учебных занятий формируется образовательной организацией самостоятельно	4	2	
	10	**Лекционные занятия №20** Информационные основы построения системы охранной сигнализации.	2	1	
	11	**Лекционные занятия №21** Назначение, классификация технических средств обнаружения.	2	1	
	12	**Практическая подготовка №8** Построение систем обеспечения безопасности объекта.	4	2	
	13	**Практическая подготовка №9** Периметровые средства обнаружения: назначение, устройство, принцип действия.	4	2	
	14	**Лекционные занятия №22** Объектовые средства обнаружения: назначение, устройство, принцип действия.	2	1	
	15	**Практические занятия №12** Монтаж датчиков пожарной и охранной сигнализации. Часть 1	2	2	
	16	**Практические занятия №13** Монтаж датчиков пожарной и охранной сигнализации. Часть 2	2	2	
	17	**Лекционные занятия №23** Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД	2	1	
	18	**Лекционные занятия №24** Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД	2	1	
	19	**Лекционные занятия №25** Классификация средств управления доступом. Средства идентификации и аутентификации.	2	1	
	20	**Лекционные занятия №26** Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	2	1	
	21	**Практическая подготовка №10** Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	4	2	
	22	**Практические занятия №14** Рассмотрение принципов устройства, работы и применения средств контроля доступа	2	2	
	23	**Лекционные занятия №27** Аналоговые и цифровые системы видеонаблюдения.	2	1	
	24	**Лекционные занятия №28** Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	2	1	
	25	**Практические занятия №15** Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	2	2	
	26	**Лекционные занятия №29** Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации.	2	1	
	27	**Лекционные занятия №30** Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	2	1	
	28	**Практическая подготовка №11** Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	4	2	
	29	**Лекционные занятия №31** Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	2	1	
	30	**Практические занятия №16** Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	2	2	
	31	**Лекционные занятия №32** 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.	2	1	
	32	**Практическая подготовка №12** Порядок применения устройств отображения и документирования информации.	4	2	
	33	**Практическая подготовка №13** Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	2	2	

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихс, курсовая работа (проект) (если предусмотрены)	Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Курсовая работа		**30**	30	ОК 09., ОК 04., ОК 07., ОК 10., ПК 3.2., ПК 3.1., ПК 3.4., ОК 08., ПК 3.5., ОК 03., ОК 02., ОК 05., ПК 3.3., ОК 01., ОК 06., ЛР 1, ЛР 14, ЛР 20, ЛР 28
Форма(-ы) контроля - 4 семестр, Дифференцированный зачет; 5 семестр, Экзамен; 5 семестр, Курсовая работа				
Всего по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		180		
МДК.03.01 Техническая защита информации		172		

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

Наименование разделов ПМ, МДК и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихс, курсовая работа (проект) (если предусмотрены)		Объём в часах	Уровень освоения	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
Тема 2 Практические занятия	Содержание учебного материала				ОК 02., ОК 05., ПК 3.5., ПК 3.3., ЛР 16, ЛР 22, ОК 01., ОК 06., ОК 08., ЛР 1, ЛР 10, ЛР 3
	1	**Практические занятия №1** Автономный регистратор сотовых разговоров SpRecord SpGate MR	2	2	
	2	**Практические занятия №2** Видеоглазок беспроводной Radio DVR	2	2	
	3	**Практические занятия №3** Видеоэндоскоп MaxiVideo MV208	2	2	
	4	**Практические занятия №4** Видеоэндоскоп MaxiVideo MV208	2	2	
	5	**Практические занятия №5** Видеорегистратор LawMate PV-550SE с камерой 618CA	2	2	
	6	**Практические занятия №6** Подавитель диктофонов Бубен-ультра	2	2	
	7	**Практические занятия №7** Беспроводная IP-камера для помещений Link 128 МИНИ	2	2	
	8	**Практические занятия №8** Адаптер записи с телефонной линии ICON TRX1	2	2	
	9	**Практические занятия №9** Угрозы безопасности информации на предприятии	2	2	
	10	**Практические занятия №10** Защита информации от традиционного шпионажа и диверсий	2	2	
	11	**Практические занятия №11** Защита информации от случайных угроз	2	2	
	12	**Практические занятия №12** Основные этапы проектирования системы защиты информации	2	2	
	13	**Практические занятия №13** Специфика персонала предприятия как объекта защиты	2	2	
	14	**Практические занятия №14** Разработка моделей объектов защиты	2	2	
	15	**Практические занятия №15** Электронно-цифровая подпись	2	2	
Тема 3 Практическая подготовка	Содержание учебного материала				ОК 01., ОК 06., ОК 08., ЛР 10, ЛР 3, ЛР 16, ЛР 22, ОК 02., ОК 05., ПК 3.5., ПК 3.3., ЛР 1
	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 пользователейс помощью электронного замка «СОБОЛЬ-PCI. Управление ключами криптографической защиты электронной почты в комплексе программных средств	2	2	
Тема 4 Промежуточная аттестация	Содержание учебного материала				ОК 01., ОК 02., ОК 05., ПК 3.5., ПК 3.3., ОК 06., ОК 08., ЛР 1, ЛР 16, ЛР 10, ЛР 3, ЛР 22, , ОК 03., ОК 04., ОК 07., ОК 09., ОК 10., ПК 3.1., ПК 3.2., ПК 3.4.
	1	**Часы на контроль** Промежуточная аттестация	18	2	
Форма(-ы) контроля - 3 семестр, Дифференцированный зачет; 4 семестр, Экзамен					
Всего по МДК.03.01 Техническая защита информации			172		
Всего по ПМ.03 Защита информации техническими средствами			**352**		

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 - ознакомительный (ознакомление с ранее изученными объектами, свойствами);
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.03.02 Инженерно-технические средства физической защиты объектов информатизации предполагает наличие помещений:

Компьютерный класс
Кабинет информатики
Лаборатория технологии разработки баз данных
Лаборатория системного и прикладного программирования
Лаборатория информационно-коммуникационных систем
Лаборатория управления проектной деятельностью
Лаборатория вычислительной техники, архитектуры персонального компьютера и периферийных устройств
Лаборатория программного обеспечения и сопровождения компьютерных систем
Лаборатория программирования и баз данных
Лаборатория организации и принципов построения информационных систем
Лаборатория информационных ресурсов

- Клавиатура (16 шт.)
- Матрешка – Z (набор – конструктор) (5 шт.)
- Robobuilder RQ – HUNO (Многофункциональный робот-андроид) (1 шт.)
- Монитор (16 шт.)
- Мышь компьютерная (16 шт.)
- Плакаты (32 шт.)
- Системный блок (16 шт.)
- Стенды (4 шт.)

Реализация МДК.03.01 Техническая защита информации предполагает наличие помещений:

Компьютерный класс
Кабинет информатики
Лаборатория технологии разработки баз данных
Лаборатория системного и прикладного программирования
Лаборатория информационно-коммуникационных систем
Лаборатория управления проектной деятельностью
Лаборатория вычислительной техники, архитектуры персонального компьютера и

периферийных устройств
Лаборатория программного обеспечения и сопровождения компьютерных систем
Лаборатория программирования и баз данных
Лаборатория организации и принципов построения информационных систем
Лаборатория информационных ресурсов

- Клавиатура (16 шт.)
- Матрешка – Z (набор – конструктор) (5 шт.)
- Robobuilder RQ – HUNO (Многофункциональный робот-андроид) (1 шт.)
- Монитор (16 шт.)
- Мышь компьютерная (16 шт.)
- Плакаты (32 шт.)
- Системный блок (16 шт.)
- Стенды (4 шт.)

3.2. Учебно-методическое и информационное обеспечение профессионального модуля

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

Основная литература:

1. 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:

1. 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:

1. Электронно-библиотечная система Znanium.com
2. Электронно- библиотечная система BOOK.RU

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

Основная литература:

1. 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:

1. 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:

1. Электронно-библиотечная система Znanium.com
2. Электронно- библиотечная система BOOK.RU

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

4.1. Таблица соответствия компетенций показателям оценки результата

Результаты (освоенные профессиональные и общие компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ОК		Данные не найдены (основные показатели оценки результата)
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Данные не найдены (формы и методы контроля и оценки)	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Данные не найдены (формы и методы контроля и оценки)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Данные не найдены (формы и методы контроля и оценки)	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	Данные не найдены (формы и методы контроля и оценки)	
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Данные не найдены (формы и методы контроля и оценки)	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Данные не найдены (формы и методы контроля и оценки)	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	Данные не найдены (формы и методы контроля и оценки)	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Данные не найдены (формы и методы контроля и оценки)	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Данные не найдены (формы и методы контроля и оценки)	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	Данные не найдены (формы и методы контроля и оценки)	
ПК		Данные не найдены (основные показатели оценки результата)
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Данные не найдены (формы и методы контроля и оценки)	
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	Данные не найдены (формы и методы контроля и оценки)	
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Данные не найдены (формы и методы контроля и оценки)	
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.	Данные не найдены (формы и методы контроля и оценки)	
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Данные не найдены (формы и методы контроля и оценки)	

4.2. Образовательные результаты освоения образовательной программы профессионального модуля, подлежащие проверке

Наименование образовательного результата	Показатели оценки результата	Формы и методы контроля и оценки результата
Знание		
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	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	Коллоквиум
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
основные понятия криптографии и типовых криптографических методов и средств защиты информации;	Знать основные понятия криптографии и типовых криптографических методов и средств защиты информации;	Коллоквиум
методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	Знать методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	Коллоквиум
типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	Знать типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	Коллоквиум
Умение		
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	Тестирование
применять инженерно-технические средства физической защиты объектов информатизации	уметь применять инженерно-технические средства физической защиты объектов информатизации	Тестирование
использовать типовые программные криптографические средства, в том числе электронную подпись;	Уметь использовать типовые программные криптографические средства, в том числе электронную подпись;	Тестирование
проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;	Уметь проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;	Тестирование

4.3. Матрица соответствия контрольно-оценочных средств образовательным результатам профессионального модуля

Результаты обучения	Коды компетенций	Фонды оценочных средств
Знание		
основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации	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. (МДК.03.02);	Вопросы к дифференцированному зачёту №1-10 (МДК.03.02);
методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации	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. (МДК.03.02);	Вопросы к дифференцированному зачёту №11-20 (МДК.03.02);

Результаты обучения	Коды компетенций	Фонды оценочных средств
номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации	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. (МДК.03.02);	Вопросы к дифференцированному зачёту №21-30 (МДК.03.02);
основные понятия криптографии и типовых криптографических методов и средств защиты информации;	ЛР 1, ЛР 10, ЛР 16, 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. (МДК.03.01);	Вопросы на экзамен №10-19 (МДК.03.01);
методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;	ЛР 1, ЛР 10, ЛР 16, 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. (МДК.03.01);	Вопросы на экзамен №1-9 (МДК.03.01);
типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	ЛР 1, ЛР 10, ЛР 16, 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. (МДК.03.01);	Вопросы на экзамен №20-29 (МДК.03.01);
Умение		
применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных	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. (МДК.03.02);	Вопросы к дифференцированному зачёту №31-40 (МДК.03.02);
применять инженерно-технические средства физической защиты объектов информатизации	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. (МДК.03.02);	Вопросы к дифференцированному зачёту №41-50 (МДК.03.02);
использовать типовые программные криптографические средства, в том числе электронную подпись;	ЛР 1, ЛР 10, ЛР 16, 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. (МДК.03.01);	Вопросы на экзамен №30-39 (МДК.03.01);
проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;	ЛР 1, ЛР 10, ЛР 16, 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. (МДК.03.01);	Вопросы на экзамен №40-50 (МДК.03.01);