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 УВР
_____ Н.А. Андреева
«29» 04 2024 г.

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

рабочая программа дисциплины

Кафедра: **Информационной безопасности**
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
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 ИТСС, к.т.н., доцент Борисов Б.П.

Рецензенты:
Ведущий сотрудник ФГУП «РНИИРС», д.т.н., доцент Елисеев А.В.

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 образования и науки 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 № 9 от 22.04.2024, и утвержденного директором СКФ МТУСИ 22.04.2024 г.

Рассмотрена и одобрена на заседании кафедры
«Информационная безопасность»

Протокол от «24» апреля 2024 г. № 9

Зав. кафедрой _____ Д.В. Маршаков

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры

"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР _____
-__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____

---

1. Цели изучения дисциплины

Целями изучения дисциплины *" Защита информации от утечки по техническим каналам "* являются 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 выпускника способности решать профессиональные задачи в соответствии с ***эксплуатационной деятельностью.***

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

Компетенции выпускника, формируемые в результате освоения дисциплины (в части, обеспечиваемой дисциплиной)
ОПК-9: способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности;
Знать:
классификацию и количественные характеристики технических каналов утечки информации, возожности технических разведок; способы и средства защиты информации от утечки по техническим каналам, контроля их эффективно
Уметь:
анализировать и оценивать угрозы информационной безопасности объекта информатизации;- применять на практике штатные средства технической защиты информации и средства- способы и средства защиты ин-формации от утечки по техническим каналам, контроля их эффективности; контроля (мониторинга) их эффективности
Владеть:
методами и средствами технической защиты информации

3. Место дисциплины в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины, модули, темы):	
1	Б1.О.20 Физика
2	Б1.О.21 Электротехника
3	Б1.О.19 Теория информации
4	Б1.О.25 Аппаратные средства вычислительной техники
Последующие дисциплины и практики, для которых освоение данной дисциплины необходимо:	
1	Б1.В.02 Стеганографические методы скрытия информации
2	Б1.О.33 Комплексное обеспечение защиты информации объекта информатизации

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

4. Структура и содержание дисциплины

4.1 Очная форма обучения, 4 года (всего 144 часов, 52 аудиторных часов, 56 часов самостоятельной работы)

Код зан.	Тема и краткое содержание занятия	Вид зан.	Кол. часов	Компетенции	УМИО
Курс 4, Семестр 7					
Модуль 1. Технические каналы утечки информации					
1.1	Лекция 1. Источники и носители защищаемой информации 1. Основные термины и определения 2. Возможности видов технической разведки 3. Задачи систем защиты информации	Лк 1	2	ОПК-9	Л1.1 Л1.2 Л1.3
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 передачи ее по каналам связи	Лк 2	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.3	Лекция 3. Технические каналы утечки речевой информации 1. Краткие сведения по акустике 2. Характеристики речевой информации 3. Акустические каналы утечки речевой информации	Лк 3	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.4	Лабораторная работа №1 Исследование акустоэлектрического канала утечки информации с использованием закладного устройства «Телефонное ухо»	Лр 1	4	ОПК-9	Л1.1 Л1.2
1.5	Лабораторная работа №2 Исследование акустоэлектрического канала утечки информации в среде Multisim с использованием закладного устройства в сети электропитания	Лр 2	4	ОПК-9	
1.6	Лекция 4. Технические каналы утечки видовой информации 1. Способы скрытого видеонаблюдения и съемки 2. Характеристики оборудования	Лк 4	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.7	Лекция 5. Демаскирующие признаки объектов 1. Общая характеристика 2. Демаскирующие признаки объектов в диапазонах электромагнитного спектра	Лк 5	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.8	Практическое занятие №1. Средства выявления каналов утечки информации 1. Общие сведения 2. Индикаторы электромагнитного поля и сканирующие радиоприемники 3. Многофункциональные комплекты для выявления каналов утечки информации	Пз 1	2	ОПК-9	Л1.1 Л1.2 Л1.3
1.9	Практическое занятие №2 Изучение перехвата ПЭМИ, создаваемого монитором ВТ	Пз 2	4	ОПК-9	Л1.1 Л1.2
1.10	Практическое занятие №3 Проведение радио мониторинга на информационном объекте	Пз 3	4	ОПК-9	

1.11	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	СР	28	ОПК-9	Л1.1 Л1.2 Л1.3 Л2.1
Модуль 2 Скрытие и защита информации от утечки по техническим каналам					
2.1	Лекция 6 Концепция и методы инженерно-технической защиты информации 1. Экранирование электромагнитных волн 2. Безопасность оптоволоконных кабельных систем 3. Заземление технических средств и подавление информационных сигналов в цепях заземления	Лк 6	2	ОПК-9	Л1.1 Л1.2 Л1.3
2.2	Практическое занятие №4 Фильтрация информационных сигналов 1. Основные сведения о помехоподавляющих фильтрах 2. Выбор типа фильтра	Пз 4	2	ОПК-9	Л1.1 Л1.2 Л1.3
2.3	Лабораторная работа №3 Исследование электрических параметров помехоподавляющих фильтров в среде Multisim	Лр 3	4	ОПК-9	Л1.1 Л1.2
2.4	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	Лк 7	2	ОПК-9	Л1.1 Л1.2 Л1.3
2.5	Лабораторная работа №4 Исследование информационного скрытия речевого сообщения в тональном канале связи методом частотного скремблирования в среде Multisim	Лр 4	4	ОПК-9	Л1.1 Л1.2
2.6	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	Лк 8	2	ОПК-9	Л3.1
2.7	Лабораторная работа №5 Исследование электрических параметров СЗИ «Гранит-8» в среде Multisim	Лр 5	2	ОПК-9	Л1.1 Л1.2
2.8	Лекция 9. Защита конфиденциальной информации от несанкционированного доступа в автоматизированных системах 1. Программно-аппаратные комплексы 2. Программные продукты	Лк 9	2	ОПК-9	Л3.1
2.9	Практическое занятие №5 Изучение активной защиты от перехвата ПЭМИ	Пз 5	4	ОПК-9	

2.10	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.	СР	28	ОПК-9	Л1.1 Л1.2 Л1.3 Л2.1
Итого – 144 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, 2014. – 442 с.	5
Л1.2	А.М. Голиков	Защита информации от утечки по техническим каналам	Томский Государственный университет Систем управления и радиоэлектроники, 2015	Э1
Л1.3	Бузов Г.А.	Защита информации ограниченного доступа от утечки по техническим каналам	М.: Гор. линия-Телеком, 2015. - 586 с.: 60х90 1/16 (Обложка) ISBN 978-5-9912-0424-8	Э2

5.1.2. Дополнительная литература

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Е. Б. Белов, В.П. Лось, Р. В. Мещеряков, Д. А. Шелупанов	Основы информационной безопасности	М.: Гор. линия-Телеком, 2011. - 558 с.: ил.; 60х88 1/16. - (Специальность; Учебное пособие для высших учебных заведений.	Э3

5.2. Электронные образовательные ресурсы

Э1	https://www.iprbookshop.ru/72090.html
Э2	http://znanium.com/catalog/product/895240
Э3	http://znanium.com/catalog/product/405159

5.3. Программное обеспечение

П.1	Linux (свободное ПО)
П.2	LibreOffice (свободное ПО)
П.3	Kaspersky Endpoint Security (лицензия)

6. Материально-техническое обеспечение дисциплины

6.1 МТО лекционных занятий

1	Лекционная аудитория, оборудованная интерактивной доской, проектором
6.2 МТО лабораторных работ и практических занятий	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет
6.3 МТО рубежных контролей, экзамена	
1	Компьютерные аудитории с возможностью выхода в локальную сеть Филиала и Интернет

7. Методические рекомендации для обучающихся по самостоятельной работе

Указания по подготовке к различным видам занятий

Подготовка к лекционным занятиям осуществляется систематически и сводится к повторению изученного материала и отработке тем, вынесенных на самостоятельную работу. При этом должен быть доработан конспект лекций, а также получены ответы на контрольные вопросы, которые, как правило, приводятся в конце каждого раздела учебных пособий. Особое внимание необходимо уделить пониманию изучаемого материала. Зафиксировать вопросы, которые следует задать преподавателю.

Подготовка к лабораторным и практическим занятиям должна проводиться в объеме тех указаний, которые приводятся в каждом методическом пособии для проведения соответствующего занятия. Тема очередного занятия объявляется преподавателем накануне.

После повторения лекционного материала необходимо ознакомиться с предлагаемыми практическими заданиями, уяснить их суть, продумать порядок их выполнения, уточнить достаточность своих знаний для выполнения задания. Целесообразно выполнить возможные заготовки из состава отчета, который предстоит оформить на занятии. Это позволит выполнить и защитить работу в период плановых часов. Перед проведением каждого занятия должно быть полное представление о сути и порядке выполнения предстоящей работы.

Существенное значение имеет самостоятельная работа студента.

Темы для самостоятельного изучения для различных форм обучения, информационные источники и рекомендуемое время указаны в Разделе 4 настоящей Рабочей программы.

Самостоятельная работа студентов по дисциплине проводится в течение всего семестра и складывается из нескольких составляющих.

Подготовка к плановым аудиторным занятиям. В начале семестра студентов знакомят с календарным планом проведения всех видов учебных занятий. Чтобы студенты могли проверить качество своей подготовки к занятиям, в учебных пособиях и методических указаниях к лабораторным работам имеются вопросы для проверки уровня знаний перед выполнением работы и контрольные вопросы, позволяющие студенту оценить качество полученных результатов после выполнения работы. Предлагаемые студентам учебные пособия кроме контрольных вопросов содержат примеры с решениями и упражнения по основным темам.

Изучение технической литературы. Студенты самостоятельно изучают рекомендованную преподавателем техническую литературу.

Дополнительные самостоятельные исследования в лаборатории. Студенты, желающие получить более глубокие знания, имеют возможность выполнить дополнительные самостоятельные исследования в лаборатории. С этой целью в плановых лабораторных работах предусмотрены возможности для дополнительных исследований. Перечень разделов программы, предлагаемых для самостоятельных исследований, доводится до сведения студентов в начале семестра.

Самостоятельная работа на ПЭВМ. Для повышения эффективности самостоятельной работы студентам во второй половине дня предоставляется возможность выполнить в лаборатории самостоятельные исследования с использованием программно-аппаратного комплекса, состоящего из виртуальных электронных приборов, отображаемых на экране ПЭВМ, и моделирующих программ.

Исследуемые схемы могут собираться из реальных компонентов на лабораторном стенде или виртуальных компонентов, хранящихся в библиотеке ПЭВМ.

Источники, рекомендуемые для углубленного изучения учебного материала

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие. – М.: ДМК Пресс, 2011. – 416 с.;
2. Бирюков А.А. Информационная безопасность: защита и нападение. 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с.
3. Маршаков, Д. В. Программно-аппаратные средства защиты информации: учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону: Донской ГТУ, 2021. — 228 с.
4. Воронов В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. – М.: Горячая линия - Телеком, 2013.
5. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. 3-е изд., испр. и доп. – Москва: ИНФРА-М, 2022. – 327 с.
6. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Управление безопасностью критических информационных инфраструктур. – М.: Горячая линия – Телеком, 2021.
7. Климентьев, К. Е. Введение в защиту компьютерной информации: учебное пособие / К. Е. Климентьев. — Самара: Самарский университет, 2020. — 183 с.
8. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с..
9. Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование: учеб-ное пособие для вузов / С. Н. Никифоров. — 4-е изд., стер. — Санкт-Петербург: Лань, 2022. — 124 с.
10. Язов Ю.К., Соловьев С.В. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Воронеж: Кварта, 2018. – 588 с.
11. Профильные журналы «Электросвязь», «T-Comm: Телекоммуникации и транспорт» и другие.

Использование Интернет-ресурсов

1. Электронный ресурс https://www.securitylab.ru/
2. Электронный ресурс https://securelist.ru/
3. Электронный ресурс https://www.kaspersky.ru/
4. Электронный ресурс https://encyclopedia.kaspersky.ru/
5. Электронный ресурс https://www.drweb.ru/
6. Электронный ресурс http://infoprotect.net/category/news
7. Электронный ресурс https://www.it-world.ru/it-news/security/
8. Электронный ресурс https://threatpost.ru/
9. Электронный ресурс https://www.anti-malware.ru/

Рекомендации по подготовке к рубежным аттестациям

Подготовка к сдаче модуля сводится защите на дату проведения последнего занятия в рамках модуля всех практических и лабораторных занятий, а также к подготовке к ответам по тестовым заданиям.

Объем вопросов по каждому лабораторному и практическому занятию отражен в методических указаниях по проведению соответствующего занятия. Кроме того студент должен быть готов к пояснениям по сути практических приемов работы и доказыванию обоснованности принятых решений. Если работа не выполнена или не защищена своевременно, то это следует сделать в часы самоподготовки и консультаций до даты последнего занятия в рамках сдаваемого модуля.

Подготовка к выполнению теста обеспечивается изучением и повторением того материала, который изучался на лекционных занятиях и входе лабораторных и практических занятий. Материал

повторяется по конспектам и учебным пособиям, указанным в списке литературы и методических указаниях.

Подготовка к зачету осуществляется на протяжении всего времени изучения дисциплины.

Для более конкретной, целенаправленной и качественной подготовки к зачету необходимо перед началом изучения дисциплины познакомиться с содержанием рабочей программы. Уяснить логику и последовательность изучения материала, уточнить конкретные конечные результаты, которые должны быть достигнуты в итоге изучения конкретных тем и занятий. Познакомиться с перечнем вопросов и заданий, выносимых на экзамен.

В ходе каждого занятия необходимо изучить все учебные вопросы и выполнить практические задания. Для оперативного оценивания уровня достижения учебных целей следует ответить на контрольные вопросы, которые имеются в руководстве для каждого практического и лабораторного занятия. В случае выявленных затруднений следует провести дополнительное изучение материала в часы самостоятельной работы или в период консультаций с преподавателем. Все учебные материалы должны быть отражены в конспекте, он должен дополняться и уточняться по мере отработки и уточнения учебных вопросов. Само ведение конспекта концентрирует внимание, упорядочивает знания, стимулирует активность в усвоении. К моменту выхода на непосредственную подготовку к зачету в конспекте не должно остаться непонятных вопросов.

В силу ограниченного времени, отводимого на непосредственную подготовку к зачету, целесообразно материал повторять в основном по отработанному конспекту. Это экономит время и дает возможность работать по уже знакомым записям, что улучшает запоминание материала. Остается спланировать работу в соответствии с имеющимся временем и жестко придерживаться намеченного плана. В период обязательных плановых предэкзаменационных консультаций необходимо уточнить организационные вопросы проведения экзамена и при необходимости - сложные вопросы по существу материала.

Дополнения и изменения в Рабочей программе