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

2024 г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупненной группы специальностей 10.00.00 Информационная безопасность.

Организация-разработчик: государственное бюджетное профессиональное образовательное учреждение Новосибирской области «Новосибирский профессионально-педагогический колледж».

Разработчики:

ФИО., преподаватель

Рассмотрена и принята на заседании кафедры информационных технологий и дизайна

Протокол № 1 от 29.08.2024 г.

Руководитель кафедры _____ О.Ю.Ануфриева

(подпись)

СОДЕРЖАНИЕ

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	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, применять стандарты антикоррупционного поведения.
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.
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

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	− 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.

1.2 Количество часов, отводимое на освоение профессионального модуля

Всего 961 часов

в том числе в форме практической подготовки 408 часа

Из них на освоение МДК 03.01 742 часа

в том числе самостоятельная работа 101 час

практики, в том числе производственная 180 часов

Промежуточная аттестация 39 часов

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля			Объем профессионального модуля, ак. час.							
		Суммарный объем нагрузки, час.	В т.ч. в форме практ.	Работа обучающихся во взаимодействии с преподавателем							Самостоятельная работа[1]
				Обучение по МДК				Практики		Консультации[2]	
				Всего	В том числе			Учебная	Производственная		
					Практических	Лаборат. и практ. занятий	Курсовых работ (проектов)[3]				
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
ПК 3.1-ПК.3.5 ОК 1– ОК10	**МДК.03.01** Техническая защита информации	**742**	408	**742**	39	408					101
	Производственная практика	**180**							**180**		
	Промежуточная аттестация	**39**									
	Всего:	**961**	408	**742**	**39**	408			**180**		101

[1] Самостоятельная работа в рамках образовательной программы планируется образовательной организацией в соответствии с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием междисциплинарного курса.

[2] Консультации вставляются в случае отсутствия в учебном плане недель на промежуточную аттестацию по модулю.

[3] Данная колонка указывается только для специальностей СПО.

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
МДК.03.01 Техническая защита информации		**742**
Раздел 1. Концепция инженерно-технической защиты информации		637
Тема 1.1 Предмет и задачи технической защиты информации	**Содержание**	**14**
	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.	6
Тема 1.2 Общие положения защиты информации техническими средствами	**Содержание**	4
	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.	8
Раздел 2. Теоретические основы инженерно-технической защиты информации		
Тема 2.1 Информация как предмет защиты	**Содержание**	**184**
	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.	10
	В том числе практических занятий	
	Основные виды угроз информации. Классификация демаскирующих признаков. Содержательный анализ основных руководящих, нормативных и методических документов по	8

	защите информации и противодействию технической разведке.	
Тема 2.2 Технические каналы утечки информации	**Содержание**	**18**
	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.	8
	В том числе практических занятий	
	Содержательный анализ уязвимостей системы. Классификация угроз информационной безопасности. Типовая структура технических каналов утечки информации.	10
Тема 2.3 Методы и средства технической разведки	**Содержание**	**20**
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	10
	В том числе практических занятий	
	Способы и средства технической разведки. Способы и средства обнаружения злоумышленника. Содержательный анализ о возможности оптической разведки и дистанционного съёма информации.	10
Раздел 3. Физические основы технической защиты информации		
Тема 3.1 Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**24**
	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	10
	В том числе практических занятий	
	Определение путей проникновения злоумышленником по каналам побочных электромагнитных излучений и наводок. Работа обнаружителей электромагнитного поля.	14

	Измерение параметров физических полей. Составление комплексной системы защиты.	
Тема 3.2 Физические процессы при подавлении опасных сигналов	**Содержание**	**26**
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	10
	В том числе практических занятий	
	Способы скрытия речевой информации. Способы подавления опасных сигналов акустоэлектрических преобразований. Содержательный анализ процесса экранирования. Выявление плюсов и недостатков. Моделирование угроз информации	16
Раздел 4. Системы защиты от утечки информации		
Тема 4.1 Системы защиты от утечки информации по акустическому каналу	**Содержание**	**18**
	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.	12
	В том числе практических занятий	
	Содержательный анализ средств акустической разведки. Работа остронаправленных микрофонов. Защита от утечки по акустическому каналу	6
Тема 4.2 Системы защиты от утечки информации по проводному каналу	**Содержание**	**24**
	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.	14
	В том числе практических занятий	
	Защита информации от диктофонов. Обнаружители и подавители диктофонов.	10
Промежуточная аттестация по МДК.03.01		**2**
Тема 4.3 Системы	**Содержание**	**24**
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи.	10

защиты от утечки информации по вибрационному каналу	Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	
	В том числе практических занятий	
	Содержательный анализ угрозы лазерного подслушивания. Системы защиты информации от утечки по вибрационному каналу. Защита от утечки по виброакустическому каналу	14
Тема 4.4 Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	**33**
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации с пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	14
	В том числе практических занятий	
	Формирование системы зашиты от прослушивания радиотелефонов. Формирование системы защиты от радиозакладок. Защита от утечки по цепям электропитания и заземления Определение каналов утечки ПЭМИН	19
Тема 4.5 Системы защиты от утечки информации по телефонному каналу	**Содержание**	**30**
	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.	12
	В том числе практических занятий	
	Анализаторы телефонных линий. Утечка информации по сотовым цепям связи. Формирование системы защиты от утечки информации по телефонному каналу.	12
	Самостоятельная работа	
	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.	6

Тема 4.6 Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**20**
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	6
	В том числе практических занятий	
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Формирование системы защиты от утечки информации по электросетевому каналу.	10
	Самостоятельная работа	
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации.	4
Тема 4.7 Системы защиты от утечки информации по оптическому каналу	**Содержание**	**20**
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	6
	В том числе практических занятий	
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	12
	Самостоятельная работа	
	Системы защиты информации по оптическому каналу.	2
Раздел 5. Применение и эксплуатация технических средств защиты информации		
Тема 5.1 Применение технических средств защиты информации	**Содержание**	**28**
	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. 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.	8
	В том числе практических занятий	
	Способы и правила уничтожения информации и её носителей.	18

	Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений. Содержательный анализ применения технических средств защиты информации.	
	Самостоятельная работа	
	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	2
Тема 5.2 Эксплуатация технических средств защиты информации	**Содержание**	**30**
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. 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.	10
	В том числе практических занятий	
	Этапы эксплуатации технических средств защиты информации. Установка и настройка возможных технических средств защиты информации. Правила проведения технического обслуживания средств защиты информации. Проведение аттестации автоматизированного рабочего места (АРМ) Система устранения отказов и восстановление работоспособности технических средств защиты информации.	20
Промежуточная аттестация по МДК.03.01		**2**
Виды самостоятельной работы 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 лабораторно-практических работ, отчетов к их защите.		
Раздел 6. Применение инженерно-технических средств физической защиты объектов информатизации		
Тема 6.1 Цели и задачи физической защиты объектов	**Содержание**	**26**
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Категорирование объектов информатизации. Особенности задач	8

информатизации	охраны различных типов объектов.	
	В том числе практических занятий	
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Категорирование объектов информатизации.	14
	Самостоятельная работа	
	Основные понятия инженерно-технических средств физической защиты. Модель нарушителя и возможные пути, и способы его проникновения на охраняемый объект.	4
Тема 6.2 Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**30**
	Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты.	6
	В том числе практических занятий	
	Общие принципы обеспечения безопасности объектов. Принципы построения интегрированных систем охраны. Содержательный анализ требований к инженерным средствам физической защиты.	16
	Самостоятельная работа	
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	8
Раздел 7. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 7.1 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**	**28**
	Информационные основы построения системы охранной сигнализации.	2
	В том числе практических занятий	
	Классификация технических средств обнаружения. Содержательный анализ средств обнаружения: назначение, устройство, принцип действия. Правила монтажа датчиков пожарной и охранной сигнализации.	16
	Самостоятельная работа	
	Информационные основы построения системы охранной сигнализации.	10

	Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	
Тема 7.2 Система контроля и управления доступом	**Содержание**	**38**
	В том числе практических занятий	
	Основные виды средств контроля доступа и их характеристика. Содержательный анализ особенностей построения и размещения средств контроля доступа. Рассмотрение принципов устройства, работы и применения средств контроля доступа. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя. Основные методы удостоверения личности.	20
	Самостоятельная работа	
	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.	18
Тема 7.3 Система телевизионного наблюдения	**Содержание**	**32**
	Детекторы движения.	2
Промежуточная аттестация по МДК.03.01		**2**
	В том числе практических занятий	
	Содержательный анализ аналоговых и цифровых систем видеонаблюдения. Состав системы телевизионного наблюдения. Способ создания системы видеонаблюдения.	18

	Принцип работы детекторов движения.	
	Самостоятельная работа	
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители.	12
Тема 7.4 Система сбора, обработки, отображения и документирования информации	**Содержание**	**38**
	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.	8
	В том числе практических занятий	
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	14
	Самостоятельная работа	
	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.	16
Тема 7.5 Система воздействия	**Содержание**	**26**
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	4
	В том числе практических занятий	
	Назначение и классификация технических средств воздействия. Содержательный анализ показателей технических средств воздействия. Формирования системы воздействия на информацию.	16
	Самостоятельная работа	
	Назначение и классификация технических средств воздействия.	6

	Основные показатели технических средств воздействия.	
Раздел 8. Применение и эксплуатация инженерно-технических средств физической защиты		
Тема 8.1 Применение инженерно-технических средств физической защиты	**Содержание**	**36**
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	10
	В том числе практических занятий	
	Анализ особенностей организации пропускного режима на КПП. Формирование системы порядка устройств отображения и документирования информации. Принципы управления системой воздействия.	16
	Самостоятельная работа	
	Периметровые и объектовые средства обнаружения, порядок применения. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	10
Тема 8.2 Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**30**
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. 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.	9
	В том числе практических занятий	
	Составление этапов эксплуатации инженерно-технических средств физической защиты. Способы установки и настройки периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Способы устранения отказов и восстановления работоспособности технических средств физической защиты.	18

	Самостоятельная работа	
	Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	3
Раздел 9. Корпоративная защита от внутренних угроз		**105**
Тема 9.1 Технологии политики безопасности в системе корпоративной защиты информации от внутренних угроз	**Содержание**	**16**
	Принципы и технологии обеспечения корпоративной защиты от внутренних угроз.	8
	Регламентирующие документы в области безопасности информационных систем.	
	Подходы к построению сети и сетевые устройства в системе корпоративной защиты. Версии DLP систем.	
	Особенности работы основных гипервизоров VirtualBox, VMWare Workstation, Microsoft HyperV и др.	
	В том числе практических занятий	**8**
	Схема развертывания DLP системы.	2
	Запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров.	2
	Конфигурация сетевой инфраструктуры: настроить хост-машину, сетевое окружение, виртуальные машины и др.	2
	Проверка работоспособности сети и сетевых устройств в виртуальной среде.	2
Тема 9.2 Установка и конфигурирование компонентов DLP системы	**Содержание**	**39**
	Компоненты системы корпоративной защиты от внутренних угроз.	8
	ПО для защиты от утечек типа InfoWatch Traffic Monitor.	
	Серверная компонента для защиты рабочих станций корпоративной среды InfoWatch Device Monitor.	
	Навыки системного администрирования в ОС Windows Server и Linux Red Hat Enterprise.	
	В том числе практических занятий	**32**
	Установка и конфигурирование компонентов DLP системы. Меры предосторожности.	2
	Установка агентской части СКЗ от внутренних угроз InfoWatch Traffic Monitor.	4
	Установка сервера СУБД Oracle/ PostgreSQL.	2
	Установка и настройка базы данных.	4
	Настройка ПО InfoWatch Traffic Monitor.	4
	Установка ПО серверной компоненты СКЗ от ВУ InfoWatch Device Monitor.	4

	Настройка InfoWatch Device Monitor и Crawler.	4
	Запуск системы, проверка функциональности настроек целевой сетевой инфраструктуре.	4
	Проверка работоспособности DLP системы. Контрольные проверки. Устранение неисправностей.	2
	Провести имитацию процесса утечки конфиденциальной информации в системе.	2
Тема 9.3 Технологии агентского мониторинга	**Содержание**	**22**
	Методы мониторинга и аудита, выявления угроз информационной безопасности АС.	8
	Разработка и применение политики агентского мониторинга для работы с носителями и устройствами.	
	Основные направления обеспечения защиты от НСД и несанкционированного копирования информации.	
	Администрирование системы корпоративной защиты информации.	
	В том числе практических занятий	**14**
	Управление доступом пользователей. Защита входа в систему.	2
	Выявление потоков передачи данных и возможные каналы утечки информации.	2
	Разработка политики агентского мониторинга для работы с носителями, устройствами и файлами.	2
	Контроль печати конфиденциальной информации.	2
	Конфигурирование СКЗ при получении теневых копий.	2
	Мониторинг работы пользователей. Настройка регистрации событий в СКЗИ.	2
	Создание регулярных выражений.	2
Тема 9.4 Разработка политик безопасности, анализ выявленных инцидентов	**Содержание**	**28**
	Разработка и модификация политики безопасности для перекрытия каналов передачи данных и возможных инцидентов.	**5**
	Защита системы с помощью цифровых сертификатов.	
	Технологии управления системы корпоративной защиты информации в IWTM.	
	В том числе практических занятий	**22**
	Создание и разрешение инцидентов в IWTM, используя Генератор трафика и инцидентов.	4
	Разработка политики для контроля трафика, выявления и блокирования инцидентов безопасности.	4
	Защита системы с помощью цифровых сертификатов.	4
	Анализ сложных, комплексных ситуаций и проблем при защите от внутренних угроз.	4
	Анализ работы серверной части СКЗ. Управление режимом потоков.	4

	Работа с интерфейсом управления системы корпоративной защиты информации IWTM.	2
Виды самостоятельной работы при изучении 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 лабораторно-практических работ, отчетов к их защите. Определение задач работы, изучение литературных источников, проведение исследования.		**101**
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 съёма и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.		**180**
Промежуточная аттестация		**39**
Всего		**961**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 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:

рабочие места студентов, оборудованные персональными компьютерами;

лабораторные учебные макеты;

аппаратные средства аутентификации пользователя;

средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок;

средства измерения параметров физических полей;

стенд физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов;

рабочее место преподавателя;

учебно-методическое обеспечение модуля;

интерактивная доска, комплект презентаций.

В условиях дистанционного обучения:

- инструктаж и выдача задания производится в форме телеконференции в программе Zoom;
- вся необходимая документация высылается по электронной почте;
- обратная связь и консультации осуществляются в Moodle и по электронной почте;
- зачет и экзамен осуществляется в форме телеконференции в программе Zoom.

3.2 Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендованные ФУМО, для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации 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 печатные 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 (дата обращения: 26.09.2023).

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 (дата обращения: 26.09.2023).

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 (дата обращения: 26.09.2023).

3.2.2 Дополнительные 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 июня1995 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 недекларированных 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 2006г.

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.

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» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru

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 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

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 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 3.5 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 квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на 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 выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	– использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция	

	результатов собственной работы	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик	
ОК 09. Использовать информационные технологии в профессиональной деятельности	- эффективность использования информационно-коммуникационных технологий в	

	профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	
ЛР 13-21	Выполнение работ в соответствии с установленными регламентами с соблюдением правил безопасности труда, санитарными нормами	экспертное наблюдение выполнения практических работ