

приложение 1.3
к ОПОП по специальности
10.02.05 Обеспечение информационной
безопасности автоматизированных систем

**РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ**

Добавлено примечание (11): Удалить

СОДЕРЖАНИЕ

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО
МОДУЛЯ**

**3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
«ПМ.03 Защита информации техническими средствами»**

1.1. Цель и планируемые результаты освоения профессионального модуля

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

1.1.1 Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 3	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.
ОК 4	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 5	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 6	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных Российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.
ОК 7	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2 Перечень профессиональных компетенций

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.

1.1.3

В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – 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.
--	--

1.2 Количество часов, отводимое на освоение профессионального модуля

Всего 594 часов

в том числе:

в форме практической подготовки 276 ч

на освоение МДК 468 ч

производственная практика 108 ч

Промежуточная аттестация (экзамен по профессиональному модулю) – 18 ч

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объем профессионального модуля, час.					
			Обучение по МДК, в час.				Практики	
			всего, часов	в том числе			учебная практика, часов	производственная практика, часов
				лабораторных и практических занятий	Самостоятельная работа/консультации	курсовая работа (проект), часов		
ПК 3.1-ПК.3.4 ОК.01 – ОК09	Раздел 1 модуля. Применение технической защиты информации	235	199	44	20/20	–	-	36
ПК 3.5 ОК. 01– ОК.09	Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации	217	181	50	20/20	30	-	36
ПК.3.1-3.5 ОК.01-ОК.09	Раздел 3 модуля. Корпоративная защита от внутренних угроз	124	88	44	10/10	-	-	36
	Экзамен по профессиональному модулю	18	-	–	-	–	–	–

	Bcero:	594	468	138	50/50	30	-	108
--	---------------	------------	------------	-----	-------	----	---	------------

2.2 Тематический план и содержание профессионального модуля

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 модуля. Применение технической защиты информации		235
МДК.03.01 Техническая защита информации		199
Раздел 1. Концепция инженерно-технической защиты информации		
Тема 1.1. Предмет и задачи технической защиты информации	Содержание ТЗ.1 Предмет и задачи технической защиты информации. ТЗ.2 Характеристика инженерно-технической защиты информации как области информационной безопасности. ТЗ.3 Системный подход при решении задач инженерно-технической защиты информации. ТЗ.4 Основные параметры системы защиты информации. ПЗ.1 Решение задач инженерно-технической защиты информации. ПЗ.2 Параметры системы защиты информации	2 2 2 2 2 2
Тема 1.2. Общие положения защиты информации техническими	Содержание ТЗ.5 Задачи и требования к способам и средствам защиты информации техническими средствами. ТЗ.6 Принципы системного анализа проблем инженерно-технической защиты информации. ТЗ.7 Классификация способов и средств защиты информации.	2 2

средствами		2
	ПЗ.3 Средства защиты информации	2
Раздел 2. Теоретические основы инженерно-технической защиты информации		
Тема 2.1. Информация как предмет защиты	Содержание	
	ТЗ.8 Особенности информации как предмета защиты.	2
	ТЗ.9 Свойства информации.	2
	ТЗ.10 Виды, источники и носители защищаемой информации.	2
	ТЗ.11 Демаскирующие признаки объектов наблюдения, сигналов и веществ.	2
	ТЗ.12 Понятие об опасном сигнале.	2
	ТЗ.13 Источники опасных сигналов.	2
	ТЗ.14 Основные и вспомогательные технические средства и системы.	2
	ТЗ.15 Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.4 Содержательный анализ основных руководящих по защите информации.	2
	ПЗ.5 Анализ нормативных документов по защите информации.	2
	ПЗ.6 Анализ методических документов по защите информации.	2

	ПЗ.7 Содержательный анализ основных руководящих документов по противодействию технической разведке.	2
	ПЗ.8 Анализ нормативных документов по противодействию технической разведке.	2
	ПЗ.9 Анализ методических документов по противодействию технической разведке.	2
Тема 2.2. Технические каналы утечки информации	Содержание	
	ТЗ.16 Понятие и особенности утечки информации.	2
	ТЗ.17 Структура канала утечки информации.	2
	ТЗ.18 Классификация существующих физических полей и технических каналов утечки информации.	2
	ТЗ.19 Характеристика каналов утечки информации.	2
	ТЗ.20 Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.10 Оптические каналы утечки информации, их характеристика.	2
ПЗ.11 Акустические каналы утечки информации, их характеристика.	2	
ПЗ.12 Радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	2	
Тема 2.3. Методы и средства технической разведки	Содержание	
	ТЗ.21 Классификация технических средств разведки.	2
	ТЗ.22 Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки.	2
	ТЗ.23 Средства дистанционного съема информации.	2

	Тематика практических занятий и лабораторных работ	
	ПЗ.13 Несанкционированный доступ к информации	2
	ПЗ.14 Оптическая разведка	2
	ПЗ.15 Дистанционный съем информации	2
Раздел 3. Физические основы технической защиты информации		
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание	
	ТЗ.24 Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. ТЗ.25 Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.	2
	ТЗ.26 Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.16,17 Измерение параметров физических полей	2
	ПЗ.18 Утечка информации по цепям электропитания и заземления	2
		2
Тема 3.2. Физические процессы при подавлении опасных сигналов	Содержание	
	ТЗ.27 Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.19 Скрытие речевой информации в каналах связи.	2

	ПЗ.20 Подавление опасных сигналов акустоэлектрических преобразований.	2
Раздел 4. Системы защиты от утечки информации		
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	Содержание	
	ТЗ.28 Технические средства акустической разведки. Непосредственное подслушивание звуковой информации.	2
	ТЗ.29 Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.21,22 Защита от утечки по акустическому каналу	2
		2
Тема 4.2. Системы защиты от утечки информации по проводному каналу	Содержание	
	ТЗ.30 Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов.	2
	Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.23 Негласная запись информации на диктофоны.	2
ПЗ.24 Системы защиты от диктофонов.	2	
Консультации		8

Самостоятельная работа		8
Промежуточная аттестация в форме экзамена		18
Итого за семестр		122
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	Содержание	
	ТЗ.1 Электронные стетоскопы.	2
	ТЗ.2 Лазерные системы подслушивания.	2
	ТЗ.3 Гидроакустические преобразователи.	2
	ТЗ.4 Системы защиты информации от утечки по вибрационному каналу.	2
	ТЗ.5 Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	2
	Тематика практических занятий и лабораторных работ	
ПЗ.1 Защита от утечки по виброакустическому каналу	2	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	Содержание	
	ТЗ.6 Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры.	2
	СР.1 Прослушивание информации от радиозакладок.	2
	ТЗ.7 Приемники информации с радиозакладок.	2
	СР.2 Прослушивание информации о пассивных закладок.	2
	СР.3 Системы защиты от утечки по электромагнитному каналу.	2
		2

	ТЗ.8 Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	
	Тематика практических занятий и лабораторных работ	
	ПЗ.2 Определение каналов утечки ПЭМИН	2
	ПЗ.3 Защита от утечки по цепям электропитания и заземления	2
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	Содержание	
	ТЗ.9 Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.	2
	ТЗ.10 Использование микрофона телефонного аппарата при положенной телефонной трубке.	2
	ТЗ.11 Утечка информации по сотовым цепям связи.	2
	ТЗ.12 Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.4 Системы защиты от утечки информации по телефонному каналу	2
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	Содержание	
	ТЗ.13 Низкочастотное устройство съема информации.	2
	ТЗ.14 Высокочастотное устройство съема информации.	2
	ТЗ.15 Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	2

	Тематика практических занятий и лабораторных работ	
	ПЗ.5 Системы защиты от утечки информации по электросетевому каналу	2
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	Содержание	2
	ТЗ.16 Телевизионные системы наблюдения.	2
	ТЗ.17 Приборы ночного видения.	2
	ТЗ.18 Системы защиты информации по оптическому каналу.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.6 Системы защиты от утечки информации по оптическому каналу	2
Раздел 5. Применение и эксплуатация технических средств защиты информации		
Тема 5.1. Применение технических средств защиты информации	Содержание	
	ТЗ.19 Технические средства для уничтожения информации и носителей информации, порядок применения.	1
	К.1 Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.	2
	К.2 Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.	2
	К.3 Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	2
	ПЗ.7 Применение технических средств защиты информации	2

Тема 5.2. Эксплуатация технических средств защиты информации	Содержание	
	К.4 Этапы эксплуатации технических средств защиты информации.	2
	К.5 Виды, содержание и порядок проведения технического обслуживания средств защиты информации.	2
	К.6 Установка и настройка технических средств защиты информации.	2
	СР.4 Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.	2
	СР.5 Организация ремонта технических средств защиты информации.	2
	СР.6 Проведение аттестации объектов информатизации.	
Тематика практических занятий и лабораторных работ		
ПЗ.8 Эксплуатация технических средств защиты информации	2	
Промежуточная аттестация в форме контрольной работы		-
Итого за семестр		77
Производственная практика ПП.03.01 Техническая защита информации		36
ВСЕГО ПО РАЗДЕЛУ 1		235
Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации		217

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		181
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		
Тема 1.1. Цели и задачи физической защиты объектов информатизации	Содержание	
	ТЗ.1 Характеристики потенциально опасных объектов.	2
	ТЗ.2 Содержание и задачи физической защиты объектов информатизации.	2
	ТЗ.3 Основные понятия инженерно-технических средств физической защиты.	2
	ТЗ.4 Категорирование объектов информатизации.	2
	ТЗ.5 Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.	2
	ТЗ.6 Особенности задач охраны различных типов объектов.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.1 Физическая защита объектов информатизации.	2
	ПЗ.2 Инженерно-технические средства физической защиты.	2
ПЗ.3 Категорирование объектов информатизации.	2	
ПЗ.4 Охрана различных типов объектов.	2	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	Содержание	
	ТЗ.7 Общие принципы обеспечения безопасности объектов.	2
	ТЗ.8 Жизненный цикл системы физической защиты.	2
	ТЗ.9 Принципы построения интегрированных систем охраны.	2

	ТЗ.10 Классификация и состав интегрированных систем охраны.	2
	ТЗ.11 Требования к инженерным средствам физической защиты.	2
	ТЗ.12 Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	2
Тематика практических занятий и лабораторных работ		
	ПЗ.5 Обеспечение безопасности объектов.	2
	ПЗ.6 Интегрированные системы охраны.	2
	ПЗ.7 Инженерные средства физической защиты.	2
	ПЗ.8 Инженерные конструкции, применяемые для защиты информации	2
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	Содержание	
	ТЗ.13 Информационные основы построения системы охранной сигнализации.	2
	ТЗ.14 Назначение, классификация технических средств обнаружения.	2
	ТЗ.15 Построение систем обеспечения безопасности объекта.	2
	ТЗ.16 Периметровые средства обнаружения: назначение, устройство, принцип действия.	2
	ТЗ.17 Объектовые средства обнаружения: назначение, устройство, принцип действия.	2
	Тематика практических занятий и лабораторных работ	
ПЗ. 9-13 Монтаж датчиков пожарной и охранной сигнализации	2,2,2,2,2	
	Содержание	

Тема 2.2. Система контроля и управления доступом	ТЗ.18 Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности.	2	
	ТЗ.19 Особенности построения и размещения СКУД.	2	
	ТЗ.20 Структура и состав СКУД.	2	
	ТЗ.21 Периферийное оборудование и носители информации в СКУД.	2	
	ТЗ.22 Основы построения и принципы функционирования	2	
	ТЗ.23 СКУД. Классификация средств управления доступом.	2	
	ТЗ.24 Средства идентификации и аутентификации.	2	
	К.1 Методы удостоверения личности, применяемые в СКУД.	2	
	К.2 Обнаружение металлических предметов и радиоактивных веществ.	2	
	Тематика практических занятий и лабораторных работ		
	ПЗ.14-15 Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	2,2	
ПЗ.16-17 Рассмотрение принципов устройства, работы и применения средств контроля доступа	2,2		
Тема 2.3. Система телевизионного наблюдения	Содержание		
	К.3 Аналоговые и цифровые системы видеонаблюдения.	2	
	К.4 Назначение системы телевизионного наблюдения.	2	
	СР.1 Состав системы телевизионного наблюдения.	2	
	СР.2 Видеокамеры. Объективы. Термокожухи.	2	

	СР.3 Поворотные системы.	2
	СР.4 Инфракрасные осветители. Детекторы движения.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.18-20 Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	2,2,2
	Промежуточная аттестация в форме контрольной работы	-
	Итого за семестр	104
Тема 2.4. Система сбора, обработки, отображения и документирования информации	Содержание	
	ТЗ.1 Классификация системы сбора и обработки информации.	2
	ТЗ.2 Схема функционирования системы сбора и обработки информации.	2
	ТЗ.3 Варианты структур построения системы сбора и обработки информации.	2
	ТЗ.4 Устройства отображения и документирования информации.	2
	Тематика практических занятий и лабораторных работ	
ПЗ.1,2 Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	2 2	
Тема 2.5 Система воздействия	Содержание	
	ТЗ.5 Назначение и классификация технических средств воздействия.	2
	ТЗ.6 Основные показатели технических средств воздействия.	2
	Тематика практических занятий и лабораторных работ	
	ПЗ.3 Система воздействия	2,2

Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		
Тема 3.1 Применение	Содержание	
инженерно-технических средств физической защиты	К.1 Периметровые и объектовые средства обнаружения, порядок применения.	2
	К.2 Работа с периферийным оборудованием системы контроля и управления доступом.	2
	К.3 Особенности организации пропускного режима на КПП.	2
	К.4 Управление системой телевизионного наблюдения с автоматизированного рабочего места.	2
	К.5 Порядок применения устройств отображения и документирования информации.	2
	К.6 Управление системой воздействия.	2
	Тематика практических занятий и лабораторных работ	
ПЗ.4 Управление системой телевизионного наблюдения с автоматизированного рабочего места.	2	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	Содержание	
инженерно-технических средств физической защиты	СР.1 Этапы эксплуатации.	2
	СР.2 Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.	2
	СР.3,4 Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	2
	СР.5 Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.	2
	СР.6 Организация ремонта технических средств физической защиты.	2

	Тематика практических занятий и лабораторных работ	
	ПЗ.5 Эксплуатация инженерно-технических средств физической защиты	2
Курсовой проект (работа)		30
Примерная тематика курсового проекта (работы)		
<ol style="list-style-type: none"> 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. 		
Промежуточная аттестация в форме защиты курсового проекта (работы)		
Итого за семестр		77
Производственная практика ПП.03.02 Инженерно-технические средства физической защиты объектов информатизации		36
ВСЕГО ПО РАЗДЕЛУ 2		217
Производственная практика профессионального модуля		
Виды работ		
<ol style="list-style-type: none"> 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 съёма и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. 		

РАЗДЕЛ 3. Корпоративная защита от внутренних угроз	124
МДК.03.03 Корпоративная защита от внутренних угроз	88

Раздел 1. Корпоративная защита и информационная безопасность		
Тема 1.1. Корпоративная защита	Содержание	22
	ТЗ.1 Границы собственных знаний, навыков и полномочий.	2
	ТЗ.2 Ситуации, требующие вмешательства службы поддержки.	2
	ТЗ.3 Формирование процессов и процедур аудита ИБ.	2
	ТЗ.4 Состояние корпоративной информации.	2
	К.1 Препятствия реализации проектов по обеспечению корпоративной защиты от внутренних угроз.	2
	К.2 Алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных.	2
	ТЗ.5 Типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации.	2
	ТЗ.6 Роль фильтров при анализе перехваченного трафика.	2
	СР.1,2 Юридические вопросы использования DLP-систем: личная и семейная тайны; тайна связи; специальные технические средства.	2
	СР.3 Практика правоприменения при расследовании инцидентов, связанных с нарушениями режима внутренней информационной безопасности (Post-DLP).	2
		2
		2
	Тематика практических занятий и лабораторных работ	24
	ПЗ.1 Технические ограничения механизма фильтрации, его преимущества и недостатки.	2
	ПЗ.2 Разделы системы корпоративной безопасности, которые используются офицером безопасности в повседневной работе.	2
	ПЗ.3 Технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации.	2

	ПЗ.4 Организационно-технические и правовые основы использования электронного документооборота в информационных системах.	2
	ПЗ.5 Архитектуру и особенности внедрения IDS-технологий.	2
	ПЗ.6,7 Особенности настройки событий агентского мониторинга. Агентские политики DLP.	2
	ПЗ.8 Механизмы диагностики агента, подходы к защите агента.	2
	ПЗ.9 Групповые политики различных ОС.	2
	ПЗ.10,11 Типовой пакет нормативных документов, необходимого для развёртывания и эксплуатации системы корпоративной защиты в организации.	2
	ПЗ.12 Виды типовых отчетных форм о выявленных угрозах и инцидентах.	2
		2
		2
Тема 1.2 Информационная безопасность	Содержание	22
	ТЗ.7 Системы управления учетными данными пользователей	2
	ТЗ.8 Принципы управления жизненным циклом информационных систем	2
	ТЗ.9 Методы планирования своей работы	2
	ТЗ.10 Методы декомпозиции и приоритизации поставленных задач	2
	СР.4 Важность проверки выполненной работы в каждом ее аспекте	2
	ТЗ.11 Современные тенденции в области информационных технологий и в подходах к построению ИТ-инфраструктуры	2
	ТЗ.12 Отраслевые стандарты и системы профессиональных сертификаций	2
	СР.5 Стандарты профессиональной коммуникации при работе в системах поддержки пользователей	2
	К.3,4 Формирование базы знаний	2
	К.5 Применение аналитических навыков для диагностики и устранения неисправностей в работе информационных систем и сетей	2
		2,2

		2
	Тематика практических занятий и лабораторных работ	20
	ПЗ.13 Методы эффективной работы в составе команды	2
	ПЗ.14 Методы демонстрации и презентации материала	2
	ПЗ.15 Поиск информации в открытых источниках и работа с технической документацией	2
	ПЗ.16,17 Формирование корректных, отвечающих требованиям и ограничениям, рекомендаций на основе запросов и потребностей заказчика	2,2
	ПЗ.18,19 Выстраивание эффективного письменного и устного общения на русском и английском языке	2
	ПЗ.20 Точное описание инцидента и документирование решения проблемы	2,2
	ПЗ.21,22 Разработка документации к существующей или проектируемой информационной структуре предприятия	2
		2,2
	Промежуточная аттестация в форме контрольной работы	-
	Итого за семестр	88

Производственная практика ПП.03.03 Корпоративная защита от внутренних угроз	36
Виды работ:	
<ul style="list-style-type: none"> • Создание инструкций и регламентов, учитывающих требования заказчиков • Документирование процесса решения технических проблем • Составление технического паспорта информационной структуры предприятия • Настройка ограничений механизмов фильтрации и оценка их эффективности 	

<ul style="list-style-type: none"> • Настройка событий агентского мониторинга и разработка агентских политик DLP • Диагностика состояния агентов защиты и настройка мер противодействия угрозам • Программирование групповых политик различных операционных систем • Заполнение шаблонов отчетности по обнаруженным инцидентам и угрозам 	
ВСЕГО ПО РАЗДЕЛУ 3	124
<i>Экзамен по профессиональному модулю</i>	18
<i>Всего</i>	<i>594</i>

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

лаборатория «Технических средств защиты информации», оснащенная в соответствии с ОПОП по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

3.2 Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд колледжа имеет печатные и/или электронные образовательные и информационные ресурсы, рекомендованные ФУМО, для использования в образовательном процессе. При формировании библиотечного фонда колледжем выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список, может быть дополнен новыми изданиями.

3.2.1 Основные электронные издания

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518006>.

2. Казарин, О. В. Надежность и безопасность программного обеспечения: учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/515435>.

3. Панарина, М. М. Корпоративная безопасность: система управления рисками и комплаенс в компании: учебное пособие для вузов / М. М. Панарина. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 155 с. — (Высшее образование). — ISBN 978-5-534-16725-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/531591>.

**4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

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 по профессиональному модулю, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной 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 по профессиональному модулю, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной 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 по профессиональному модулю, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ,

		оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной практике
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	тестирование, экзамен по профессиональному модулю, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экзамен по профессиональному модулю, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на производственной практике
ОК.01 Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при

<p>ОК.02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.</p>	<p>- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач</p>	<p>выполнении работ по учебной и производственной практикам экзамен по профессиональному модулю</p>
<p>ОК.03 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.</p>	<p>- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;</p>	
<p>ОК.04 Эффективно взаимодействовать и работать в коллективе и команде.</p>	<p>- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)</p>	
<p>ОК.05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.</p>	<p>- демонстрация грамотности устной и письменной речи, - ясность формулирования и изложения мыслей</p>	
<p>ОК.06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных Российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты</p>	<p>- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик, - соблюдение стандартов антикоррупционного поведения</p>	

антикоррупционного поведения.		
ОК.07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.	<ul style="list-style-type: none"> - эффективное выполнение правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности 	
ОК.08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	- эффективность использования средств физической культуры для сохранения и укрепления здоровья при выполнении профессиональной деятельности.	
ОК.09 Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	