

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САМАРСКОЙ ОБЛАСТИ
«ГУБЕРНСКИЙ КОЛЛЕДЖ Г. СЫЗРАНИ»

СОГЛАСОВАНО

Директор ООО "ЦЕНТР ЗАЩИТЫ

ИНФОРМАЦИИ"

 Д.А. Полоса

«» 20 21 г.

М.П.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

профессиональный цикл

программы подготовки специалистов среднего звена по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Сызрань, 2021 г.

РАССМОТРЕНА

Предметной (цикловой) комиссией
общепрофессиональных и профессиональных
дисциплин
от «27» мая 2021 г. протокол № 10

Составитель: А.Л.Анищенко методист строительного профиля ГБПОУ «ГК г. Сызрани»

Внутренняя экспертиза (техническая и содержательная): А.Л.Анищенко, методист
строительного профиля ГБПОУ «ГК г. Сызрани»

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	7
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	8
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	12
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	15
6. ПРИЛОЖЕНИЯ	16
7. ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	22

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить вид деятельности *Защита информации техническими средствами* и соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
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.

1.1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	установки, монтажа и настройки технических средств защиты информации; технического обслуживания технических средств защиты информации; применения основных типов технических средств защиты информации; выявления технических каналов утечки информации; участия в мониторинге эффективности технических средств защиты информации; диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.
уметь	применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации
знать	порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации.

1.3. Количество часов на освоение программы профессионального модуля

Вид учебной деятельности	Объём часов
Всего часов на учебную дисциплину	638
Самостоятельная работа	16
Всего во взаимодействии с преподавателем	622
из них:	
Теоретическое обучение	90
Лабораторные и практические занятия	202
Курсовая работа (проект)	30
Консультации	18
Промежуточная аттестация МДК	18
Учебная практика	108
Производственная практика	144
Экзамен (квалификационный) по профессиональному модулю	12
Промежуточная аттестация в форме экзамена	

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Тематический план профессионального модуля

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Занятия во взаимодействии с преподавателем, час.							Квалификационный экзамен	Самостоятельная работа	
			Обучение по МДК, в час.					Практики				
			Теоретическое обучение	Лабораторных и практических занятий	Курсовых работ (проектов)	Консультации	Промежуточная аттестация	Учебная	Производственная (если предусмотрена рассредоточенная практика)			
1	2	3	4	5	6			7	8		9	
<i>ПК 3.1-3.2</i>	Раздел 1. Применение технической защиты информации	152	36	98		6	6					6
<i>ПК 3.3.-3.4.</i>	Раздел 2. Применение инженерно-технических средств физической защиты объектов информатизации	330	54	104	30	12	12	108				10
	Производственная практика	144							144			
	Квалификационный экзамен	12								12		
	Всего:	638	90	202	30	18	18	108	144	12		16

3.2 Содержание обучения по профессиональному модулю

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов
1	2	3
Раздел 1. Применение технической защиты информации		
МДК.03.01 Техническая защита информации		
Тема 1. Концепция инженерно-технической защиты информации		
Тема 1.1. Предмет и задачи технической защиты информации	Содержание	2
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	
Тема 1.2. Общие положения защиты информации техническими средствами	Содержание	2
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.	
Тема 2. Теоретические основы инженерно-технической защиты информации		
Тема 2.1. Информация как предмет защиты	Содержание	2
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	
	Тематика практических занятий и лабораторных работ	6
	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	
Тема 2.2. Технические каналы утечки информации	Содержание	2
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	
	Тематика практических занятий и лабораторных работ	8

	Изучение устройств обнаружения и локализации закладных устройств для снятия информации. Тестирование шлейфовых линий для обнаружения несанкционированных подключений.	
Тема 2.3. Методы и средства технической разведки	Содержание	2
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	
	Тематика практических занятий и лабораторных работ	28
	Изучение, диагностика отказов и практическое использование объемного датчика движения Изучение, диагностика отказов датчика охраны границ объекта и его практическое использование Изучение автомобильной сигнализации Устройство кодового замка, диагностика отказов и восстановление работоспособности. Изучение системы охранно-пожарной сигнализации и ее практическое применение. Изучение устройства контроля и ограничения доступа. Система видеонаблюдения и ее практическое использование.	
Тема 3. Физические основы технической защиты информации		
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание	4
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	
	Тематика практических занятий и лабораторных работ	4
	Измерение параметров физических полей	
Тема 3.2. Физические процессы при подавлении опасных сигналов	Содержание	2
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	
	Тематика практических занятий и лабораторных работ	
Тема 4. Системы защиты от утечки информации		
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	Содержание	2
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	
	Тематика практических занятий и лабораторных работ	4

	Защита от утечки по акустическому каналу	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	Содержание	2
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	
	Тематика практических занятий и лабораторных работ	
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу		2
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	
	Тематика практических занятий и лабораторных работ	4
	Защита от утечки по виброакустическому каналу	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	Содержание	2
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	
	Тематика практических занятий и лабораторных работ	8
	Определение каналов утечки ПЭМИН	
	Защита от утечки по цепям электропитания и заземления	
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	Содержание	2
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	
	Тематика практических занятий и лабораторных работ	4
	Защита от утечки по телефонному каналу	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	Содержание	2
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
	Тематика практических занятий и лабораторных работ	4
	Защита от утечки по электросетевому каналу	
Тема 4.7. Системы	Содержание	2

защиты от утечки информации по оптическому каналу	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	
	Тематика практических занятий и лабораторных работ	4
	Защита от утечки по оптическому каналу	
Тема 5. Применение и эксплуатация технических средств защиты информации		
Тема 5.1. Применение технических средств защиты информации	Содержание	4
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.	
	Тематика практических занятий и лабораторных работ	10
	Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.	
	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	
Тема 5.2. Эксплуатация технических средств защиты информации	Содержание	2
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.	
	Тематика практических занятий и лабораторных работ	14
	Установка и настройка технических средств защиты информации.	
	Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.	
	Организация ремонта технических средств защиты информации.	
	Проведение аттестации объектов информатизации.	-
Самостоятельная работа при изучении раздела 1 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.		6
Консультации		6
Промежуточная аттестация по МДК.03.01		6
Учебная практика Виды работ		
Раздел 2. Применение инженерно-технических средств физической защиты объектов информатизации		
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		
Тема 1. Построение и основные характеристики инженерно-технических средств физической защиты		
Тема 1.1. Цели и задачи	Содержание	6

физической защиты объектов информатизации	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Особенности задач охраны различных типов объектов.	
	Тематика практических занятий и лабораторных работ	8
	Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	Содержание	6
	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.	
	Тематика практических занятий и лабораторных работ	8
	Рассмотрение инженерных конструкций, применяемые для предотвращения проникновения злоумышленника к источникам информации.	
Тема 2. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	Содержание	6
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	
	Тематика практических занятий и лабораторных работ	10
	Монтаж датчиков пожарной и охранной сигнализации	
Тема 2.2. Система контроля и управления доступом	Содержание	6
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	
	Тематика практических занятий и лабораторных работ	10
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	
	Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Тема 2.3. Система телевизионного наблюдения	Содержание	4
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	
	Тематика практических занятий и лабораторных работ	8

	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	
Тема 2.4. Система сбора, обработки, отображения и документирования информации	Содержание	4
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	
	Тематика практических занятий и лабораторных работ	8
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	
Тема 2.5 Система воздействия	Содержание	2
	Назначение и классификация технических средств воздействия.	
	Тематика практических занятий и лабораторных работ	8
	Определение основных показателей технических средств воздействия.	
Тема 3. Применение и эксплуатация инженерно-технических средств физической защиты		
Тема 3.1 Применение инженерно-технических средств физической защиты	Содержание	4
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП.	
	Тематика практических занятий и лабораторных работ	12
	Управление системой телевизионного наблюдения с автоматизированного рабочего места.	
	Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	Содержание	2
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.	
	Тематика практических занятий и лабораторных работ	12
	Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	
	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.	
Курсовой проект (работа)		30
Примерная тематика курсового проекта (работы)		
1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации.		
2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации.		
3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.		
Примерная тематика самостоятельной работы при изучении МДК.03.02		10

– Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты.		
– Размещение периметровых средств обнаружения на местности.		
– Самостоятельное изучения порядка допуска субъектов на охраняемые объекты.		
Консультации		6
Промежуточная аттестация по МДК.03.02		6
МДК.03.03 Физические основы защиты информации		
Тема 1. Построение и основные характеристики средств физической защиты		
Тема 1.1. Введение. Технические каналы утечки информации. Постановка задачи. Физические основы.	Содержание Физические процессы построения средств защиты от съема информации. Технические средства получения информации. Задачи физических средств ЗИ. Защита информации от утечки по техническим каналам. Характеристика технических каналов утечки информации. Каналы утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации. Явления, процессы и действия, выполняемые и существующие при решении задач защиты информации от утечки по техническим каналам. Характеристики радиоканала передачи информации. Оценка влияния мощности источника излучения (передатчика), влияние передающей антенны, влияние приемника (с оценкой достижимости характеристик по чувствительности, избирательности и другим), влияние приемных антенн. Возможности и ограничения методов защиты от утечки информации основанных на электромагнитном экранировании, на применении генераторов шума. Методы обнаружения электромагнитных излучений и источников излучений с применением широкополосных индикаторов поля, узкополосных сканирующих приемников, анализаторов спектра, нелинейных локаторов.	10
	Тематика практических занятий и лабораторных работ	12
	Создание модели ситуаций возникновения утечки информации и описание этих каналов с оценкой их реальности, опасности, дальности действий, требуемых мер по защите	
Тема 1.2. Основы нормативной базы организации защиты информации в Российской Федерации	Содержание	-
	Тематика практических занятий и лабораторных работ	8
	Изучение Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 02.07.2013) "Об информации, информационных технологиях и о защите информации"	
Тема 1.3. Доктрина информационной безопасности Российской Федерации.	Содержание Информационная безопасность Российской Федерации Методы обеспечения информационной безопасности Российской Федерации Основные положения государственной политики обеспечения информационной безопасности РФ и первоочередные мероприятия по ее реализации	4

	Организационная основа системы обеспечения информационной безопасности РФ	
	Тематика практических занятий и лабораторных работ	-
Самостоятельная работа при изучении раздела 2 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.		10
Консультации		6
Промежуточная аттестация по МДК.03.03		6
Учебная практика по разделу 2 модуля Измерение параметров физических полей. Определение каналов утечки ПЭМИН. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Установка и настройка технических средств защиты информации. Проведение измерений параметров побочных электромагнитных излучений и наводок. Проведение аттестации объектов информатизации. Монтаж различных типов датчиков. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. Рассмотрение системы контроля и управления доступом. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. Рассмотрение датчиков периметра, их принципов работы. Выполнение звукоизоляции помещений системы шумления. Реализация защиты от утечки по цепям электропитания и заземления. Разработка организационных и технических мероприятий по заданию преподавателя; Разработка основной документации по инженерно-технической защите информации.		108
Производственная практика профессионального модуля Виды работ 1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; 3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съема и утечки по		144

техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	
Экзамен (квалификационный) по профессиональному модулю	<i>12</i>
Всего	<i>638</i>

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1 Требования к минимальному материально-техническому обеспечению

Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

лекционные аудитории с мультимедийным оборудованием; лаборатория «Технических средств защиты информации».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест – не менее 30, рабочее место преподавателя, проектор, персональный компьютер, интерактивная доска, комплект презентаций.

Оборудование лаборатории «Технических средств защиты информации» и рабочих мест лаборатории:

- 1) рабочие места студентов, оборудованные персональными компьютерами;
- 2) лабораторные учебные макеты;
- 3) аппаратные средства аутентификации пользователя;
- 4) средства защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок;
- 5) средства измерения параметров физических полей;
- 6) стенд физической защиты объектов информатизации, оснащенный средствами контроля доступа, системами видеонаблюдения и охраны объектов;
- 7) рабочее место преподавателя;
- 8) учебно-методическое обеспечение модуля;
- 9) интерактивная доска, комплект презентаций.

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.

2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015.

3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013. – 172 с.

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

5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

6. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2012

7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012

8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с.

3.2.2. Дополнительные печатные источники:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

35. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

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

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

38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых

электромагнитных воздействий. Общие положения. Росстандарт, 2014.

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

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

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

42. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

43. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

44. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

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

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

47. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

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

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

50. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

3.2.3 Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru/>
4. справочно-правовая система «Консультант Плюс» www.consultant.ru
5. справочно-правовая система «Гарант» www.garant.ru
6. Федеральный портал «Российское образование» www.edu.ru

7. Федеральный правовой портал «Юридическая Россия» <http://www.law.edu.ru/>
8. Федеральный портал «Информационно-коммуникационные технологии в образовании»
<http://www.ict.edu.ru>
9. Сайт Научной электронной библиотеки www.elibrary.ru

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

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

<p>ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации</p>	<p>Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации</p>	<p>тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
<p>ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации</p>	<p>Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации</p>	<p>тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>

ПРИЛОЖЕНИЕ 3
к рабочей программе профессионального модуля

**ПЛАНИРОВАНИЕ УЧЕБНЫХ ЗАНЯТИЙ С ИСПОЛЬЗОВАНИЕМ
АКТИВНЫХ И ИНТЕРАКТИВНЫХ ФОРМ И МЕТОДОВ ОБУЧЕНИЯ
СТУДЕНТОВ**

№ п/п	Тема учебного занятия	Активные и интерактивные формы и методы обучения	Код формируемых компетенций
1.	Предмет и задачи технической защиты информации.	Урок презентация	ОК 02-04, ПК 1.1
2.	Классификация технических средств разведки.	семинар	ОК 05, ПК 1.1.
3.	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.	Решение практической задачи	ПК 1.3, ОК 02, ОК 09
4.	Классификация системы сбора и обработки информации.	Работа в м/группах	ПК 1.3, ОК 02, ОК 09
5.	Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.	Урок с элементами проблемного обучения	ОК 01-ОК 05

ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

Дата актуализации	Результаты актуализации	Фамилия И.О. и подпись лица, ответственного за актуализацию