Департамент внутренней и кадровой политики Белгородской области
Областное государственное автономное профессиональное образовательное учреждение
«Белгородский индустриальный колледж»

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

по специальности
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

квалификация
техник по защите информации

Белгород 2020 г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности **10.02.04 Обеспечение информационной безопасности телекоммуникационных систем** примерной основной образовательной программы (разработчик ПООП: **Федеральное учебно-методическое объединение в системе среднего профессионального образования по укрупненной группе специальностей 10.00.00 «Информационная безопасность», 2017 год**).

Рассмотрено цикловой комиссией Протокол заседания № 1 от «31» августа 2020г. Председатель цикловой комиссии _____/Чобану Л.А./	Согласовано Зам.директора по УМР _____/Бакалова Е.Е. «31» августа 2020 г.	Утверждаю Зам.директора по УР _____ /Выручаева Н.В. «31» августа 2020 г.
Рассмотрено цикловой комиссией Протокол заседания № 1 от «___» августа 2021 г. Председатель цикловой комиссии _____/_____		
Рассмотрено цикловой комиссией Протокол заседания № 1 от «___» августа 2022 г Председатель цикловой комиссии _____/_____		
Рассмотрено цикловой комиссией Протокол заседания № 1 от «___» августа 2023 г Председатель цикловой комиссии _____/_____		

Организация-разработчик: ОГАПОУ «Белгородский индустриальный колледж»
Составитель:
преподаватель ОГАПОУ «Белгородского индустриального колледж»
Петрушин С.Д.
Экспертиза:
(*внутренний рецензент*) ОГАПОУ «Белгородский индустриальный колледж», преподаватель, Чобану Л.А.
(внешний рецензент) ФГУП РТРС филиала «Белгородский ОРТПЦ», директор, Моисеев С.П.

СОДЕРЖАНИЕ

	стр.
1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	8
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	19
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)	22

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Область применения программы

Рабочая программа профессионального модуля (далее рабочая программа) является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности (специальностям) СПО **10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.**

1.2. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности **Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты** и соответствующие ему общие и профессиональные компетенции:

1.2.1. Перечень общих компетенций

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 9.	Использовать информационные технологии в профессиональной деятельности.

1.2.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВПД 3	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно-телекоммуникационных системах и сетях
ПК 3.2.	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях
ПК 3.3.	Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями
ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

1.2.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации; проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; установка, монтаж и настройка, техническое обслуживание,

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

1.4. Рекомендуемое количество часов на освоение программы профессионального модуля:

Всего часов: 616 часов, в том числе:
на освоение МДК, в том числе промежуточную аттестацию – 394 часов,
на практики 216 часов, в том числе:
учебную – 72 часов,
производственную – 144 часов.
консультации – 4 часов;
самостоятельную – 12 часов.
промежуточная аттестация – 6 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

2.1. Структура профессионального модуля

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, час.						Самостоятельная работа обучающегося[1]	Консультации
			Обучение по МДК, в час.				Практики			
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Промежуточная аттестация	Учебная, часов	Производственная, часов		
1	2	3	4	5	6	7	8	9	10	11
ПК 3.1- ПК.3.4 ОК 1 – ОК 7, ОК 9	Раздел 1. Защита информации в ИТКС с использованием технических средств защиты	216	200	74		6			6	4
ПК 3.4 ОК 1 – ОК 7, ОК 9	Раздел 2. Физическая защита линий связи ИТКС	178	172	70					6	
	Учебная практика	72					72			
	Производственная практика	144						144		
Экзамен по модулю		6								
Всего:		616	372	144		6	216		12	4

1Примерная тематика самостоятельных работ в рамках образовательной программы планируется образовательной организацией соответствия с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины.

2.2. Тематический план и содержание профессионального модуля ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)		Объем часов
1	2		3
Раздел 1. Защита информации в ИТКС с использованием технических средств защиты			**216**
МДК.03.01. Защита информации в ИТКС с использованием технических средств защиты			216
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**		**8**
	1	Предмет и задачи технической защиты информации.	8
	2	Характеристика инженерно-технической защиты информации как области информационной безопасности.	
	3	Системный подход при решении задач инженерно-технической защиты информации.	
	4	Основные параметры системы защиты информации.	
Тема 1.2. Общие положения защиты информации	**Содержание**		**6**
	1	Задачи и требования к способам и средствам защиты информации техническими средствами.	6
	2	Принципы системного анализа проблем инженерно-технической защиты информации.	

техническими средствами	3	Классификация способов и средств защиты информации.	
Тема 2.1. Информация как предмет защиты	**Содержание**		**14**
	1	Особенности информации как предмета защиты. Свойства информации.	10
	2	Виды, источники и носители защищаемой информации.	
	3	Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале.	
	4	Источники опасных сигналов. Основные и вспомогательные технические средства, и системы.	
	5	Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	
	Лабораторные работы		4
	1-2	Обнаружение скрытого видеонаблюдения	
Тема 2.2. Технические каналы утечки информации	**Содержание**		**10**
	1	Понятие и особенности утечки информации. Структура канала утечки информации.	6
	2	Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации.	
	3	Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	
	Лабораторные работы		4
	3-4	Ознакомление с многофункциональным имитатором сигналов «Шиповник 2»	
Тема 2.3. Методы и средства технической разведки	**Содержание**		**12**
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.		8
	Лабораторные работы		4
	5-6	Работа с устройствами комбинированной защиты объектов информатизации	
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных	**Содержание**		**12**
	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		8

излучений и наводок	электромагнитных излучений и наводок, параметров фоновых шумов и физических полей		
	Лабораторные работы		4
	7-8	Аттестации помещения по требованиям безопасности информации	
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание**		**10**
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.		6
	Лабораторные работы		4
	9-10	Технические средства защиты информации в телефонных линиях	
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**		**12**
	1	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации.	8
	2	Прослушивание информации направленными микрофонами.	
	3	Система защиты от утечки по акустическому каналу.	
	4	Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу	
	Лабораторные работы		4
	11-12	Поиск и измерение побочных электромагнитных излучений и наводок	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**		**18**
	1	Принцип работы микрофона и телефона.	10
	2	Использование коммуникаций в качестве соединительных проводов.	
	3	Негласная запись информации на диктофоны.	
	4	Системы защиты от диктофонов.	
	5	Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	
	Лабораторные работы		8
	13-14	Генераторы псевдослучайных последовательностей.	
	15-16	Линейный конгруэнтный и рекуррентный генераторы ПСП.	
Тема 4.3. Системы защиты от утечки информации по	**Содержание**		**12**
	1	Электронные стетоскопы. Лазерные системы подслушивания.	8
	2	Гидроакустические преобразователи.	

вибрационному каналу	3	Системы защиты информации от утечки по вибрационному каналу.	
	4	Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	
	Лабораторные работы		4
	17-18	Контроль эффективности защиты речевой информации	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**		**16**
	1	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры.	8
	2	Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладках.	
	3	Системы защиты от утечки по электромагнитному каналу.	
	4	Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	
	Лабораторные работы		8
	19-20	Исследование принципов формирования псевдослучайных последовательностей и методов их тестирования	
	21-22	Оценка защищенности помещения от утечки информации по каналам акустоэлектрических преобразований технических средств	
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**		**12**
	1	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.	8
	2	Использование микрофона телефонного аппарата при положенной телефонной трубке.	
	3	Утечка информации по сотовым цепям связи.	
	4	Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	
	Лабораторные работы		4
	23-24	Поиск каналов утечки речевой информации	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**		**12**
	1	Низкочастотное устройство съема информации.	8
	2	Высокочастотное устройство съема информации.	
	3	Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
	Лабораторные работы		4

	25-26	Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации.	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**		**10**
	1	Телевизионные системы наблюдения.	6
	2	Приборы ночного видения.	
	3	Системы защиты информации по оптическому каналу.	
	Лабораторные работы		4
	27-28	Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации, использующих силовые линии сети переменного тока и линии систем охранной (пожарной) сигнализации	
Тема 5.1. Применение технических средств защиты информации	**Содержание**		**18**
	1	Технические средства для уничтожения информации и носителей информации, порядок применения.	10
	2	Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.	
	3	Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.	
	4	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	
	Лабораторные работы		8
	29-30	Исследование принципов построения симметричных криптосистем и их использования для защиты данных	
	31-32	Исследование процедуры формирования и проверки электронной цифровой подписи на основе ассиметричного алгоритма RSA	
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**		**18**
	1	Этапы эксплуатации технических средств защиты информации.	8
	2	Виды, содержание и порядок проведения технического обслуживания средств защиты информации.	
	3	Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.	
	4	Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.	
	Лабораторные работы		10
	33-34	Исследование схемы разделения секрета	
	35-36	Изучение средств выявления каналов утечки информации на примере высокочувствительного	

		сканирующего приемника AR-5000A «КВАДРАТ»	
	37	Обнаружение приборов наблюдения и оптических приборов	
Самостоятельная учебная работа при изучении раздела ПМ. 03 **Примерная тематика домашних заданий:** 1. Классификация способов и средств защиты информации. 2. Основные и вспомогательные технические средства, и системы. 3. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. 4. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика. 5. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу. 6. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу. 7. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу. 8. Технические средства для уничтожения информации и носителей информации, порядок применения.			**6**
Консультации			**4**
Промежуточная аттестация			**6**
Раздел 2. Физическая защита линий связи ИТКС			**178**
МДК.03.02. Физическая защита линий связи ИТКС			178
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**		**12**
	1	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации.	10
	2	Основные понятия инженерно-технических средств физической защиты.	
	3	Категорирование объектов информатизации.	
	4	Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.	
	5	Особенности задач охраны различных типов объектов.	
	Лабораторные работы		2
	1	Обнаружение приборов наблюдения и оптических приборов	

Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**		**24**
	1	Общие принципы обеспечения безопасности объектов.	12
	2	Жизненный цикл системы физической защиты.	
	3	Принципы построения интегрированных систем охраны.	
	4	Классификация и состав интегрированных систем охраны.	
	5	Требования к инженерным средствам физической защиты.	
	6	Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	
	Лабораторные работы		12
	2-4	Поиск каналов утечки информации с помощью нелинейного локатора. Поиск и обнаружение радиозакладок в помещении	
	5-7	Поиск каналов утечки информации с помощью индикатора поля. Поиск и обнаружение радиозакладок в помещении	
Тема 2.1. Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**		**14**
	1	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения.	8
	2	Построение систем обеспечения безопасности объекта.	
	3	Периметровые средства обнаружения: назначение, устройство, принцип действия.	
	4	Объектовые средства обнаружения: назначение, устройство, принцип действия.	
	Лабораторные работы		6
	8-10	Изучение средств выявления каналов утечки информации на примере программно-аппаратного комплекса измерения ПЭМИН «СИГУРД»»	
Тема 2.2. Система контроля и управления доступом	**Содержание**		**28**
	1	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности.	20
	2	Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД.	
	3	Основы построения и принципы функционирования СКУД. Классификация средств управления доступом.	
	4	Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД.	
	5	Обнаружение металлических предметов и радиоактивных веществ.	
	Лабораторные работы		8
	11-12	Взлом моноалфавитного подстановочного шифра методом частотной атаки	

	13-14	Одноразовые блокноты	
Тема 2.3. Система телевизионного наблюдения	**Содержание**		**20**
	1	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения.	16
	2	Состав системы телевизионного наблюдения.	
	3	Видеокамеры. Объективы. Термокожухи.	
	4	Поворотные системы. Инфракрасные осветители. Детекторы движения.	
	Лабораторные работы		4
	15-16	Сеть Фейштеля	
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание**		**12**
	1	Классификация системы сбора и обработки информации.	8
	2	Схема функционирования системы сбора и обработки информации.	
	3	Варианты структур построения системы сбора и обработки информации.	
	4	Устройства отображения и документирования информации.	
	Лабораторные работы		4
	17-18	Шифрование с открытым ключом и электронная цифровая подпись на GPG	
Тема 2.5. Система воздействия	**Содержание**		**8**
	1	Назначение и классификация технических средств воздействия.	4
	2	Основные показатели технических средств воздействия.	
	Лабораторные работы		4
	19-20	Метод шифрования с открытым ключом RSA	
Тема 3.1. Применение инженерно-технических средств физической защиты	**Содержание**		**28**
	1	Периметровые и объектовые средства обнаружения, порядок применения.	12
	2	Работа с периферийным оборудованием системы контроля и управления доступом.	
	3	Особенности организации пропускного режима на КПП.	
	4	Управление системой телевизионного наблюдения с автоматизированного рабочего места.	
	5	Порядок применения устройств отображения и документирования информации.	
	6	Управление системой воздействия.	
	Лабораторные работы		16
	21-22	Использование хэш-функций на примере MD5. Оценка устойчивости пароля ко взлому.	

	23-25	Исследование основных характеристик сигналов на основе использования аппаратно-программного комплекса радиоконтроля «КВАДРАТ»	
	26-28	Скрытая передача информации в JPEG изображениях	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**		**24**
	1	Этапы эксплуатации.	12
	2	Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.	
	3	Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	
	4	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.	
	5	Организация ремонта технических средств физической защиты.	
	Лабораторные работы		12
	29-31	Запись и чтение информации для пластиковых карт с магнитной полосой	
	32-35	Виды штрих-кодов, их генерация и считывание	
Самостоятельная учебная работа при изучении раздела модуля ПМ. 03 **Примерная тематика домашних заданий:** 1.Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) 2.Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.			**6**
Учебная практика (по профилю специальности) Вводное занятие. Инструктаж по технике безопасности. Цели и задачи практики, требования. 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 зашумления. Реализация защиты от утечки по цепям электропитания и заземления. Разработка организационных и технических мероприятий по заданию преподавателя;			**72**

Разработка основной документации по инженерно-технической защите информации.	
Производственная практика (по профилю специальности) Вводное занятие. Инструктаж по технике безопасности. Цели и задачи практики, требования Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности Участие в монтаже, обслуживании и эксплуатации инженерной защиты и технической охраны объектов, Участие в монтаже, обслуживании и эксплуатации средств систем видеонаблюдения; Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма Участие в монтаже, обслуживании и эксплуатации средств утечки по техническим каналам; Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. Оформление отчета по итогам практики Участие в зачетной конференции по итогам практики	**144**
Экзамен по модулю	**6**
Всего:	**616**

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Лаборатория «Защиты информации от утечки по техническим каналам».

Оборудование лаборатории и рабочих мест:

- автоматизированное рабочее место преподавателя;
- посадочные места обучающихся (по количеству обучающихся);
- маркерная доска;
-компьютеры (рабочие станции);
- локальная сеть;
- мультимедийный класс;
- комплект учебно-методической документации;
- комплект нормативно-правовой документации;
-лицензионное программное обеспечение.

Технические средства обучения:

-рабочее место преподавателя, оснащенное компьютером с лицензионным программным обеспечением, мультимедиа проектором и электронной доской.

- обучающие видеофильмы, презентации

Реализация программы профессионального модуля предполагает обязательную производственную практику (по профилю специальности).

Производственную практику (по профилю специальности) рекомендуется проводить концентрированно в специально выделенный период на рабочих местах баз практики.

Оборудование и технологическое оснащение рабочих мест: необходимо наличие современной техники, использование новейших технологий, применение передовых методов организации труда, поддержание строгой дисциплины на производстве, наличие достаточного количества квалифицированного персонала, способного осуществлять систематическую помощь и контроль над процессом прохождения практики, а также наличие материалов, необходимых для составления отчета. Лаборатория должна быть оснащена: средствами защиты информации от утечки по акустическому (виброакустическому) каналу; средствами защиты информации от утечки по каналам, формируемым за счет побочных электромагнитных излучений и наводок; средствами контроля эффективности защиты информации от утечки по акустическому (виброакустическому) каналу и каналам побочных электромагнитных излучений и наводок; шумогенераторы; комплексный поисковый прибор; прожигатели телефонных линий; устройство обнаружения скрытых видеокамер; виброакустические генераторы; подавители диктофонов; подавители устройств сотовой связи; устройство защиты аналоговых сигналов; устройство защиты цифровых сигналов; стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения, охранно-пожарной

сигнализации и охраны объектов; комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1. Печатные издания

1. Белов Е.Б. 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.
2. Бубнов, А.А. Основы информационной безопасности [Текст]: учеб. пособие для студентов учреждений среднего проф. образования / А. А. Бубнов, В. Н. Пржегорлинский, О. А. Савинкин. - 3-е изд., стер. - М.: Академия, 2017. - 256 с.
3. Мельников В.П. Информационная безопасность.: учебник / В.П. Мельников под ред., А.И. Куприянов — М.: КноРус, 2020. — 267 с.
4. Новикова Е. Л. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи [Текст]: учебник для использования в образовательном процессе образовательных организаций, реализующих программы среднего профессионального образования по специальности "Инфокоммуникационные сети и системы связи" / Е. Л. Новикова. – М.: Академия, 2018. – 192 с.
5. Пеньков Т.С. Основы построения технических систем охраны периметров / Т.С. Пеньков – М.: Учебное пособие, 2018. – 20 с.
6. Сперанский, Д. В. Моделирование, тестирование и диагностика цифровых устройств / Д. В. Сперанский, Ю. А. Скобцов, В. Ю. Скобцов. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 529 с.
7. . Основы надежности средств связи: учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов: Ай Пи Эр Медиа, 2019. — 227 с. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/80290.html (дата обращения: 05.11.2019). — Режим доступа: для авторизир. пользователей

3.2.2. Электронные издания (электронные ресурсы)

Интернет-ресурсы:

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

5. http://www.morion.ru/

6. http://www.nateks.ru/

7. http://www.iskratel.com/

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

9. http://3m.com/

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

3.2.3. Дополнительные источники

1. Аминев А.В. Измерения в телекоммуникационных системах [Электронный ресурс]: учебное пособие / А.В. Аминев, А.В. Блохин. - Электрон. текстовые данные. - Екатеринбург: Уральский федеральный университет, ЭБС АСВ, 2015. -224 с. -Режим доступа: http://www.iprbookshop.ru/65927.html

2. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие / П.Н. Башлы, А.В. Бабаш, Е.К. Баранова. - Электрон. текстовые данные. - М.: Евразийский открытый институт, 2016. - 311 с. - Режим доступа: http://www.iprbookshop.ru/10677.html

3. Нестеров С.А. Основы информационной безопасности [Электронный ресурс] Нестеров С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / Нестеров С. А. - Электрон. текстовые данные. - СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2016. - 322 с. - Режим доступа: http://www.iprbookshop.ru/43960.html: учебное пособие / Нестеров С. А. - Электрон. текстовые данные. - СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2016. - 322 с. - Режим доступа: http://www.iprbookshop.ru/43960.html

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в ИТКС.	**Практический опыт:** установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам;	Экспертное наблюдение
	Умения: проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации;	
	Знания: способов защиты информации от утечки по техническим каналам с использованием технических средств защиты; основных типов технических средств защиты информации от утечки по техническим каналам; законодательства в области информационной безопасности, структуру государственной системы защиты информации, нормативных актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;	
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в ИТКС.	**Практический опыт:** установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам; проведения технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;	Экспертное наблюдение
	Умения: проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации;	

	Знания: основных типов технических средств защиты информации от утечки по техническим каналам; организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам; порядка и правил ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;	
ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями.	**Практический опыт:** защиты информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;	Экспертное наблюдение
	Умения: проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации;	
	Знания: способов защиты информации от утечки по техническим каналам с использованием технических средств защиты; основных типов технических средств защиты информации от утечки по техническим каналам; методик измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам; порядка и правил ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;	
ПК 3.4. Проводить отдельные работы по физической защите линий связи ИТКС.	**Практический опыт:** проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации.	Экспертное наблюдение
	Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных.	

	Знания: номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам.	

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки**
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	**Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника).	Экспертное наблюдение Экзамен
	Знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте. алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности.	
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной	**Умения:** определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска	Экспертное наблюдение Экзамен

деятельности.	**Знания:** номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	**Умения**: определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития	Экспертное наблюдение Экзамен
	Знания: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	**Умения**: организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами	Экспертное наблюдение Экзамен
	Знания: психология коллектива; психология личности; основы проектной деятельности	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	**Умения:** излагать свои мысли на государственном языке; оформлять документы.	Экспертное наблюдение Экзамен
	Знания: особенности социального и культурного контекста; правила оформления документов.	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	**Умения:** описывать значимость своей профессии Презентовать структуру профессиональной деятельности по профессии (специальности)	Экспертное наблюдение Экзамен
	Знания: сущность гражданско-патриотической позиции Общечеловеческие ценности Правила поведения в ходе выполнения профессиональной деятельности	
ОК 07.Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	**Умения:** соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по профессии (специальности).	Экспертное наблюдение Экзамен
	Знания: правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения**.**	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	**Умения:** применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение	Экспертное наблюдение Экзамен

	Знания: современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности.	