МИНИСТЕРСТВО ОБРАЗОВАНИЯ АРХАНГЕЛЬСКОЙ ОБЛАСТИ
Государственное автономное профессиональное образовательное
учреждение Архангельской области
«Архангельский политехнический техникум»
(ГАПОУ АО «Архангельский политехнический техникум»)

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной
работе
_____ А.В. Афанасьева
«22» января 2024 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.05 Техническое обслуживание программно-аппаратных средств защиты информации в компьютерных сетях

ОПОП специальности 25.02.08 Эксплуатация беспилотных авиационных систем

Уровень образования – основное общее

Преподаватель Мамонова Наталья Владимировна

Распределение часов	Количество часов						Промежуточная аттестация без взаимодействия с преподавателем	Вид промежуточной аттестации
	всего	в т.ч. на теорию	в т.ч. на лаб-практич. занятия	в т.ч. на практику	в т.ч. на самостоятельную работу	в т.ч. на промежуточную аттестацию (во взаимодействии с преподавателем)		
на всю дисциплину по учебному плану	288	48	40	180	20		12	Э, дз, эк
на 1 семестр								
на 2 семестр								
на 3 семестр								
на 4 семестр								
на 5 семестр								
на 6 семестр								
на 7 семестр	108	48	40		20		12	Э
на 8 семестр				180				Дз, эк

Программа профессионального модуля ПМ.05 Техническое обслуживание программно-аппаратных средств защиты информации в компьютерных сетях разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по специальности 25.02.08 Эксплуатация беспилотных авиационных систем, входящей в состав укрупненной группы специальностей 25.00.00 Аэронавигация и эксплуатация авиационной и ракетно-космической техники, утвержденного приказом Министерства просвещения Российской Федерации от 09 января 2023 года № 2

Организация-разработчик: ГАПОУ АО «Архангельский политехнический техникум»

Разработчики:

Мамонова М.В., преподаватель _____
Ф.И.О., ученая степень, звание, должность подпись

Рассмотрено и одобрено на заседании ПЦК преподавателей и мастеров производственного обучения сферы строительства, машиностроения и наземного транспорта
Протокол № 5 от «15» января 2024 г.

Председатель Машанова М.В. _____
подпись

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ПМ.05 Техническое обслуживание программно-аппаратных средств защиты информации в компьютерных сетях»

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен освоить вид деятельности техническое обслуживание программно-аппаратных средств защиты информации в компьютерных сетях и соответствующие ему общие компетенции и профессиональные компетенции.

1.1.1. Перечень общих компетенций и личностных результатов

Код	Наименование общих компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях;
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2. Перечень профессиональных компетенций

Код	**Наименование вида деятельности и профессиональных компетенций**
ВД 5	Техническое обслуживание программно-аппаратных средств защиты информации в компьютерных сетях
ПК 5.1.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 5.2	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 5.3	Организовывать отдельные работы по физической защите объектов информатизации
ПК 5.4	Использовать автоматизированные информационные системы (АИС) для различных проектов.
ПК 5.5	Определять возможные каналы утечки информации и выбирать средства для их устранения и защиты.
ПК 5.6	Отслеживать и использовать новейшие технологии защиты информации.
ПК 5.7	Отслеживать изменения требований и стандартов, относящихся к программно-аппаратным средствам защиты информации со стороны законодательства, ФСО и ФСБ.

1.1.3. В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт	- 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 защит;
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 математический аппарат для выполнения криптографических преобразований; - использовать типовые программные криптографические средства, в том числе электронную подпись.
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; - 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 часов 288 часов

Из них *максимальная учебная нагрузка 288 часов*

на освоение МДК 108 часов

(*в том числе*) самостоятельная работа *20 часов*

практики, в том числе учебная 36 часов

производственная 144 часа

Промежуточная аттестация в форме экзамена квалификационного

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Объем профессионального модуля, ак. час.									
		Суммарный объем нагрузки, час. *(МДК, практики и самостоятельная работа)*	В т.ч. в форме практ. подготовки	Работа обучающихся во взаимодействии с преподавателем							Самостоятельная работа
				Обучение по МДК				Практики		Консультации	
				Всего	В том числе			Учебная	Производственная		
					Промежут. аттест.	Лаборат. и практ. занятий	Курсовых работ (проектов)				
1	*2*	*3*	*4*	***5***	*6*	*7*	*8*	***9***	***10***	***11***	***12***
ПК 5.1-5.7 ОК 01-09	МДК.01.01 Концепция инженерно-технической защиты информации	**36**		**36**	Э*	10	-			-	8
	МДК.01.02 Подсистема защиты современных операционных систем	**72**		**72**	Э*	30				-	12
	Учебная практика	**72**	36					**36**			
	Производственная практика	**144**	*144*						**144**		
	Всего:	***288***	***180***	***108***		***40***	**-**	***36***	***144***	**-**	20

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Номер учебного занятия	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект) *(если предусмотрены)*	Объем, час.	Коды ПК, ОК и личностных результатов, формированию которых способствует элемент программы
1	**2**	**3**	**4**	**5**
МДК.05.01 Концепция инженерно-технической защиты информации			**36**	ПК 5.1-5.7 ОК 01-09
Тема 1. Общие положения защиты информации техническими средствами		**Содержание учебного материала**	**6**	
	1	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.	2	
	2	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации.	2	
	3	**Самостоятельная работа** Классификация способов и средств защиты информации.	2	
Тема 2. Информация как предмет защиты		**Содержание учебного материала**	**6**	
	4	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.	2	
	5	Основные и вспомогательные технические средства, и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	2	

	6	**Практическое занятие № 1** Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	2	
Тема 3. Технические каналы утечки информации		**Содержание учебного материала**	**6**	
	7	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации.	2	
	8	**Самостоятельная работа** Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	2	
	9	**Практическое занятие № 2** Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации	2	
Тема 4. Методы и средства технической разведки		**Содержание учебного материала**	**6**	
	10	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации.	2	
	11	Средства и возможности оптической разведки. Средства дистанционного съема информации	2	
	12	**Практическое занятие № 3** Модель несанкционированного доступа. Дистанционный съем информации	2	
Тема 5. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок		**Содержание учебного материала**	**8**	
	13	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок..	2	
	14	**Самостоятельная работа** Физические явления, вызывающие утечку информации по цепям электропитания и заземления	2	
	15	**Самостоятельная работа** Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	2	
	16	**Практическое занятие № 4** Измерение параметров физических полей	2	
Тема 6.		**Содержание учебного материала**	**4**	
	17	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление	2	

Физические процессы при подавлении опасных сигналов	**18**	**Практическое занятие № 5** Скрытие речевой информации. Подавление опасных сигналов	2	
Промежуточная аттестация в форме экзамена*				
МДК.05.02 Подсистема защиты современных операционных систем			**72**	ПК 5.1-5.7 ОК 01-09
Тема 1. Системы защиты от утечки информации по акустическому каналу		**Содержание учебного материала**	**6**	
	1	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами.	2	
	2	Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	2	
	3	**Практическое занятие № 1** Защита от утечки по акустическому каналу	2	
Тема 2. Системы защиты от утечки информации по проводному каналу		**Содержание учебного материала**	**8**	
	4	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны.	2	
	5	Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	2	
	6	**Практическое занятие № 2** Системы защиты от микрофонов.	2	
	7	**Практическое занятие № 3** Защита от несанкционированного доступа по проводному каналу	2	
Тема 3. Системы защиты от утечки информации по вибрационному каналу		**Содержание учебного материала**	**6**	
	8	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи.	2	
	9	Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	2	
	10	**Практическое занятие № 4** Защита от утечки по виброакустическому каналу	2	
Тема 4.		**Содержание учебного материала**	**8**	

Системы защиты от утечки информации по электромагнитному каналу	**11**	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок.	2	
	12	Прослушивание информации о пассивных закладках. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	2	
	13	**Практическое занятие № 5** Определение каналов утечки ПЭМИН	2	
	14	**Практическое занятие № 6** Защита от утечки по цепям электропитания и заземления	2	
Тема 5. Системы защиты от утечки информации по телефонному каналу		**Содержание учебного материала**	**8**	
	15	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке.	2	
	16	Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	2	
	17	**Практическое занятие № 7** Методы съема информации за счет непосредственного подключения к телефонной линии.	2	
	18	**Практическое занятие № 8** Защита информации от утечки по сотовым цепям связи.	2	
Тема 6. Системы защиты от утечки информации по электросетевому каналу		**Содержание учебного материала**	**6**	
	19	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации.	2	
	20	Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	2	
	21	**Практическое занятие № 9** Разночастотное устройство съема информации	2	
Тема 7. Системы защиты от утечки информации по оптическому каналу		**Содержание учебного материала**		
	22	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.		
	23	**Практическое занятие № 10** Защита информации по оптическому каналу		
Тема 8.		**Содержание учебного материала**		

Применение технических средств защиты информации	**24**	Технические средства для уничтожения информации и носителей информации, порядок применения		
	25	Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.		
	26	**Практическое занятие № 11** Уничтожения информации и носителей информации		
	27	**Практическое занятие № 12** Защита информации в условиях применения мобильных устройств.		
Тема 9. Измерение ПЭМИН		**Содержание учебного материала**		
	28	**Самостоятельная работа** Проведение измерений параметров побочных электромагнитных излучений. Проведение измерение наводок.		
	29	**Самостоятельная работа** Проведение аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами		
	30	**Практическое занятие № 13** Измерение ПЭМИН и наводок		
	31	**Практическое занятие № 14** Измерение параметров фоновых шумов.		
Тема 10. Эксплуатация технических средств защиты информации		**Содержание учебного материала**		
	32	**Самостоятельная работа** Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.		
	33	**Самостоятельная работа** Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.		
Тема 11. Аттестация объектов информатизации		**Содержание учебного материала**		
	34	**Самостоятельная работа** Стандарты по проведению аттестации. Организационно-технические меры для аттестации		
	35	**Самостоятельная работа** Проведение аттестации объектов информатизации. Заключение аттестационных испытаний		
	36	**Практическое занятие № 15** Проведение аттестации объектов информатизации		
Промежуточная аттестация в форме экзамена*				
Учебная практика **Виды работ**			**72**	ПК 5.1-5.7 ОК 01-09

- Измерение параметров физических полей. - Определение каналов утечки ПЭМИН. - Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. - Установка и настройка технических средств защиты информации. - Проведение измерений параметров побочных электромагнитных излучений и наводок. - Проведение аттестации объектов информатизации. - 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. - Разработка основной документации по инженерно-технической защите информации. Промежуточная аттестация в форме дифференцированного зачета*				
Производственная практика **Виды работ** - Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; - Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; - Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам; - Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации Промежуточная аттестация в форме дифференцированного зачета*				ПК 5.1-5.7 ОК 01-09
		Всего (включая самостоятельную работу), час.	**288**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация программы предполагает наличие учебных кабинетов – лекционные аудитории с мультимедийным оборудованием; лаборатории «Технических средств защиты информации». Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест - 25, рабочее место преподавателя, проектор, персональный компьютер, комплект презентаций.

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

- рабочие места обучающихся, 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.

3.2. Информационное обеспечение реализации программы

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

3.2.1 Основные печатные источники:

1. Зайцев, А.П. Технические средства и методы защиты информации. / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. - 7-е изд., испр. 2021.

2. Пеньков, Т.С. Основы построения технических систем охраны периметров. Учебное пособие. / Т.С. Пеньков. - М. 2019.

3. Новиков, В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб. пособие. / В.К. Новиков. – М.: МИЭТ, 2020. – 172 с.

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

5. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие. / М.А. Иванов, И.В. Чугунков. - Москва: МИФИ, 2018.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

6. Мельников, В.П. Информационная безопасность и защита информации. / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Академия, - 336 с. – 2019

7. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях. / В.Ф. Шаньгин. - Изд-во: ДМК Пресс, - 2017

8. Каторин, Ю.Ф. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2018. – 416 с.

3.2.2. Дополнительные печатные источники:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об

утверждении перечня сведений конфиденциального характера».

8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 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 2006 г.

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

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

3.2.3. Периодические издания:

1. Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

2. Защита информации. Инсайд: Информационно-методический журнал

3. Информационная безопасность регионов: Научно-практический журнал

4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/

5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

3.2.4. Электронные источники:

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

Справочно-правовая система «Консультант Плюс» www.consultant.ru

Справочно-правовая система «Гарант» » www.garant.ru

Федеральный портал «Российское образование www.edu.ru

Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

Российский биометрический портал www.biometrics.ru

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

Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 5.1. 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 Оценка результатов выполнения тестовых заданий Практическая работа
ПК 5.2. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Тестирование Оценка результатов выполнения тестовых заданий Практическая работа

ограниченного доступа.		
ПК 5.3. 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 Оценка результатов выполнения тестовых заданий Практическая работа
ПК 5.4. Использовать автоматизированные информационные системы (АИС) для различных проектов.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Тестирование Оценка результатов выполнения тестовых заданий Практическая работа
ПК 5.5. Определять возможные каналы утечки информации и выбирать средства для их устранения и защиты.	Демонстрировать знания и умения в поиске и нахождении возможных каналов утечки информации в автоматизированных системах, выполнять подбор соответствующих средств для их устранения	Тестирование Оценка результатов выполнения тестовых заданий Практическая рабо
ПК 5.6. Отслеживать и использовать новейшие технологии защиты информации	Демонстрировать умения и практические навыки в использовании, установке и настройке новейших программных средств в области защиты информации	Тестирование Оценка результатов выполнения тестовых заданий Практическая рабо
ПК 5.7. Отслеживать изменения требований и стандартов, относящихся к программно-аппаратным средствам защиты информации со стороны законодательства, ФСО и ФСБ.	Демонстрировать знания по изменению стандартов, относящихся к программно-аппаратным средствам защиты информации.	Тестирование Оценка результатов выполнения тестовых заданий Практическая рабо
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 наблюдения за деятельностью обучающихсяв процессе освоения образзевательной программы. Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	использование различных источников, включая электронные ресурсы, медиа ресурсы, Интернет- ресурсы, периодические издания по специальности для решения профессиональных задач	

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях	демонстрация ответственности за принятые решения обоснованность самоанализа и коррекция результатов собственной работы;	производственой практикам. Экзамен квалификационный
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	- 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 Российской Федерации 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, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства,	эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих технологий	

эффективно действовать в чрезвычайных ситуациях		
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	эффективность использования средств физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	Эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке	
Промежуточная аттестация в форме экзамена квалификационного		