

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Пашнанов Эрдне Лиджиев
Должность: И.о. директора филиала
Дата подписания: 31.07.2024 09:37:20
Уникальный программный ключ:
f29e48b9891aa9797b1ae9fac0693fa267ac161d

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»**

КАЛМЫЦКИЙ ФИЛИАЛ



УТВЕРЖДАЮ
Директор филиала
Э.Л. Пашнанов

« 1 » 06 2022г.

**РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

03 Защита информации техническими средствами

10.02.05 Обеспечение информационной безопасности

автоматизированных систем



квалификация – техник по защите информации


Элиста, 2022 г.


ОДОБРЕНА
Предметно – цикловой комиссией
естественнонаучных и
математических дисциплин

Разработана на основе
Федерального образовательного
стандарта среднего
профессионального образования по
специальности 10.02.05
Обеспечение информационной
безопасности автоматизированных
систем

Протокол № 10
От « 19 » 04 2022 г.

председатель предметно-цикловой комиссии
Катрикова Ц.Ю. / 
начальник учебного-методического
отдела
 Н.С. Бамбушева

Составители:  Пипенко В.В., высшая квалификационная
категория, преподаватель Калмыцкий филиал
ФГБОУ ИВО «Московский государственный
гуманитарно-экономический университет»

Рецензенты:  Лиджи-Гаряев Б.Б., высшая квалификационная
категория, преподаватель Калмыцкий филиал
ФГБОУ ИВО «Московский государственный
гуманитарно-экономический университет»



Агеев С.С., Ведущий администратор базы
данных КУ РК «Центр учета и отчетности в
организациях государственного сектора

РЕЦЕНЗИЯ

на рабочую программу профессионального модуля
ПМ.03 Защита информации техническими средствами
по специальности 10.02.05 Обеспечение информационной безопасности
автоматизированных систем, разработанную преподавателем Калмыцкого филиала
ФГБОУ ИВО «Московский государственный гуманитарно-экономический университет»
Пипенко В.В.

Представленная рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами разработана в соответствии с требованиями Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Структура рабочей программы соответствует структуре примерных программ профессиональных модулей среднего профессионального образования.

Рецензируемая рабочая программа профессионального модуля имеет чёткую структуру и включает все необходимые компоненты.

В общей характеристике рабочей программы раскрываются цели и задачи сформулированы цели и планируемые результаты освоения профессионального модуля.

Объём профессионального модуля, виды учебной работы, тематический план и содержание профессионального модуля раскрывают структуру и содержание профессионального модуля. Указанные объём часов обязательной аудиторной учебной нагрузки, практических занятий обучающихся и форма промежуточной аттестации соответствуют учебному плану.

В тематическом плане и содержании профессионального модуля раскрывается последовательность изучения разделов и тем программы, показывается распределение учебных часов по разделам, темам. Дидактические единицы, отраженные в содержании учебного материала, направлены на качественное усвоение учебного материала. Для приобретения практических навыков и повышения уровня знаний предусмотрены практические занятия.

Условия реализации профессионального модуля определяют требования к необходимому материально-техническому обеспечению к оборудованию учебной лаборатории и техническим средствам обучения.

Информационное обеспечение обучения содержит современный перечень основных печатных источников, дополнительных печатных источников и электронных источников.

Контроль и оценка результатов освоения профессионального модуля содержит код и наименование профессиональных и общих компетенций, критерии оценки, и методы оценки результатов обучения, которые осуществляются преподавателем в процессе проведения различных форм учебных занятий.

Рецензируемая рабочая программа рекомендуется для реализации в образовательном процессе.

Рецензент

С.С. Агеев, ведущий администратор базы данных КУ РК
«Центр учета и отчетности в организациях
государственного сектора»

РЕЦЕНЗИЯ

на рабочую программу профессионального модуля
ПМ.03 Защита информации техническими средствами
по специальности 10.02.05 Обеспечение информационной безопасности
автоматизированных систем, разработанную преподавателем Калмыцкого филиала
ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет»
Пипенко В.В.

Представленная рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами разработана в соответствии с требованиями Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Структура рабочей программы соответствует структуре примерных программ профессиональных модулей среднего профессионального образования.

Рецензируемая рабочая программа профессионального модуля имеет чёткую структуру и включает все необходимые компоненты.

В общей характеристике рабочей программы раскрываются цели и задачи сформулированы цели и планируемые результаты освоения профессионального модуля.

Объём профессионального модуля, виды учебной работы, тематический план и содержание профессионального модуля раскрывают структуру и содержание профессионального модуля. Указанные объём часов обязательной аудиторной учебной нагрузки, практических занятий обучающихся и форма промежуточной аттестации соответствуют учебному плану.

В тематическом плане и содержании профессионального модуля раскрывается последовательность изучения разделов и тем программы, показывается распределение учебных часов по разделам, темам. Дидактические единицы, отраженные в содержании учебного материала, направлены на качественное усвоение учебного материала. Для приобретения практических навыков и повышения уровня знаний предусмотрены практические занятия.

Условия реализации профессионального модуля определяют требования к необходимому материально-техническому обеспечению к оборудованию учебной лаборатории и техническим средствам обучения.

Информационное обеспечение обучения содержит современный перечень основных печатных источников, дополнительных печатных источников и электронных источников.

Контроль и оценка результатов освоения профессионального модуля содержит код и наименование профессиональных и общих компетенций, критерии оценки, и методы оценки результатов обучения, которые осуществляются преподавателем в процессе проведения различных форм учебных занятий.

Рецензируемая рабочая программа рекомендуется для реализации в образовательном процессе.

Рецензент



Лиджи-Гаряев Б.Б., высшая квалификационная категория, преподаватель
Калмыцкий филиал ФГБОУ ИВО «Московский государственный
гуманитарно-экономический университет»

РЕЦЕНЗИЯ
на рабочую программу профессионального модуля
ПМ.03 Защита информации техническими средствами
по специальности 10.02.05 Обеспечение информационной безопасности
автоматизированных систем, разработанную преподавателем Калмыцкого филиала
ФГБОУ ИВО «Московский государственный гуманитарно-экономический университет»
Пипенко В.В.

Представленная рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами разработана в соответствии с требованиями Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Структура рабочей программы соответствует структуре примерных программ профессиональных модулей среднего профессионального образования.

Рецензируемая рабочая программа профессионального модуля имеет чёткую структуру и включает все необходимые компоненты.

В общей характеристике рабочей программы раскрываются цели и задачи сформулированы цели и планируемые результаты освоения профессионального модуля.

Объём профессионального модуля, виды учебной работы, тематический план и содержание профессионального модуля раскрывают структуру и содержание профессионального модуля. Указанные объём часов обязательной аудиторной учебной нагрузки, практических занятий обучающихся и форма промежуточной аттестации соответствуют учебному плану.

В тематическом плане и содержании профессионального модуля раскрывается последовательность изучения разделов и тем программы, показывается распределение учебных часов по разделам, темам. Дидактические единицы, отраженные в содержании учебного материала, направлены на качественное усвоение учебного материала. Для приобретения практических навыков и повышения уровня знаний предусмотрены практические занятия.

Условия реализации профессионального модуля определяют требования к необходимому материально-техническому обеспечению к оборудованию учебной лаборатории и техническим средствам обучения.

Информационное обеспечение обучения содержит современный перечень основных печатных источников, дополнительных печатных источников и электронных источников.

Контроль и оценка результатов освоения профессионального модуля содержит код и наименование профессиональных и общих компетенций, критерии оценки, и методы оценки результатов обучения, которые осуществляются преподавателем в процессе проведения различных форм учебных занятий.

Рецензируемая рабочая программа рекомендуется для реализации в образовательном процессе.

Рецензент



С.С. Агеев, ведущий администратор базы данных КУ РК
«Центр учета и отчетности в организациях
государственного сектора»

РЕЦЕНЗИЯ

на рабочую программу профессионального модуля
ПМ.03 Защита информации техническими средствами
по специальности 10.02.05 Обеспечение информационной безопасности
автоматизированных систем, разработанную преподавателем Калмыцкого филиала
ФГБОУИ ВО «Московский государственный гуманитарно-экономический университет»
Пипенко В.В.

Представленная рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами разработана в соответствии с требованиями Федерального государственного образовательного стандарта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Структура рабочей программы соответствует структуре примерных программ профессиональных модулей среднего профессионального образования.

Рецензируемая рабочая программа профессионального модуля имеет чёткую структуру и включает все необходимые компоненты.

В общей характеристике рабочей программы раскрываются цели и задачи сформулированы цели и планируемые результаты освоения профессионального модуля.

Объём профессионального модуля, виды учебной работы, тематический план и содержание профессионального модуля раскрывают структуру и содержание профессионального модуля. Указанные объём часов обязательной аудиторной учебной нагрузки, практических занятий обучающихся и форма промежуточной аттестации соответствуют учебному плану.

В тематическом плане и содержании профессионального модуля раскрывается последовательность изучения разделов и тем программы, показывается распределение учебных часов по разделам, темам. Дидактические единицы, отраженные в содержании учебного материала, направлены на качественное усвоение учебного материала. Для приобретения практических навыков и повышения уровня знаний предусмотрены практические занятия.

Условия реализации профессионального модуля определяют требования к необходимому материально-техническому обеспечению к оборудованию учебной лаборатории и техническим средствам обучения.

Информационное обеспечение обучения содержит современный перечень основных печатных источников, дополнительных печатных источников и электронных источников.

Контроль и оценка результатов освоения профессионального модуля содержит код и наименование профессиональных и общих компетенций, критерии оценки, и методы оценки результатов обучения, которые осуществляются преподавателем в процессе проведения различных форм учебных занятий.

Рецензируемая рабочая программа рекомендуется для реализации в образовательном процессе.

Рецензент _____ Лиджи-Гаряев Б.Б., высшая квалификационная категория, преподаватель Калмыцкий филиал ФГБОУ ИВО «Московский государственный гуманитарно-экономический университет»

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 03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

1.1. Цель и планируемые результаты освоения профессионального модуля

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

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Защита информации техническими средствами
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

1.1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционного антикоррупционного поведения.
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

1.1.3. В результате освоения профессионального модуля студент 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.
-------------------------	--

<p>уметь</p>	<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
<p>знать</p>	<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
	<p>объектах информатизации;</p> <ul style="list-style-type: none"> – 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 528 час, из них на освоение МДК – 300 час, в том числе на промежуточную аттестацию по МДК – 12 часов, на практики – 216 часов

1.3. Воспитательная цель

В результате освоения профессионального модуля в соответствии с рабочей программой воспитания образовательной программы профессионального образования подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», Квалификация – техник по защите информации, реализуется воспитательная цель – личностное развитие обучающихся и их социализация, проявляющиеся в развитии их позитивных отношений к общественным ценностям, приобретении опыта поведения и применения сформированных общих компетенций специалистов среднего звена на практике. Личностное развитие обучающихся и их социализация, проявляющиеся в развитии их позитивных отношений к общественным ценностям, приобретении опыта поведения и применения сформированных общих компетенций представлено следующими личностными результатами:

ПМ.02 Защита информации техническими средствами	ЛР1, ЛР13, ЛР14, ЛР20, ЛР 21, ЛР 24
Личностные результаты реализации программы воспитания	
Осознающий себя гражданином и защитником великой страны	ЛР 1
Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности	
Демонстрирующий готовность и способность вести с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности	ЛР 13
Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности	ЛР 14
Личностные результаты реализации программы воспитания, определенные ключевыми работодателями	

Осознанный выбор будущей профессии как путь и способ реализации собственных жизненных планов	ЛР 20
Способный к трудовой профессиональной деятельности как к возможности участия в решении личных, общественных, государственных, общенациональных проблем	ЛР 21
Стрессоустойчивость, коммуникабельность	ЛР 24

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля 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		Самостоятельная работа
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
лабораторных и практических занятий	курсовая работа (проект), часов							
ПК 3.1- ПК.3.4 ОК 1– ОК10	Раздел 1 модуля. Применение технической защиты информации	180	144	66	–	36	–	–
ПК 3.5 ОК 01–ОК10	Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации	180	144	30	30	36	–	–
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	144					144	–
	Промежуточная аттестация	12	12	–	–	–	–	–
	Экзамен по профессиональному модулю	12	12	–	–	–	–	–
	Всего:	528	312	96	30	72	144	–

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов
1	2	3
Раздел 1 модуля. Применение технической защиты информации		186
МДК.03.01 Техническая защита информации		150
Раздел 1. Концепция инженерно-технической защиты информации		
Тема 1.1. Предмет и задачи технической защиты информации	Содержание	2
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	
Тема 1.2. Общие положения защиты информации техническими средствами	Содержание	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.	
Раздел 2. Теоретические основы инженерно-технической защиты информации		
Тема 2.1. Информация как предмет защиты	Содержание	6
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	
	Тематика практических занятий и лабораторных работ	4
	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	
Тема 2.2. Технические	Содержание	6

каналы утечки информации	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов	
	утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	
	Тематика практических занятий и лабораторных работ	4
	Расчёт зон для основных технических средств и систем, размещённых в помещении.	
Тема 2.3. Методы и средства технической разведки	Содержание	4
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съёма информации.	
	Тематика практических занятий и лабораторных работ	4
	Работа с техническими средствами защиты информации.	
Раздел 3. Физические основы технической защиты информации		
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание	8
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	
	Тематика практических занятий и лабораторных работ	4
	Измерение параметров физических полей	
Тема 3.2. Физические процессы при подавлении опасных сигналов	Содержание	2
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	
	Тематика практических занятий и лабораторных работ	4
	Выделение речевого сигнала на фоне шумов и помех. Контроль эффективности защиты речевой информации	

Раздел 4. Системы защиты от утечки информации		
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	Содержание	4
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	
	Тематика практических занятий и лабораторных работ	4
	Защита от утечки по акустическому каналу	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	Содержание	4
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	
	Тематика практических занятий и лабораторных работ	4
	Устройства несанкционированного съема акустической информации.	
Промежуточная аттестация по МДК.03.01		6
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	Содержание	6
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	
	Тематика практических занятий и лабораторных работ	4
	Защита от утечки по виброакустическому каналу	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	Содержание	4
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	
	Тематика практических занятий и лабораторных работ	8

	Определение каналов утечки ПЭМИН	
	Защита от утечки по цепям электропитания и заземления	
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	Содержание	4
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	
	Тематика практических занятий и лабораторных работ	4
	Методы и средства съема информации с телефонных линий.	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	Содержание	4
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
	Тематика практических занятий и лабораторных работ	4
	Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации, использующих силовые линии сети переменного тока и линии систем пожарной и охранной сигнализаций	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	Содержание	4
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	
	Тематика практических занятий и лабораторных работ	2
	Определение разрешения объектов защиты от возможного наблюдения с использованием современных визуально-оптических и оптикоэлектронных приборов	
Раздел 5. Применение и эксплуатация технических средств защиты информации		
Тема 5.1. Применение	Содержание	8

технических средств защиты информации	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.	
	Тематика практических занятий и лабораторных работ	6
	Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	
Тема 5.2. Эксплуатация технических средств защиты информации	Содержание	8
	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.	
	Тематика практических занятий и лабораторных работ	2
	Работа с техническими средствами защиты информации	
Учебная практика Виды работ:		36

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

Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации		186
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		150
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		
Тема 1.1. Цели и задачи физической защиты объектов информатизации	Содержание	10
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.	
	Тематика практических занятий и лабораторных работ	2
	Создание моделей нарушителя и возможные пути и способы его проникновения на охраняемый объект	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	Содержание	10
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	
	Тематика практических занятий и лабораторных работ	2
	Разработка инженерных конструкций, применяемых для предотвращения проникновения злоумышленника к источникам информации.	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	Содержание	10
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	
	Тематика практических занятий и лабораторных работ	4
	Монтаж датчиков пожарной и охранной сигнализации	
Тема 2.2. Система	Содержание	10

контроля и управления доступом	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	
	Тематика практических занятий и лабораторных работ	4
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	
	Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Тема 2.3. Система телевизионного наблюдения	Содержание	14
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	
	Тематика практических занятий и лабораторных работ	4
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	
Тема 2.4. Система сбора, обработки, отображения и документирования информации	Содержание	6
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	
	Тематика практических занятий и лабораторных работ	4
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	
Тема 2.5 Система воздействия	Содержание	4
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	
	Тематика практических занятий и лабораторных работ	4
	Управление системой воздействия.	
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		
Тема 3.1 Применение	Содержание	10

инженерно-технических	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным	
средств физической защиты	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.	
	Тематика практических занятий и лабораторных работ	4
	организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	Содержание	10
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженернотехнических 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.	
	Тематика практических занятий и лабораторных работ	2
	Диагностика и ремонт технических средств физической защиты	
Курсовой проект (работа)		30
Примерная тематика курсового проекта (работы)		
	1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.	
Промежуточная аттестация по МДК.03.02		6

Учебная практика по разделу 2 модуля	36
<ol style="list-style-type: none"> 1. Монтаж различных типов датчиков. 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. 4. Рассмотрение системы контроля и управления доступом. 5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 6. Рассмотрение датчиков периметра, их принципов работы. 7. Выполнение звукоизоляции помещений системы шумления. 8. Реализация защиты от утечки по цепям электропитания и заземления. 9. Разработка организационных и технических мероприятий по заданию преподавателя; 10. Разработка основной документации по инженерно-технической защите информации. 	
Производственная практика профессионального модуля	144
<p>Виды работ</p> <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. 	
Промежуточная аттестация (демонстрационный экзамен)	12
Всего	528

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»; мастерская «Кибербезопасность».

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

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

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

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации: Учебник для СПО / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2018 – 508 с. ISBN 978-5-94275-454-9

3.2.2. Дополнительные печатные источники:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

3.2.3. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям

образования и тематике <http://depobr.gov35.ru/>

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

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

6. Федеральный портал «Российское образование» www.edu.ru

7. Федеральный правовой портал «Юридическая
Россия»

<http://www.law.edu.ru/>

8. Федеральный портал «Информационно-
коммуникационные
технологии в образовании» <http://www.ict.edu.ru>

9. Сайт Научной электронной библиотеки www.elibrary.ru

3.3. Особенности обучения инвалидов и лиц с ограниченными возможностями здоровья

Учебные занятия инвалидов и лиц с ограниченными возможностями здоровья организуются совместно с другими обучающимися в учебных группах, а также индивидуально, в соответствии с графиком индивидуальных занятий.

При этом необходимо учитывать несколько аспектов:

- особенности нозологии обучающихся инвалидов и лиц с ограниченными возможностями здоровья;
- психоэмоциональное состояние обучающихся;
- психологический климат, который сложился в студенческой группе;
- настрой отдельных обучающихся и группы в целом на процесс обучения.

При организации учебных занятий в учебных группах используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений, создания комфортного психологического климата в группе.

В образовательной деятельности применяются материальнотехническое оснащение, специализированные технические средства приемапередачи учебной информации в доступных формах для обучающихся с различными особенностями здоровья, электронные образовательные ресурсы в адаптированных формах.

Специфика обучения инвалидов и обучающихся с ограниченными возможностями здоровья предполагает использование игрового,

практикоориентированного, занимательного материала, который необходим для получения знаний и формирования необходимых компетенций. Подготовка обучающимися заданий для учебных занятий должна сочетать устные и письменные формы в соответствии с их особенностями здоровья.

Для того чтобы предотвращать наступление у обучающихся с инвалидностью и обучающихся, имеющих ограниченные возможности здоровья, быстрого утомления можно использовать следующие методы работы:

- чередование умственной и практической деятельности;
- преподнесение материала с использованием средств наглядности;
- использование технических средств обучения, чередование предъявляемой на слух информации с наглядно-демонстрационным материалом.

При освоении дисциплин инвалидами и лицами с ограниченными возможностями здоровья большое значение должно отводиться проведению с ними индивидуальной работы со стороны преподавателей. В индивидуальную работу включается:

- индивидуальная учебная работа (консультации), то есть дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы;
- индивидуальная воспитательная работа.

Особенности обучения обучающихся с нарушениями опорнодвигательного аппарата.

Для обучающегося, имеющего нарушения опорно-двигательного аппарата, необходимо посоветовать использовать вспомогательные средства для усвоения программы, например, диктофон и другие электронные носители информации.

При проведении аудиторных занятий с обучающимися, имеющими осложнения с моторикой рук, возможно использование следующих вариантов работы:

- обеспечение обучающихся электронными текстами лекций и заданий к учебным занятиям;
- использование технических средств фиксации текста (диктофоны) с последующим составлением тезисов лекции в ходе самостоятельной работы обучающегося, которые они впоследствии могут использовать при подготовке и ответах на учебных занятиях.

Одним из видов работы для обучающихся, испытывающих трудности в письме может быть подготовка к учебным занятиям таких заданий, которые не требуют от них написания длинных текстов ответов. Наиболее

оптимальным вариантом такого задания, выполняемого в письменной форме, может служить тестовое задание. Использование тестирования обучающихся необходимо совмещать с обсуждением вариантов ответов.

Контроль знаний можно вести как в устном, так и в письменном виде.

Особенности обучения обучающихся с нарушением слуха.

При организации образовательного процесса со слабослышащей аудиторией рекомендуется использовать следующие педагогические принципы:

- наглядности преподаваемого материала;
- индивидуального подхода к каждому обучающемуся;
- использования информационных технологий;
- использования учебных пособий, адаптированных для восприятия обучающимися с нарушением слуха.

Обучающемуся с нарушением слуха следует предложить занять место на передних партах аудитории, а преподавателю больше времени находиться рядом с рабочим местом этого обучающегося. Учитывая, что такие обучающиеся лучше понимают по губам, желательно располагаться к ним лицом, говорить громко и четко.

Для повышения уровня восприятия учебной информации обучающимися рассматриваемой группы, рекомендуется применение звукоусиливающей аппаратуры, мультимедийных и других средств. Сложные для понимания темы следует снабжать как можно большим количеством наглядного материала. Особую роль в обучении лиц с нарушенным слухом, играют видеоматериалы. По возможности, предъявляемая видеоинформация может сопровождаться текстовой бегущей строкой или сурдологическим переводом.

Контроль знаний обучающихся указанной нозологии может вестись преимущественно в письменном виде, но для развития устной речи, рекомендуется предложить обучающемуся рассказать ответ на задание в тезисах.

Особенности обучения обучающихся с нарушением зрения.

Специфика обучения слабовидящих обучающихся заключается в следующем:

- необходимо дозировать учебную нагрузку;
- применять специальные формы и методы обучения, технические средства, позволяющие воспринимать информацию, а также оптические и тифлопедагогические устройства, расширяющие познавательные возможности обучающихся;

- увеличивать искусственную освещенность помещений, в которых занимаются обучающиеся с пониженным зрением.

При зрительной работе у слабовидящих обучающихся быстро наступает утомление, что снижает их работоспособность, поэтому необходимо проводить небольшие перерывы или переключение рабочей активности.

При чтении лекций, слабовидящим обучающимся следует разрешить использовать звукозаписывающие устройства и компьютеры, как способ конспектирования, во время занятий. Необходимо комментировать свои жесты и надписи на доске и передавать словами то, что часто выражается мимикой и жестами.

При работе на компьютере следует использовать принцип максимального снижения зрительных нагрузок, дозирование и чередование зрительных нагрузок с другими видами деятельности. Кроме того необходимо использовать специальные программные средства для увеличения изображения на экране или для озвучивания информации.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

1. информация по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, на электронном носителе, в печатной форме увеличенным шрифтом и т.п.);

2. доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа);

3. доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, устно и др.).

При необходимости для обучающихся с инвалидностью и обучающихся с ограниченными возможностями здоровья процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов, а также может быть предоставлено дополнительное время для подготовки ответа на зачете или экзамене.

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

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Методы оценки
<p>ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.</p>	<ul style="list-style-type: none"> – демонстрация умений осуществлять управление различной информацией; – демонстрация умений использовать основные принципы документооборота; – демонстрация умений разбираться в различных видах обеспечения автоматизированных информационных систем; – демонстрация умений работать с автоматизированными информационными системами правового законодательства; – демонстрация умений проектирования баз данных; – демонстрация умений осуществлять формализацию и моделирование; – демонстрация умений работать с руководством пользователя. 	<p>Экспертная оценка на практическом экзамене Экспертная оценка в процессе защиты реферата; Экспертная оценка выполнения практического задания</p>

<p>ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации</p>	<ul style="list-style-type: none"> – демонстрация умений использования различных способов получения и хранения информации; – демонстрация умений классифицировать виды, источники и носители информации; – демонстрация умений выбирать подходы к оценке уровней угрозы безопасности информации; – демонстрация умений характеризовать каналы утечки информации; – демонстрация умений использовать различные способы и средства предотвращения утечки информации; – демонстрация умений классифицировать технические средства защиты информации; – демонстрация умений применять различные виды технических средств защиты информации; – демонстрация умений осуществлять технический контроль эффективности защиты информации. 	<p>Экспертная оценка на практическом экзамене</p> <p>Экспертная оценка выполнения практической работы</p>
<p>ПК 3.3. Осуществлять измерение параметров</p>	<ul style="list-style-type: none"> – демонстрация умений применять основные положения доктрины 	<p>Экспертная оценка на практическом</p>
<p>побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.</p>	<p>информационной безопасности;</p> <ul style="list-style-type: none"> – демонстрация умений анализировать концептуальную модель информационной безопасности; – демонстрация умений построения гипотетического нарушителя информационной безопасности; – демонстрация умений осуществлять дублирование информации; – демонстрация умений защиты информации от несанкционированного доступа. 	<p>экзамене</p>

<p>ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.</p>	<ul style="list-style-type: none"> – демонстрация умений вести документацию установленного образца по охране труда, соблюдать сроки ее заполнения и условия хранения; – демонстрация умений использовать экобиозащитную и противопожарную технику, средства коллективной и индивидуальной защиты; – демонстрация умений определять и проводить анализ опасных и вредных факторов в сфере профессиональной деятельности; – демонстрация умений оценивать состояние техники безопасности на объекте; – демонстрация умений применять безопасные приемы труда на территории организации и в производственных помещениях; – демонстрация умений проводить аттестацию рабочих мест по условиям труда, в т.ч. оценку условий труда и травмобезопасности; – демонстрация умений инструктировать подчиненных работников (персонал) по вопросам техники безопасности; – демонстрация умений соблюдать правила безопасности труда, производственной санитарии и пожарной безопасности. 	<p>Экспертная оценка на практическом экзамене</p> <p>Экспертная оценка выполнения лабораторных работ</p>
<p>ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации</p>	<ul style="list-style-type: none"> – демонстрация умений классифицировать сети на основе области действий; – демонстрация умений выполнять передачу данных различными способами; – демонстрация умений характеризовать различные типы 	<p>Экспертная оценка на практическом экзамене</p> <p>Экспертная оценка выполнения практических работ</p>

	<p>локальных сетей;</p> <ul style="list-style-type: none">– демонстрация умений использовать брандмауэры и маршрутизаторы соединений;– демонстрация умений построения логической модели локальной компьютерной сети;– демонстрация умений построения логической модели глобальной компьютерной сети.	
--	--	--

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Номер и дата протокола заседания Научно- методического совета	Перечень измененных пунктов
1.	Протокол №1 от 31.08.2020	1.Обновлено информационное обеспечение реализации программы (п.3.2.)
2.	Протокол №2 от 22.10.2020	2. В разделе 2 после слов «практическое(ие) занятие(я)», «лабораторная(ые) работа(ы)» дополнить словами «в том числе практическая подготовка»

Перечень вопросов к экзамену по ПМ 03 МДК 03.01 Технические средства обеспечения информационной безопасности

1. Цели и задачи инженерно-технической защиты информации.
2. Виды информации, защищаемой техническими средствами.
3. Системный подход при решении задач инженерно-технической защиты информации.
4. Основные признаки аналоговых и дискретных электрических сигналов, средств связи, лазерных излучений.
5. Демаскирующие признаки объектов защиты. Видовые, сигнальные и вещественные демаскирующие признаки.
6. Принципы системного анализа проблем инженерно-технической защиты информации.
7. Классификация способов и средств защиты.
8. Физические эффекты в технических системах.
9. Основы функционирования электромагнитных каналов связи.
10. Свойства физических полей, электрических сигналов и материальных тел как носителей информации
11. Способы доступа к источникам конфиденциальной информации. Наблюдение, перехват, подслушивание.
12. Текущие и эталонные первичные и вторичные признаковые структуры.
13. Принципы идентификации и интерпретации признаков обнаружения и распознавания объектов, измерение их характеристик.
14. Условия и особенности утечки информации.
15. Структура канала утечки. Виды каналов утечки. Условия образования каналов утечки. Характеристики каналов утечки информации.
16. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Акустические каналы утечки информации.
17. Классификация технических средств разведки по видам их носителей.
18. Методы и средства технической разведки.
19. Потенциальные каналы утечки информации на предприятиях.
20. Средства несанкционированного доступа к информации
21. Способы и средства защиты объектов от химической и радиационной разведок.
22. Технические средства акустической разведки: принцип действия, основные функции.
23. Упрощенный принцип работы микрофона и телефона.

- 24.Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи.
- 25.Общая характеристика радиоэлектронной разведки, ее особенности.
- 26.Контактный и бесконтактный метод съема информации за счет непосредственного подключения аппаратуры к телефонной линии: непосредственное подключение к телефонной линии, применение трансформаторов, применение индуктивных датчиков, применение преобразователей Холла.
- 27.Использование микрофона телефонного аппарата при положенной телефонной трубке: общий принцип телефонного аппарата, доработка телефонного аппарата с целью использования его микрофона, беззаходовый НСИ.
- 28.Утечка информации по сотовым цепям связи.
- 29.Особенности передачи сигнала по электросетевому каналу.
- 30.Низкочастотное устройство съема информации. Высокочастотное устройство съема информации.
- 31.Приборы ночного видения. Телевизионные системы наблюдения. Системы защиты от утечки по оптическому каналу
- 32.Организация работ по инженерно-технической защите на предприятиях и в учреждениях государственных и коммерческих структур.
- 33.Основные руководящие документы по защите предприятий и учреждений от технической разведки.
- 34.Нормы допустимых уровней излучений.
- 35.Аттестация выделенных помещений. Особенности защиты информации о продукции на различных этапах ее жизненного цикла.
- 36.Организационные и технические мероприятия по защите информации в учреждениях и на предприятиях.
- 37.Поиск СНСИ и пути подавления. Методика комплексной проверки выделенных помещений.
- 38.Структурные, функциональные и информационные модели объектов защиты и каналов утечки. Принципы построения комплексных моделей объектов защиты и каналов утечки.
- 39.Подходы к оценке угрозы каналов утечки и безопасности конфиденциальной информации.
- 40.Модели систем защиты и показатели эффективности. Стоимость защиты.

Организационные и инженерно-технические средства обеспечения информационной безопасности

1. Понятие об информации как предмете защиты.
2. Классификация демаскирующих признаков..
3. Виды источников и носителей информации.
4. Прямые и косвенные источники семантической информации.
5. Принципы записи и съема информации с её носителя.
6. Понятие модуляции, манипуляции, демодуляции.
7. Побочные электромагнитные излучения и наводки.
8. Угрозы утечки информации. Угрозы преднамеренных воздействий. Угрозы случайных воздействий.
9. Технические каналы утечки информации: наблюдение, подслушивание, перехват.
10. Источники угроз безопасности информации. Опасные сигналы и их источники.
11. Способы и средства наблюдения в оптическом диапазоне.
12. Обработка информации в оптическом приемнике.
13. Способы и средства наблюдения в радиодиапазоне.
14. Способы и средства перехвата сигналов.
15. Способы и средства подслушивания.
16. Типовая структура и виды технических каналов утечки информации.
17. Каналы утечки речевой информации.
18. Каналы утечки информации при её передаче по каналам связи.
19. Акустические и виброакустические каналы утечки речевой информации из объемов выделенных помещений.
20. Каналы утечки информации за счет побочных электромагнитных излучений и наводок
21. Способы доступа к источникам конфиденциальной информации без нарушения государственной границы, без проникновения на объект защиты.
22. Основные показатели технических средств фотографической, телевизионной, инфракрасной и лазерной разведок и каналы утечки информации.
23. Принципы оптической разведки. Основные показатели технических средств визуальной, разведки.
24. Средства наблюдения в оптическом диапазоне. Визуально-оптические приборы, фото- и киноаппараты, средства телевизионного наблюдения, средства наблюдения в инфракрасном и радиодиапазоне.

25. Принципы работы акустических приемников, диктофонов, закладных устройств, лазерных средств подслушивания.
26. Основные положения системного подхода к технической защите информации.
27. Постановка задач по определению рациональных мер защиты информации.
28. Показатели эффективности системы защиты информации
29. Основные элементы системы безопасности предприятия.
30. Основные задачи и структура службы безопасности предприятия.
31. Организационные и технические меры по обеспечению инженернотехнической защиты информации и видеонаблюдения.
32. Анализ объекта защиты, выявление угроз, определение необходимых мер защиты, контроль эффективности реализуемых мер безопасности
33. Алгоритм проектирования системы защиты информации.
Моделирование объектов защиты.
34. Моделирование каналов несанкционированного доступа к защищаемой информации.
35. Моделирование каналов утечки информации. Методика оценки значений показателей моделирования.
36. Задачи и структура государственной системы технической защиты информации.
37. Нормативно-правовая база технической защиты информации.
38. Организация инженерно-технической защиты информации на предприятии.
39. Структура организационных мер инженерно-технической защиты информации.
40. Структура технических мер инженерно-технической защиты информации.
41. Виды контроля эффективности инженерно-технической защиты информации.
42. Методы технического контроля: инструментальный, инструментально-расчетный, расчетный.