

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю

Зам. директора по УР

Н.А. Андреева

«28» 09 2026 г.

Рабочая программа дисциплины

Б1.О.31 Защита информации от утечки по техническим каналам

Кафедра: **Информационная безопасность**
Направление подготовки: **10.03.01 Информационная безопасность**
Профиль: **Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)**
Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Вид учебной работы	ОФО	
	ЗЕ	часов/сем.
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	3	108/7
Контактная работа, в том числе (по семестрам, курсам):		52/7
Лекции		18/7
Лабораторных работ		18/7
Практических занятий		16/7
Семинаров		
Самостоятельная работа		56/7
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с разбивкой по семестрам (курсам)		1/7
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:

Доцент кафедры к.т.н., доцент Манин А.А.

Рабочая программа дисциплины

«Защита информации от утечки по техническим каналам»

Разработана в соответствии с ФГОС ВО:

направления подготовки **10.03.01 «Информационная безопасность»**,
утвержденным приказом Министерства науки и высшего образования Российской
Федерации от 17 ноября 2020 г. N 1427

Составлена на основании учебного плана

направления **10.03.01 «Информационная безопасность»**, профиля «Безопасность
компьютерных систем (по отрасли или в сфере профессиональной деятельности)»,
одобренного Учёным советом СКФ МТУСИ, протокол № 8 от 31.03 2026, и
утвержденного директором СКФ МТУСИ 31.03. 2026 г.

Рассмотрена и одобрена на заседании кафедры
Информационная безопасность

Протокол от «28» 04 2026 г. № 9

И.О.Зав. кафедрой  Жуковский А.Г.

1. Цели изучения дисциплины

Целью преподавания дисциплины «Защита информации от утечки по техническим каналам» является формирование у обучаемых знаний в области защиты информации, умений и навыков практического обеспечения защиты информации, передаваемой по техническим каналам при использовании комплексного подхода к защите информации.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у обучающегося способности решать профессиональные задачи в соответствии с *эксплуатационным* видом деятельности.

Результатом освоения дисциплины являются сформированные у обучающегося следующие компетенции:

ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	
Знать:	
- технические каналы утечки информации; - методы и средствами технической защиты информации от утечки информации по техническим каналам; - демаскирующие признаки объектов; - средства выявления каналов утечки информации; - способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - методы криптографического преобразования информации.	
Уметь:	
- применять средства криптографической и технической защиты информации.	
Владеть:	
- навыками анализа и оценки угроз информационной безопасности объекта защиты; - методами и средствами технической защиты информации; - навыками работы по применению средств криптографической и технической защиты информации.	

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.32 «Основы управления информационной безопасностью»
2	Б1.О.20 «Физика», Б1.О.22 «Электроника» Б1.О.26 «Сети и системы передачи информации».
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.О.33 «Комплексное обеспечение защиты информации объекта информатизации»

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 108 часов, 52 аудиторных часов)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 1					
Модуль 1. Технические каналы утечки информации (26+28) часов					
1.1	Лекция 1.	Лек	2	ОПК-9	Л1.1

	Источники и носители защищаемой информации 1. Основные термины и определения 2. Возможности видов технической разведки 3. Задачи систем защиты информации				Л1.2 Л1.3 Л2.2
1.2	Лекция 2. Технические каналы утечки информации 1. Структура, классификация и основные характеристики 2. Технические каналы утечки информации в ТСПИ 3. Технические каналы утечки информации при передаче ее по каналам связи	Лек	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.3	Лабораторная работа №1 Исследование акустоэлектрического канала утечки информации с использованием закладного устройства «Телефонное ухо»	ЛР	4	ОПК-9	Л1.1 Л1.2 Л1.4 Л2.1
1.4	Практическое занятие №1 Исследование акустоэлектрического канала утечки информации в среде Multisim с использованием закладного устройства в сети электропитания	ПЗ	4	ОПК-9	Л1.1 Л1.2 Л1.4
1.5	Лекция 4. Технические каналы утечки видовой информации 1. Способы скрытого видеонаблюдения и съемки 2. Характеристики оборудования	Лек	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.6	Лекция 5. Демаскирующие признаки объектов 1. Общая характеристика 2. Демаскирующие признаки объектов в диапазонах электромагнитного спектра	Лек	2	ОПК-9	Л1.1 Л1.2 Л2.1
1.7	Лекция 6. Средства выявления каналов утечки информации 1. Общие сведения 2. Индикаторы электромагнитного поля и сканирующие радиоприемники 3. Многофункциональные комплекты для выявления каналов утечки информации	Лек	2	ОПК-9	Л1.1 Л1.2 Л1.3 Л2.2
1.8	Практическое занятие №2 Изучение перехвата ПЭМИ, создаваемого монитором ВТ	ПЗ	4	ОПК-9	Л1.1 Л1.2 Л1.4
1.9	Лабораторная работа №2 Проведение радио мониторинга на информационном объекте	ЛР	4	ОПК-9	Л1.1 Л1.4 Л2.2
1.10	Концептуальная модель информационной безопасности. Направления обеспечения информационной безопасности. Электрические линии связи. Методы и средства инженерной защиты и технической охраны Мероприятия по выявлению и оценке свойств каналов утечки информации	СРС	28	ОПК-9	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2
Модуль 2 Скрытие и защита информации от утечки по техническим каналам (26+28)					
2.1	Лекция 6 Концепция и методы инженерно-технической защиты	Лек	2	ОПК-9	Л1.1 Л1.2

	информации 1. Экранирование электромагнитных волн 2. Безопасность оптоволоконных кабельных систем 3. Заземление технических средств и подавление информационных сигналов в цепях заземления				Л2.1 Л2.2
2.2	Лабораторная работа №3 Исследование электрических параметров помехоподавляющих фильтров в среде Multisim	ЛР	4	ОПК-9	Л1.1 Л1.4 Л2.2
2.3	Лекция 7. Устройства контроля и защиты слаботочных линий и сети 1. Особенности слаботочных линий и сетей как каналов утечки информации 2. Схемы подключения анализаторов к к электросиловым и телефонным линиям в здании 3. Устройства контроля и защиты проводных линий от утечки информации	Лек	2	ОПК-9	Л1.1 Л1.2 Л1.3 Л1.4
2.4	Практическое занятие №3 Исследование информационного скрытия речевого сообщения в тональном канале связи методом частотного скремблирования в среде Multisim	ПЗ	4	ОПК-9	Л1.1 Л1.2 Л1.4 Л2.2
2.5	Лекция 8. Скрытие и защита от утечки информации в низкочастотном диапазоне 1. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам 2. Скрытие речевой информации в телефонных системах с использование криптографических методов	Лек	2	ОПК-9	Л1.1 Л1.2 Л2.2
2.6	Лабораторная работа №4 Исследование электрических параметров СЗИ «Гранит-8» в среде Multisim	ЛР	6	ОПК-9	Л1.1 Л1.2 Л1.4 Л2.2
2.7	Лекция 9. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах 1. Программно-аппаратные комплексы 2. Программные продукты	Лек	2	ОПК-9	Л1.3 Л2.1
2.8	Практическое занятие №4 Изучение активной защиты от перехвата ПЭМИ	ПЗ	4	ОПК-9	Л1.1 Л1.4 Л2.2
2.9	Технический контроль эффективности мер защиты информации. Цели и задачи. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ. Методы испытаний ПЭВМ Методы контроля побочных электромагнитных излучений генераторов технических средств. Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации.	СРС	28	ОПК-9	Л1.1 Л1.2 Л1.3 Л1.4 Л2.2

2.10	Зачет			ОПК-9	Л1.1- Л1.4 Л2.1 Л2.2
Итого – 108 часов					

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Рекомендуемая литература				
5.1.1. Основная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	Зайцев А. П., Мещеряков Р.В., Шелупанов А. А.	Технические средства и методы защиты информации	М.: Гор. линия-Телеком, 2024.	Э1
Л1.2	А.М. Голиков	Защита информации от утечки по техническим каналам	Томский Государственный университет Систем управления и радиоэлектроники, 2015	Э2
Л1.3	Бузов Г.А.	Защита информации ограниченного доступа от утечки по техническим каналам	М.: Гор. линия-Телеком, 2024.	Э3
Л1.4	Кравченко А. С., Мельник В. А., Сахаров С. Л.	Техническая защита информации: практикум	ФКОУ ВО Воронежский институт ФСИИ России. - Иваново: Издательско-полиграфический комплекс «ПресСто», 2023.	Э4
5.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Кубанков А.Н., Булгакова Е.В.	Основы информационной безопасности	М.: МТУСИ, 2024.	Э5
Л2.2	Евстифеев А. А., Ерошев В. И., Мартынов А. П. [и др.];	Основы защиты информации от утечки по техническим каналам	Саров: РФЯЦ-ВНИИЭФ, 2019.	Э6
5.1.3 Учебно-методическое обеспечение				
Л3.1	Скрипник Д.А.	Общие вопросы технической защиты информации	М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2024.	Э7
5.2. Электронные образовательные ресурсы				
Э1	https://elib.mtuci.ru/view.php?book_id=4112			
Э2	https://www.iprbookshop.ru/72090.html			
Э3	https://elib.mtuci.ru/view.php?book_id=3168			
Э4	https://znanium.ru/catalog/document?id=447584&ysclid=mhd2o5zcv388579817			

Э5	http://elib.mtuci.ru/view.php?book_id=3659
Э6	https://viewer.rusneb.ru/ru/000199_000009_010188362?page=4&rotate=0&theme=white
Э7	https://www.iprbookshop.ru/133955
5.3 Информационно-справочные системы и профессиональные базы данных	
5.3.1	Консультант Плюс – https://www.consultant.ru/
5.3.2	Гарант – https://www.garant.ru/
5.3.2	Электронный ресурс http://www.securitylab.ru/
5.3.3	Научная электронная библиотека – https://www.elibrary.ru/
5.3.4	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)
5.3.5	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)
5.3.6	Национальный открытый университет «ИНТУИТ» - https://intuit.ru/
5.4. Программное обеспечение	
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:	
1.	Kaspersky Endpoint Security
2.	Операционная система Linux
3	MS Office - лицензионное ПО
4	VirtualBox
5	Dallas Lock

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий	
1	Лекционная аудитория, оборудованная интерактивной доской, проектором, ПК (ноутбуком), экраном.
6.2 МТО лабораторных работ и практических занятий	
1	Лаборатория «Технической защиты информации», укомплектованная специализированной мебелью, оснащенная техническими средствами защиты информации
2	Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
6.3 МТО рубежных контролей, экзамена	
1	Учебные аудитории, оборудованные компьютерной техникой с возможностью выхода в локальную сеть Филиала и Интернет.
6.4 МТО самостоятельной работы обучающихся	
1	Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

7. Оценочные материалы

Оценочные материалы и перечень видов оценочных средств текущего контроля и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

8. Методические рекомендации для обучающихся по освоению дисциплины

Методические рекомендации по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

9. Особенности реализации дисциплины (модуля) при обучении инвалидов и лиц с ограниченными возможностями здоровья

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков.

Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания.

Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.).

Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь.

Текущий контроль успеваемости осуществляется в устной форме.

При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

10. Дополнения и изменения в Рабочей программе

Лист актуализации рабочей программы дисциплины «Б1.О.31 Защита информации от утечки по техническим каналам» для использования в 20__/20__ учебном году

Утверждаю

Зам. директора по УР _____
«__» _____ 20__ г.

Направление: 10.03.01 Информационная безопасность

Профиль: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(Возможны следующие варианты):

а) Рабочая программа действует без изменений.

б) В рабочую программу вносятся следующие изменения:

- 1)
- 2)
- 3)

Разработчик (и): _____
(ФИО, ученая степень, ученое звание)

«__» _____ 20__ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБ
Протокол № _____ от «__» _____ 20__ г.

Заведующий кафедрой _____

Оценочные материалы для проведения текущего контроля и промежуточной аттестации по дисциплине

1. Оценочные материалы для проведения промежуточной аттестации по дисциплине

1.1 Шкала оценивания компетенций

Шкала оценивания компетенций		
Оценка	Уровень освоения компетенции	Критерии оценивания
«Отлично»	Высокий уровень	Обучающийся показывает всестороннее, систематическое и глубокое знание основного и дополнительного учебного материала, умеет свободно выполнять задания, предусмотренные программой; усвоил основную и знаком с дополнительной рекомендованной литературой; может объяснить взаимосвязь основных понятий дисциплины в их значении для последующей профессиональной деятельности; проявляет творческие способности в понимании, изложении и использовании учебного материала.
«Хорошо»	Повышенный уровень	Обучающийся показывает достаточный уровень знаний в пределах основного учебного материала, без существенных ошибок выполняет предусмотренные в программе задания; усвоил основную литературу, рекомендованную в программе; способен объяснить взаимосвязь основных понятий дисциплины при дополнительных вопросах преподавателя. Допускает не существенные погрешности в ответах, устраняет их без помощи преподавателя.
«Удовлетворительно»	Пороговый уровень	Обучающийся показывает знания основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы; справляется с выполнением заданий, предусмотренных программой, допуская при этом большое количество не принципиальных ошибок; знаком с основной литературой, рекомендованной программой. Допускает существенные погрешности в ответах, но обладает необходимыми знаниями для их устранения под руководством преподавателя.
«Неудовлетворительно»	Минимальный уровень не	Обучающийся обнаруживает пробелы в знаниях основного учебного материала,

	достигнут	допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не знаком с рекомендованной литературой, не может исправить допущенные ошибки. Как правило, оценка «неудовлетворительно» ставится обучающимся, которые не могут продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.
--	-----------	---

1.2 Показатели, критерии и шкалы оценивания компетенций

Показатели компетенции	Критерии оценивания	Шкала оценивания
ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности		
Знать:		
- технические каналы утечки информации; - методы и средствами технической защиты информации от утечки информации по техническим каналам; - демаскирующие признаки объектов;	Контрольная работа	Модуль 1 0÷10 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-4 «Хорошо» - 5-7 «Отлично» - 8-10
- средства выявления каналов утечки информации; - способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - методы криптографического преобразования информации.	Контрольная работа	Модуль 2 0÷10 «Неудовлетворительно» - 0-1 «Удовлетворительно» - 2-4 «Хорошо» - 5-7 «Отлично» - 8-10
Уметь		
- применять средства технической защиты информации; - применять средства криптографической защиты информации.	Лабораторная работа 1-2	Модуль 1 0÷5 за каждую ЛР «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Практическое занятие 1-2	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5

	Лабораторная работа 3-4	Модуль 2 0÷5 за каждую ЛР «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Практическое занятие 3-4	Модуль 2 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
Владеть		
- навыками анализа и оценки угроз информационной безопасности объекта защиты; - методами и средствами технической защиты информации; - навыками работы по применению средств криптографической и технической защиты информации	Лабораторная работа 1-2	Модуль 1 0÷5 за каждую ЛР «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Практическое занятие 1-2	Модуль 1 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Лабораторная работа 3-4	Модуль 2 0÷5 за каждую ЛР «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Практическое занятие 3-4	Модуль 2 0÷5 за каждое ПЗ «Неудовлетворительно» - 0-2 «Удовлетворительно» - 3 «Хорошо» - 4 «Отлично» - 5
	Зачет	0-100 «Не зачтено» - 0-40 «Зачтено» - 41-100

1.3 Оценочные материалы: типовые контрольные задания, иные материалы

1.3.1 Оценочные средства текущего контроля для очной формы обучения

Модуль 1 (50 баллов):

Модуль содержит 5 лекционных занятия 2 лабораторные работы и 2 практических занятия. Знание лекционного материала оценивается по контрольной работе, состоящей из четырех вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные и защищенные лабораторную работу и практическое задание обучающийся получает максимум по 10 баллов за каждое. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ОПК-9):

1. Виды, источники и носители защищаемой информации
2. Технические каналы утечки информации. Структура, классификация и основные характеристики
3. Технические каналы утечки информации, обрабатываемой ТСПИ
4. Технические каналы утечки информации при передаче ее по каналам связи
5. Технические каналы утечки речевой информации
6. Характеристики речевой информации
7. Акустические каналы утечки речевой информации
8. Технические каналы утечки видовой информации
9. Защита информации от утечки по визуально оптическим каналам
10. Защита информации от утечки по акустическим каналам
11. Защита информации от утечки по электромагнитным каналам
12. Защита информации от утечки по материально - вещественным каналам
13. Демаскирующие признаки объектов
14. Средства выявления каналов утечки информации

Лабораторная работа №1. Исследование акустоэлектрического канала утечки информации с использованием закладного устройства «Телефонное ухо»

Контрольные вопросы ЛР №1 (ОПК-9):

1. Что собой представляет звуковое поле?
2. Линейные характеристики звукового поля
3. Характеристика звуковых сигналов
4. Типы микрофонов и их характеристики
5. Приведите классификацию закладных устройств
6. Структура акустоэлектрического канала утечки информации
7. Как определяется звуковая мощность?
8. Методы контроля и прослушивания телефонных каналов связи.

Практическое занятие №1. Исследование акустоэлектрического канала утечки информации в среде Multisim с использованием закладного устройства в сети электропитания

Контрольные вопросы ПЗ №1 (ОПК-9):

1. Что можно моделировать в среде Multisim?
2. Укажите достоинства и недостатки среды Multisim.
3. Как образуется электрический канал утечки информации при ее передаче по линиям связи?
4. Перечислите виды паразитной связи в линиях передачи информации.
5. В чем смысл способа прослушивания телефона методом высокочастотной накачки?
6. Основные требования к закладному устройству.

7. Основные характеристики канала утечки информации.
8. Виды наводок на вторичные источники питания.
9. Основные причины появления помехи с частотой питающей сети.

Практическое занятие №2. Изучение перехвата ПЭМИ, создаваемого монитором ВТ

Контрольные вопросы ПЗ №2 (ОПК-9):

1. Виды каналов утечки информации по ПЭМИ.
2. Что является носителем информации в ТСПИ.
3. Обеспечение информационной безопасности компьютерных систем.
4. Меры защиты информации от утечки по каналам ПЭМИ.
5. Достоинства и недостатки активного метода защиты информации от утечки по каналам ПЭМИ.
6. Достоинства и недостатки пассивного метода защиты информации от утечки по каналам ПЭМИ.
7. Основные этапы экранирования компьютера.
8. В каком частотном диапазоне находятся излучения ПК?
9. Значения уровней побочного электромагнитного излучения.

Лабораторная работа №2. Проведение радио мониторинга на информационном объекте

Контрольные вопросы ЛР №2 (ОПК-9):

1. Диапазон радиоволн.
2. Основные характеристики сканирующих радиоприемников.
3. Отличительные особенности индикаторов электромагнитного поля.
4. Основные параметры и характеристики, определяющие эффективность индикаторов.
5. Принцип действия индикаторов электромагнитного поля.
6. Перечислите источники опасных радиосигналов.
7. Методы поиска и локализации источников опасных радиосигналов.
8. Приборы для определения опасных радиоизлучений.
9. Демаскирующие признаки радио закладных устройств.

Модуль 2: (50 баллов):

Модуль содержит 4 лекционных занятия 2 лабораторные работы и 2 практических занятия. Знание лекционного материала оценивается по контрольной работе, состоящей из двух вопросов, максимальное количество баллов за контрольную работу составляет 10. За выполненные и защищенные лабораторную работу и практическое задание обучающийся получает максимум по 10 баллов за каждое. Общее максимальное количество баллов за модуль 1 составляет 50.

Вопросы для контрольной работы (ОПК-9):

1. Концепция и методы инженерно-технической защиты информации
2. Экранирование электромагнитных волн
3. Безопасность оптоволоконных кабельных систем
4. Заземление технических средств и подавление информационных сигналов в цепях заземления
5. Фильтрация информационных сигналов
6. Устройства контроля и защиты слаботочных линий и сети
7. Скрытие и защита от утечки информации по акустическому и виброакустическому

каналам

8. Скрытие речевой информации в телефонных системах с использованием криптографических методов

9. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах

Лабораторная работа №3. Исследование электрических параметров помехоподавляющих фильтров в среде Multisim

Контрольные вопросы ЛР №3 (ОПК-9):

1. Основные электрические параметры фильтров.
2. Помехи в электросвязи.
3. Требования к помехоподавляющим фильтрам.
4. Основные элементы помехоподавляющих фильтров.
5. Классы помехоподавляющих фильтров.
6. Схемные решения при построении помехоподавляющих фильтров.
7. К каким методам защиты относится фильтрация?

Практическое занятие №3.

Исследование информационного скрывания речевого сообщения в тональном канале связи методом частотного скремблирования в среде Multisim

Контрольные вопросы ПЗ №3 (ОПК-9):

1. Характеристика речевого сообщения.
2. Виды защиты речевой информации.
3. Методы маскировки речевых сообщений.
4. Структурное скрывание речевой информации.
5. Виты паразитных связей.
6. Алгоритмы шифрования.
7. Способы защиты от подслушивания.
8. Способы технического закрытия.

Лабораторная работа №4. Исследование электрических параметров СЗИ «Гранит-8» в среде Multisim

Контрольные вопросы ЛР №4 (ОПК-9):

1. Виртуальные инструменты Multisim.
2. Назначение СЗИ «Гранит-8».
3. Технические характеристики СЗИ «Гранит-8».
4. Состав устройства СЗИ «Гранит-8».
5. Достоинства и недостатки СЗИ «Гранит-8».
6. Каналы несанкционированного получения информации.
7. Назначение диодного моста в схеме СЗИ «Гранит-8».
8. Затухание электрического сигнала.
9. Поясните АЧХ четырехполюсника.
10. Поясните АХ четырехполюсника.

Практическое занятие №4. Изучение активной защиты от перехвата ПЭМИ

Контрольные вопросы ПЗ №4 (ОПК-9):

1. Активные методы защиты от ПЭМИН.
2. Виды зашумления.
3. Устройства, обладающие микрофонным эффектом.
4. Приборы, используемые для обнаружения и измерения основных характеристик ПЭМИН.
5. Технические средства реализующие активные методы защиты информации от

ПЭМИН.

6. Суть пространственного зашумления.
7. Суть линейного зашумления.
8. Требования к системе пространственного зашумления, применяемой для создания маскирующих электромагнитных помех.
9. Помехи, используемые в системах пространственного зашумления.

1.3.2 Вопросы, выносимые на зачет по дисциплине «Защита информации от утечки по техническим каналам» (ОПК-9) (промежуточная аттестация):

1. Виды, источники и носители защищаемой информации.
2. Технические каналы утечки информации. Структура, классификация и основные характеристики.
3. Технические каналы утечки информации, обрабатываемой ТСПИ.
4. Технические каналы утечки информации при передаче ее по каналам связи.
5. Технические каналы утечки речевой информации.
6. Характеристики речевой информации.
7. Акустические каналы утечки речевой информации.
8. Технические каналы утечки видовой информации.
9. Защита информации от утечки по визуальным оптическим каналам.
10. Защита информации от утечки по акустическим каналам.
11. Защита информации от утечки по электромагнитным каналам.
12. Защита информации от утечки по материально - вещественным каналам.
13. Демаскирующие признаки объектов.
14. Средства выявления каналов утечки информации.
15. Концепция и методы инженерно-технической защиты информации.
16. Экранирование электромагнитных волн.
17. Безопасность оптоволоконных кабельных систем.
18. Заземление технических средств и подавление информационных сигналов в цепях заземления.
19. Фильтрация информационных сигналов.
20. Устройства контроля и защиты слаботочных линий и сети.
21. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам.
22. Способы защиты телефонных каналов.
23. Средства физической защиты информации.
24. Задачи решаемые физическими средствами защиты.
25. Программно-аппаратные средства защиты компьютерной информации от несанкционированного доступа.
26. Скрытие речевой информации в телефонных системах с использованием криптографических методов.
27. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах.
28. Аттестация объектов информатизации по требованиям безопасности информации.
29. Мероприятия по выявлению и оценке свойств каналов утечки информации.
30. Технический контроль эффективности мер защиты информации.

2. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Порядок и методика проведения текущего контроля и промежуточной аттестаций

Предусмотрены следующие виды контроля:

- текущий контроль по каждому модулю – в форме написания контрольной работы для оценки теоретических знаний;
- текущий контроль по каждому модулю – в форме отчетов по лабораторным и практическим занятиям для оценки практических навыков;
- промежуточная аттестация по дисциплине – в форме зачета.

Текущий контроль успеваемости в форме защиты лабораторных и практических проводится в два этапа:

- 1-й этап: допуск к выполнению лабораторной работы – проводится в форме письменной «летучки» (5–10 мин) с целью контроля знаний обучающихся теоретической части лабораторной работы и готовности к выполнению практических исследований;
- 2-й этап выполняется по окончании каждой лабораторной работы (практического занятия) в форме индивидуального собеседования по выполненным исследованиям или расчетам. Проводится с целью контроля закрепления теоретической части материала и степени отработки обучающимся практических навыков исследования на аппаратуре.

Контрольные работы выполняются в виде короткого письменного ответа на один вопрос, изученный на предыдущей лекции в начале каждой последующей лекции. Ответ на вопрос дается в течение 5–10 минут. Таким образом, после лекционного курса каждого модуля формируется общая оценка за теоретические знания.

С целью повышения качества обучения за счет побуждения обучающихся к активной текущей учебной работе, четкого и оперативного контроля всего хода учебного процесса, снижения роли случайных и субъективных факторов при оценивании учебной деятельности обучающихся в образовательном процессе реализована модульно-рейтинговая система.

Правила ее использования прописаны в «Положении об МРС».

Набранные обучающимся баллы в рамках текущего контроля переводятся в оценку в соответствии со следующей шкалой:

- «не зачтено» - от 0 до 40 от максимального количества баллов;
- «зачтено» - от 41 до 100 максимального количества баллов.

Соотношения максимального количества баллов, полученных обучающимся по блокам модулей, показаны в Таблице 1.

Таблица 1 - Распределение баллов по модулям дисциплины «Защита информации от утечки по техническим каналам»

Модуль	Всего баллов (Максимальное значение)	Теоретический блок (Контрольная работа)	Практический блок	
			Лаб. работы	Прак. занятия
Модуль 1	50	10	20=10+10	20=10+10
Модуль 2	50	10	20=10+10	20=10+10
Зачет	100			

Теоретический блок по дисциплине в рамках текущего контроля оценивается по результатам контрольной работы. Практический блок оценивается по результатам выполнения лабораторных работ и заданий на практических занятиях.

На зачете производится оценка тех компетенций, которые должны быть в той или иной форме освоены в процессе изучения. Рекомендуется формировать вопросы в билетах таким образом, чтобы преподаватель смог оценить все компетенции данной дисциплины.

3 Промежуточная аттестация

3.1. Промежуточная аттестация проводится в форме зачета. Зачет проводится по расписанию в устном виде по билетам к зачету. Результаты аттестации заносятся в ведомость и зачетную книжку обучающегося.

Образец билета к зачету

	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ Северо-Кавказский филиал ордена Трудового Красного Знамени федерального государственного бюджетного образовательного учреждения высшего образования «Московский технический университет связи и информатики»	Утверждаю И.о.зав. кафедрой «ИБ» _____А.Г.Жуковский «___» _____ 20__ г.
Направление подготовки: 10.03.01 Информационная безопасность Курс 2 Дисциплина: Защита информации от утечки по техническим каналам		
Билет №1 1. Виды, источники и носители защищаемой информации 2. Концепция и методы инженерно-технической защиты информации К.т.н., доцент _____ Манин А.А. «___» _____ 20__ г.		

Один комплект отпечатанных билетов к зачету, подписанных преподавателем кафедры и утвержденных заведующим кафедрой хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

4. Тестовые задания по дисциплине «Защита информации от утечки по техническим каналам»

Тестовые задания позволяют оценить уровень сформированности компетенции ОПК-9 - Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

Задания распределены по блокам в соответствии с уровнем сложности. Каждый блок содержит номер задания, и текст задания.

Базовый уровень (Блок А) содержит примерно 50 % заданий.

Он формируется из заданий с выбором одного или нескольких верных ответов из предложенных или воспроизведения фактического материала (терминология, факты, классификация, параметры и др.);

Повышенный уровень (Блок Б) в среднем составляет 35 % заданий.

В нем используются задания на сопоставление, сравнение, установление последовательности;

Высокий уровень (Блок В) в среднем составляют – 15 % заданий.

В задании используются: решения нетиповых задач, алгоритмы, доказательства, задания с развернутым ответом – определения, перечисление, изображение схемы, структуры и др.

Количество заданий по компетенции ОПК-9 равно 20.

Один комплект тестовых вопросов с указанием правильных ответов хранится у заведующего кафедрой, другой комплект – у преподавателя, ведущего дисциплину.

БЛОК А (базовый уровень) – Задание с выбором одного или нескольких верных ответов из предложенных

Инструкция по тестам Блока А: Прочитайте текст и выберите один или несколько правильных ответов

№ задания	Тексты заданий
1	Технические каналы связи по типу среды распространения делятся на: 1. Три типа; 2. Четыре типа; 3. Пять типов; 4. Шесть типов.
2	Проводные каналы связи могут быть: 1. Воздушные; 2. Кабельные; 3. Земные; 4. Спутниковые.
3	Радиоканал находится в частотном диапазоне: 1. 3 – 3000 Гц; 2 0,3 – 3000 кГц; 3 0,003 – 3000 МГц; 4 0,000003 – 3000 ГГц.
4	Утечка информации это: 1. Несанкционированное изменение содержания (структуры) информационного объекта (например, ввод ложной информации в систему обработки, изменение элементов программного обеспечения, изменение содержания банка данных и т.п.); 2. Информационный объект не утрачивается, но становится недоступным для его собственника, владельца или пользователя (потребителя) в результате физического или логического блокирования этого элемента 3. объекты не утрачиваются, однако становятся доступными посторонним лицам (например, случайное или преднамеренное подслушивание конфиденциального разговора, перехват излучений РЭС техническими средствами разведки, незаконное копирование информации в компьютерных системах, анализ и обобщение множества источников открытой информации и т.п.);

№ задания	Тексты заданий
	4. Объекты или их элементы утрачиваются, т.е. либо переходят в руки посторонних лиц (например, при хищении), либо уничтожаются или разрушаются, например, в результате стихийного бедствия или вооруженного конфликта, неграмотных действий законных пользователей, преднамеренного введения в программное обеспечение определенного типа вирусов и т.п.
5	Оптические каналы связи могут быть: 1. Открытыми; 2. Закрытыми; 3. Полузакрытыми; 4. Скрытыми;
6	Закладные устройства в зависимости от канала передачи могут быть: 1. Радио закладки, инфракрасные закладки, закладки с передачей информации по токоведущим линиям, закладки с записью на магнитофон 2. микрофонного типа, вибрационного типа, с подключением к коммуникационным линиям 3. С непрерывным излучением, с дистанционным управлением, с автоматическим включением при появлении сигнала 4. Оптические закладки, воздушные закладки, закладки с передачей информации по токоведущим линиям, закладки с записью на магнитофон
7	Закладные устройства в зависимости способа восприятия информации могут быть: 1. Радио закладки, инфракрасные закладки, закладки с передачей информации по токоведущим линиям, закладки с записью на магнитофон 2. Микрофонного типа, вибрационного типа, с подключением к коммуникационным линиям 3. С непрерывным излучением, с дистанционным управлением, с автоматическим включением при появлении сигнала 4. Оптические закладки, воздушные закладки, закладки с передачей информации по токоведущим линиям, закладки с записью на магнитофон
8	Закладные устройства по наличию устройства управления могут быть: 1. С радиоуправлением, с оптическим управлением, с передачей информации по токоведущим линиям, с записью на магнитофон 2. Микрофонного типа, вибрационного типа, с подключением к коммуникационным линиям 3. С непрерывным излучением, с дистанционным управлением, с автоматическим включением при появлении сигнала 4. Оптические закладки, воздушные закладки, закладки с передачей информации по токоведущим линиям, закладки с записью на магнитофон
9	Диаграмма направленности микрофона определяет: 1. Чувствительность микрофона в заданном направлении; 2. Снижает уровень шумов в заданном направлении; 3. Расстояние до объекта; 4. Уровень звукового давления объекта излучения.
10	Стандарт 802.11 описывает: 1. Протокол организации беспроводной локальной сети; 2. Протокол организации беспроводной городской сети; 3. Протокол организации беспроводной местной сети; 4. Протокол организации беспроводной интернет-сети.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление соответствия

Инструкция: Прочитайте текст и установите соответствие

№ задания	Тексты заданий
11	Установите соответствие действию 1. Блокирование информации 2. Искажение информации 3. Уничтожение информации 4. Утечка информации А. Объекты не утрачиваются, однако становятся доступными посторонним лицам (например, случайное или преднамеренное подслушивание конфиденциального разговора, перехват излучений РЭС техническими средствами разведки, незаконное копирование информации в компьютерных системах, анализ и обобщение множества источников открытой информации и

№ задания	Тексты заданий
	т.п.) Б. Объекты или их элементы утрачиваются, т.е. либо переходят в руки посторонних лиц (например, при хищении), либо уничтожаются или разрушаются, например, в результате стихийного бедствия или вооруженного конфликта, неграмотных действий законных пользователей, преднамеренного введения в программное обеспечение определенного типа вирусов и т.п. В. Несанкционированное изменение содержания, (структуры) информационного объекта (например, ввод ложной информации в систему обработки, изменение элементов программного обеспечения, изменение содержания банка данных и т.п.). Г. Объекты или их элементы утрачиваются, т.е. либо переходят в руки посторонних лиц (например, при хищении), либо уничтожаются или разрушаются, например, в результате стихийного бедствия или вооруженного конфликта, неграмотных действий законных пользователей, преднамеренного введения в программное обеспечение определенного типа вирусов и т.п.
12	Установите соответствие стандарта его назначению: 1. 802.11; 2. 802.15; 3. 802.16; 4. IrDa; А. Персональная сеть; Б. Локальная сеть; В. Региональная сеть; Г. Глобальная сеть.
13	Установите соответствие возможной утечки информации: 1. По цепям заземления; 2. По цепям питания; 3. По виброканалу; 4. Электроакустическому каналу; А. Асимметричная наводка; Б. Создание системы проводящих поверхностей и электрических соединений; В. Электрические сигналы, соответствующие звуковым частотам; Г. электрические звонки, громкоговорители, электромеханические реле, трансформаторы.
14	Установите соответствие техническим каналам связи 1. Проводные каналы связи; 2. Оптические каналы связи; 3. Радиоканалы связи; 4. Спутниковые каналы связи. А. Воздушные каналы связи; Б. Кабельные каналы связи; В. Беспроводные каналы связи; Г. Электрические каналы связи.

БЛОК Б (повышенный уровень) – Задание закрытого типа на установление последовательности

Инструкция: Прочитайте текст и установите правильную последовательность

№ задания	Тексты заданий
15	Расставьте радиодиапазоны в порядке возрастания полосы пропускания: 1. EHF; 2. SHF; 3. VLF; 4. LF; 5. MF; 6. HF; 7. UHF;

№ задания	Тексты заданий
	8. VHF.
16	Перечислите микрофоны в порядке увеличения осевой чувствительности: 1. Порошковые угольные микрофоны; 2. Электродинамические; 3. Пьезоэлектрические; 4. Электромагнитные.
17	Расставьте строительные конструкции в порядке ухудшения разборчивости речи при прохождении звука через них: 1. Кирпичная стена; 2. Гипсолитовая стена; 3. Деревянная стена; 4. Перегородка внутренняя; 5. Бетонная стена.

БЛОК В (высокий уровень) – Задание открытого типа с развернутым ответом
Инструкция: Прочитайте текст и запишите обоснованный ответ

№ задания	Тексты заданий
18	Добавить недостающие слова в определение утечки информации: Утечка информации — это несанкционированный доступ, неконтролируемое распространение или _____ конфиденциальных данных
19	Добавить недостающие слова в характеристики оборудования: AirMagnet Enterprise – это _____ безопасности и производительности _____ сетей
20	Определить, что относится к опасной зоне R1 и R2: Область вокруг ТСПИ, в которой наводки на случайных антеннах выше допустимого нормированного уровня – это _____ Область вокруг ТСПИ, в которой отношение «сигнал/шум» побочных электромагнитных излучений ТСПИ превышает допустимое нормированное значение и возможен их перехват с помощью идеального приемника – это _____

**Система оценивания выполнения тестовых заданий по компетенции ОПК-9,
формируемой дисциплиной «Защита информации от утечки по техническим каналам»**

Номер задания	Указания по оцениванию	Результат оценивания (баллы, полученные за выполнение задания/характеристика правильности ответа)
Задания 1-10	Задания с выбором одного или нескольких верных ответов из предложенных считается верным, если правильно указана цифра или цифры, означающие верные ответы.	Совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 11-14	Задания закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого)	Полное совпадение с верным ответом оценивается 1 баллом; неверный ответ или его отсутствие - 0 баллов.
Задания 15-17	Задания закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр	Полное совпадение с верным ответом оценивается 1 баллом; если допущены ошибки или ответ отсутствует- 0 баллов.
Задания 18-20	Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте.	Полный правильный ответ на задание оценивается 1 баллом. Если в ответе используются перечисления, то различный порядок следования правильных ответов в перечислении не считается ошибкой. Если допущена ошибка, ответ не полный, неправильный или отсутствует - 0 баллов.

Методические рекомендации по освоению дисциплины

1. Методические рекомендации преподавателю

Перед началом изучения дисциплины преподаватель должен ознакомить обучающихся с рабочей программой и оценочными материалами по дисциплине, с видами учебной и самостоятельной работы, перечнем литературы и интернет-ресурсов, с формами текущей и промежуточной аттестации, с критериями оценки качества знаний для итоговой оценки по дисциплине.

При проведении лекций преподаватель:

- 1) формулирует тему и цель занятия, объявляет учебные вопросы;
- 2) излагает основные теоретические положения;
- 3) с помощью технических средств обучения и/или под запись дает определения основных понятий, расчетных формул;
- 4) проводит примеры из отечественного и зарубежного опыта, дает текущие статистические данные для наглядного и образного представления изучаемого материала;
- 5) в конце занятия выдает вопросы для самостоятельного изучения.

На занятиях лабораторного цикла следует обратить внимание на соответствие выбираемых обучающимся средств выполнения решаемым в работе задачам.

Каждая лабораторная работа должна быть оформлена и защищена в соответствии с требованиями. Защита производится после оформления отчета по работе.

Во время выполнения заданий в учебной аудитории обучающийся может консультироваться с преподавателем, определять наиболее эффективные методы решения поставленных задач. Если какая-то часть задания остается не выполненной, обучающийся может продолжить её выполнение во время внеаудиторной самостоятельной работы.

Для оценки полученных знаний и освоения учебного материала по каждому разделу и в целом по дисциплине преподаватель использует формы текущего, промежуточного и итогового контроля знаний обучающихся.

2. Методические рекомендации обучающимся

Приступая к изучению новой учебной дисциплины, обучающиеся должны ознакомиться с рабочей программой, оценочными материалами, учебной, научной и методической литературой, имеющейся в ЭИОС СКФ МТУСИ,

Глубина усвоения дисциплины зависит от активной и систематической работы обучающегося на лекциях и практических занятиях, а также в ходе самостоятельной работы, по изучению рекомендованной литературы.

2.1 Методические указания для обучающихся по лекционным занятиям

Важно сосредоточить внимание на содержании лекции. Это поможет лучше воспринимать учебный материал и уяснить взаимосвязь проблем по всей дисциплине.

Основное содержание лекции целесообразнее записывать в тетради в виде ключевых фраз, понятий, тезисов, обобщений, схем, опорных выводов. Необходимо обращать внимание на термины, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставлять в конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющей

материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

С целью уяснения теоретических положений, разрешения спорных ситуаций необходимо задавать преподавателю уточняющие вопросы. Для закрепления содержания лекции в памяти, необходимо во время самостоятельной работы внимательно прочесть свой конспект и дополнить его записями из учебников и рекомендованной литературы.

Конспектирование читаемых лекций и их последующая доработка способствует более глубокому усвоению знаний, и поэтому являются важной формой учебной деятельности обучающихся.

2.2 Методические указания для обучающихся по подготовке к лабораторным работам

Лабораторные занятия по любой учебной дисциплине проводятся в соответствии с рабочей программой этой учебной дисциплины в установленные расписанием часы.

Инструктаж по технике безопасности, правилам пожарной безопасности и правилам внутреннего распорядка в лаборатории проводится преподавателем на первом лабораторном занятии. На этом же занятии обучающимся сообщаются:

- программа всего предстоящего лабораторного цикла;
- условия взаимодействия обучающихся с преподавателем в процессе выполнения лабораторных работ;
- условия контроля самостоятельной работы обучающихся, включая правила оформления отчетов по лабораторным работам и их последующей защиты;
- другая необходимая информация.

Организация лабораторных работ включает:

- самостоятельную внеаудиторную подготовку обучающегося к выполнению каждой отдельной лабораторной работы в соответствии с ее программой в рамках часов, выделенных на самостоятельную проработку материала в программе дисциплины;
- входной контроль преподавателем степени подготовленности каждого обучающегося к выполнению лабораторных работ;
- выполнение программы лабораторных работ в полном объеме;
- оформление отчета и его защиту каждым обучающимся в установленные сроки;
- формирование преподавателем рейтингов каждого из обучающихся по результатам выполнения и защиты им отдельных лабораторных работ и их циклов (используется Модульно-рейтинговая система).

Оценка качества выполнения лабораторных работ каждым обучающимся производится преподавателем отдельно за подготовку к работе, ее выполнение и защиту.

2.3 Методические указания для обучающихся по подготовке к практическим занятиям

Целью практических занятий является закрепление теоретических знаний, полученных при изучении дисциплины.

При подготовке к практическому занятию целесообразно выполнить следующие рекомендации:

- изучить основную литературу; ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д.;
- при необходимости доработать конспект лекций. При этом учесть рекомендации преподавателя и требования учебной программы.

При выполнении практических занятий основным методом обучения является самостоятельная работа обучающегося под управлением преподавателя. На них пополняются теоретические знания обучающихся, их умение творчески мыслить, анализировать, обобщать изученный материал, проверяется отношение обучающихся к будущей профессиональной деятельности.

Оценка выполненной работы осуществляется преподавателем комплексно: по результатам выполнения заданий, устному сообщению и оформлению работы.

После подведения итогов занятия обучающийся обязан устранить недостатки, отмеченные преподавателем при оценке его работы.

2.4 Учебно-методическое обеспечение проведения лабораторных и практических занятий

Для подготовки и выполнения лабораторных и практических занятий используются:

- учебник для обучающихся вузов «Технические средства и методы защиты информации» авторы Зайцев А. П., Мещеряков Р.В., Шелупанов имеющийся в библиотеке СКФ МТУСИ;

- учебное пособие А.М. Голиков «Защита информации от утечки по техническим каналам» <https://reader.lanbook.com/book/110328>

- учебно-методическое пособие Основы защиты информации от утечки по техническим каналам: учебно-методическое пособие / А. А. Евстифеев, В. И. Ерошев, А. П. Мартынов [и др.]; Российский федеральный ядерный центр - Всероссийский научно-исследовательский институт экспериментальной физики. — Саров: РФЯЦ-ВНИИЭФ, 2019. — 266 с.: ил., табл.: 23 см.; ISBN 978-5-9515-0426-5. https://viewer.rusneb.ru/ru/000199_000009_010188362.

- практикум: Техническая защита информации / сост. А. С. Кравченко, В. А. Мельник, С. Л. Сахаров; ФКОУ ВО Воронежский институт ФСИН России. - Иваново: Издательско-полиграфический комплекс «ПресСто», 2023. - 80 с. - Текст: электронный. - URL: <https://znanium.ru/catalog/product/2158325> – неограниченный доступ для авторизованных пользователей.

- учебное пособие Киренберг, А. Г. Защита информации от утечки по техническим каналам: / А. Г. Киренберг, В. О. Коротин. — Кемерово: КузГТУ имени Т.Ф. Горбачева, 2023. — 222 с. — ISBN 978-5-00137-407-7. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/399665> – неограниченный доступ для авторизованных пользователей.

3. Методические рекомендации для обучающихся по самостоятельной работе

Самостоятельная работа обучающихся является составной частью учебной работы и имеет целью закрепление и углубление полученных знаний и навыков, поиск и приобретение новых знаний, в том числе с использованием автоматизированных обучающих курсов (систем), а также выполнение учебных заданий, подготовку к предстоящим занятиям, зачетам и экзаменам.

Самостоятельная работа во внеаудиторное время включает в себя:

- повторение лекционного материала;
- подготовки к лабораторным работам (практическим занятиям);
- изучения учебной и научной литературы;
- решения задач, выданных на практических занятиях;
- подготовки к тестированию;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях.

- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов.

Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит инструктаж (консультацию) с определением цели задания, его содержания, сроков

выполнения, основных требований к результатам работы, критериев оценки, форм контроля и перечня источников и литературы.

Обычно постановку задачи обучаемым на проведение самостоятельной работы преподаватель осуществляет на одном из занятии, предшествующему данному.

Методику самостоятельной работы все обучаемые выбирают индивидуально.

Обучающимся очной формы обучения при освоении вопросов для самостоятельного изучения, представленных в подразделе 4.1 рабочей программы, рекомендуется соблюдать последовательность их изучения, представленную в таблице.

Таблица – Учебный материал, выносимый на самостоятельное изучение обучающимся очной формы обучения

№	Темы, разделы, вынесенные на самостоятельную подготовку, вопросы для подготовки к практическим и лабораторным занятиям; курсовые работы, содержание контрольных работ; рекомендации по использованию литературы, ЭВМ и др.	Часов всего: 54
Модуль 1		28
1	Концептуальная модель информационной безопасности.	4
2	Направления обеспечения информационной безопасности.	4
3	Электрические линии связи.	4
4	Оптические линии связи.	4
5	Доктрина информационной безопасности Российской Федерации;	4
6	Методы и средства инженерной защиты и технической охраны	4
7	Мероприятия по выявлению и оценке свойств каналов утечки информации	4
Модуль 2		28
8	Технический контроль эффективности мер защиты информации. Цели и задачи.	4
9	Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ.	4
10	Методы испытаний ПЭВМ	5
11	Методы контроля побочных электромагнитных излучений генераторов технических средств.	5
12	Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации.	5
13	Анализ моделей нарушителя; угрозы информационно-программному обеспечению вычислительных систем и их классификация.	8

Самостоятельная работа обучающихся над усвоением материала по дисциплине может выполняться в помещении для самостоятельной работы СКФ МТУСИ, посредством использования электронной библиотеки и ЭИОС.