МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Национальный исследовательский ядерный университет «МИФИ»

Саровский физико-технический институт -

филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский ядерный университет «МИФИ»

(СарФТИ НИЯУ МИФИ)

ФИЗИКО-ТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра «Радиофизика и электроника»

УТВЕРЖДАЮ
Декан ФТФ,
член-корреспондент РАН

_____А.К. Чернышев

«___» _____ 2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Технические каналы утечки информации

наименование дисциплины

Направление подготовки (специальность) 11.04.04 Электроника и наноэлектроника

Наименование образовательной программы Электронные приборы и устройства

Квалификация (степень) выпускника магистр

Форма обучения очная

Программа одобрена на заседании кафедры

протокол № 3 от 17.08.2023г.

Зав. кафедрой РФЭ
д.т.н., доцент
_____ Д.Б. Николаев

«____» _____ 2023г.

г. Саров, 2023 г.

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ на 202____/202_____ учебный год.

Заведующий кафедрой РФЭ, д.т.н., доцент Д.Б. Николаев

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ на 202____/202_____ учебный год.

Заведующий кафедрой РФЭ, д.т.н., доцент Д.Б. Николаев

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ на 202____/202_____ учебный год.

Заведующий кафедрой РФЭ, д.т.н., доцент Д.Б. Николаев

Программа переутверждена на 202____/202____учебный год с изменениями в соответствии с семестровыми учебными планами академических групп ФТФ на 202____/202_____ учебный год.

Заведующий кафедрой РФЭ, д.т.н., доцент Д.Б. Николаев

Семестр	**В форме практической подготовки**	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**СРС, час.**	**КР/ КП**	**Форма(ы) контроля, экз./зач./ЗсО/**
3		5	180	32	16	-	96		Э
ИТОГО		**5**	**180**	**32**	**16**	**-**	**96**		**36**

АННОТАЦИЯ

Учебная дисциплина «Технические каналы утечки информации» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления. Основной целью дисциплины «Технические каналы утечки информации» является изложение основополагающих принципов защиты информации от утечки по техническим каналам (техническая защита информации) на объектах информации и в выделенных помещениях.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями дисциплины «Технические каналы утечки информации» являются:

- изучение основополагающих принципов защиты информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях;
- теоретическая и практическая подготовка по вопросам применения средств криптографической и технической защиты информации для решения задач профессиональной деятельности;
- практическая реализация применения необходимых физических законов и моделей для решения задач профессиональной деятельности.

Задачи дисциплины – дать основы по выявлению на объекте информатизации или в выделенном помещении технических каналов утечки информации; оценке уровня шумов/информативных сигналов/помех; оценке соответствия объекта информатизации или выделенного помещения требованиям по безопасности от утечки информации по техническим каналам.

Дисциплина «Технические каналы утечки информации» является базовой (общепрофессиональной) частью профессиональной компетенции и базируется на таких дисциплинах как, «Информатика», «Информационные технологии», «Алгоритмические языки», «Программирование».

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Освоение дисциплины «Технические каналы утечки информации» необходимо для успешного изучения дисциплин, связанных с проектированием и эксплуатацией информационных систем с применением современных методов защиты информации. Знание основ технической защиты информации в рамках информационных систем необходимо для успешного выполнения производственной практики и научно-исследовательской работы магистра.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УКЦ-1 Способен решать исследовательские, научно-технические и производственные задачи в условиях неопределенности, в том числе выстраивать деловую коммуникацию и организовывать работу команды с использованием цифровых ресурсов и технологий в цифровой среде	З-УКЦ-1 Знать: современные цифровые технологии, используемые для выстраивания деловой коммуникации и организации индивидуальной и командной работы. У-УКЦ-1 Уметь: подбирать наиболее релевантные цифровые решения для достижения поставленных целей и задач, в том числе в условиях неопределенности. В-УКЦ-1 Владеть: навыками решения исследовательских, научно-технических и производственных задач с использованием цифровых технологий.
УКЦ-2 Способен к самообучению, самоактуализации и саморазвитию с использованием различных цифровых технологий в условиях их непрерывного совершенствования	З-УКЦ-2 Знать: основные цифровые платформы, технологи и интернет ресурсы используемые при онлайн обучении. У-УКЦ-2 Уметь: использовать различные цифровые технологии для организации обучения. В-УКЦ-2 Владеть: навыками самообучения, самооактулизации и саморазвития с использованием различных цифровых технологий.

Профессиональные компетенции в соответствии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции**	**Код и наименование индикатора достижения профессиональной компетенции**
Тип задачи профессиональной деятельности: **проектно-конструкторский**			
Анализ состояния научно-технической проблематики	Материалы, компоненты, электронные приборы, устройства, установки, методы их исследования, проектирования и конструирования, математические модели, алгоритмы решения типовых задач, современное программное и информационное обеспечение процессов моделирования и проектирования изделий электроники и наноэлектроники	ПК-12.1 Способен выполнять анализ научно-технической информации по разработке оптотехники, оптических и оптико-электронных приборов и комплексов Профессиональный стандарт «29.004. Специалист в области проектирования и сопровождения производства оптотехники, оптических и оптико-электронных приборов и комплексов» С/01.7. Анализ научно-технической информации по разработке оптотехники, оптических и оптико-электронных приборов и комплексов	З-ПК-12.1 Знать: основные достижения и проблемы современной оптотехники. У-ПК-12.1 Уметь: анализировать состояние и перспективы развития оптотехники в целом и ее отдельных направлений. В-ПК-12.1 Владеть: навыками проведения поиска и анализа научно-технической информации

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ*

№ п/п	Наименование раздела /темы дисциплины	№ недели	Виды учебной работы					
			Лекции	Практ. занятия/ семинары	Лаб. работы	СРС	Текущий контроль (форма)*	Максимальный балл (см. п. 6.3)
			32	**16**		**96**		
Семестр № 3								
1.	**Концепция инженерно-технической защиты информации**		16	8		48		
1.1.	Тема 1		4	2		12	УО	5
1.2.	Тема 2		4	2		12	УО	5
1.3.	Тема 3		4	2		12	УО	5
1.4.	Тема 4		4	2		12	УО	5
Рубежный контроль		**8**					**УО**	20
2.	**Технические средства добывания и инженерно-технической защиты информации**		16	8		48		
2.1	Тема 5		4	2		12	УО	5
2.2	Тема 6		4	2		12	УО	5
2.3	Тема 7		4	2		12	УО	5
2.4	Тема 8		4	2		12	УО	10
Рубежный контроль		**15**					**Контр.**	25
Промежуточная аттестация			**Экзамен**				**36**	**0 - 50**
Посещаемость								**5**
Итого:								**100**

***Сокращение наименований форм текущего, рубежного и промежуточного контроля:**

УО – устный опрос
Контр. – контрольная работа
Тест ***– тестирование (письменный опрос)***
Э/Зач/ЗсО – экзамен/зачет/зачет с оценкой и др.

4.2. Содержание дисциплины, структурированное по разделам (темам)

Лекционный курс

№	Наименование раздела /темы дисциплины	Содержание
1.	**Концепция инженерно-технической защиты информации**	
1.1.	Тема 1	Характеристика инженерно-технической защиты информации. Технические средства и методы защиты информации. Основные проблемы и параметры инженерно-технической защиты информации. Представление методов и средств защиты информации как системы. Показатели эффективности инженерно-технической защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Основные направления инженерно-технической защиты информации. Принципы защиты информации техническими средствами.
1.2.	Тема 2	Информация как предмет защиты. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения и сигналов. Понятие о текущей и эталонной признаковой структуре. Источники опасных сигналов. Понятие об опасном сигнале. Опасные сигналы и их источники. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и характеристика основных и вспомогательных технических средств и систем. Побочные электромагнитные излучения и наводки. Виды побочных опасных электромагнитных излучений. Случайные антенны. Виды опасных сигналов на объектах информатизации. Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процедуры добывания информации технической разведкой. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки. Основные направления развития технической разведки.
1.3	Тема 3	Технические каналы утечки информации. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их возможности. Методы инженерной защиты и технической охраны объектов. Классификация методов инженерной защиты и технической охраны объектов. Инженерные конструкции. Автономные и централизованные системы охраны объектов.
1.4	Тема 4	Модели злоумышленников. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара. Методы скрытия информации и ее носителей.

		Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрытие радио и электрических сигналов. Виды и условия зашумления сигналов.
2.	**Технические средства добывания и инженерно-технической защиты информации**	
2.1.	Тема 5	Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки. Средства инженерной защиты и технической охраны. Методы и средства инженерной защиты и технической охраны объектов. Скрытие объектов наблюдения. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.
2.2.	Тема 6	Средства управления доступом. Классификация и характеристика охранных, охраннопожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны. Средства предотвращения утечки информации по техническим каналам. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Скрытие речевой информации в каналах связи. Энергетическое скрытие акустических информативных сигналов.
2.3.	Тема 7	Средства звукоизоляции из звукопоглощения. Обнаружение и локализация закладных устройств, подавление их сигналов. Подавление опасных сигналов акустоэлектрических преобразователей, экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания. Подавление опасных сигналов. Генераторы линейного и пространственного зашумления.
2.4.	Тема 8	Государственная система защиты информации. Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств. Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности защиты информации. Основные положения методологии инженерно-технической защиты информации. Требования по защите информации от утечки по техническим каналам. Методы расчета и инструментального контроля показателей защиты

		информации. Особенности инструментального контроля эффективности инженерно-технической защиты информации. Моделирование инженерно-технической защиты информации. Концепция и методы инженерно-технической защиты информации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации. Принципы оценки эффективности инженерно-технической защиты информации. Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в защищаемых помещениях. Принципы оценки размеров опасных зон I и II.

Практические/семинарские занятия

№	Наименование раздела /темы дисциплины	Содержание
1.	**Концепция инженерно-технической защиты информации**	
1.1.	Тема 1	Моделирование систем нелинейной локации.
1.2.	Тема 2	Моделирование пассивных фильтров (низкой и высокой частоты, полосовых и режекторных фильтров).
1.3	Тема 3	Моделирование активных фильтров.
1.4	Тема 4	Организационные мероприятия по подготовке и проведению аттестации объектов информатизации по требованиям безопасности.
2.	**Технические средства добывания и инженерно-технической защиты информации**	
2.1.	Тема 5	Статистический анализ загрузки заданного радиодиапазона и обнаружение радио-закладных устройств в охраняемом помещении.
2.2.	Тема 6	Нелинейная локация Обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля. Охрана выделенных помещений. Пожарная сигнализация. Охранная сигнализация.
2.3.	Тема 7	Ограничение доступа в выделенное помещение. Система контроля и управления доступом. Охрана выделенных помещений. Система видеонаблюдения.
2.4.	Тема 8	Оценка эффективности работы системы активной защиты информации и контроль защищенности помещения от утечек речевой информации по техническим каналам.

4.3. Перечень учебно-методического обеспечения для самостоятельной работы студентов

1 Методические указания по выполнению тестовых и практических заданий по дисциплине «Технические каналы утечки информации» / СарФТИ НИЯУ МИФИ, Саров, 2021.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

5.1. Паспорт фонда оценочных средств по дисциплине

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Раздел	Темы занятий	Компетенция	Индикаторы освоения	Текущий контроль, неделя
Семестр 3				
Раздел 1	Тема 1.	УКЦ-1 УКЦ-2 ПК-12.1	З-УКЦ-1; У-УКЦ-1; В-УКЦ-1	УО - 1
	Тема 2.		З-УКЦ-2; У-УКЦ-2; В-УКЦ-2	УО - 3
	Тема 3.		З-УКЦ-2; У-УКЦ-2; В-УКЦ-2	УО - 5
	Тема 4.		З-ПК-12.1; У-ПК-12.1; В-ПК-12.1	УО - 7
Рубежный контроль		УКЦ-1 УКЦ-2 ПК-12.1	З-УКЦ-1; У-УКЦ-1; В-УКЦ-1	УО – 7
			З-УКЦ-2; У-УКЦ-2; В-УКЦ-2	
			З-ПК-12.1; У-ПК-12.1; В-ПК-12.1	
Раздел 2	Тема 5.	УКЦ-1 УКЦ-2 ПК-12.1	З-УКЦ-1; У-УКЦ-1; В-УКЦ-1	УО - 9
	Тема 6.		З-УКЦ-2; У-УКЦ-2; В-УКЦ-2	УО - 11
	Тема 7.		З-УКЦ-2; У-УКЦ-2; В-УКЦ-2	УО - 13

	Тема 8.		З-ПК-12.1; У-ПК-12.1; В-ПК-12.1	УО - 15
Рубежный контроль		УКЦ-1 УКЦ-2 ПК-12.1	З-УКЦ-1; У-УКЦ-1; В-УКЦ-1	Тест – 15 (16)
			З-УКЦ-2; У-УКЦ-2; В-УКЦ-2	
			З-ПК-12.1; У-ПК-12.1; В-ПК-12.1	
Промежуточная аттестация		УКЦ-1 УКЦ-2 ПК-12.1	З-УКЦ-1; У-УКЦ-1; В-УКЦ-1	**Экзамен**
			З-УКЦ-2; У-УКЦ-2; В-УКЦ-2	
			З-ПК-12.1; У-ПК-12.1; В-ПК-12.1	

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

5.2.1. Примерные вопросы к экзамену или зачету

а) типовые вопросы (задания):

1. Дайте определение информации, документированной информации. Каково отличие государственной тайны, конфиденциальной информации и открытой информации

2. Классификация технической разведки. Эффективность добывания информации технической разведкой.

3. Государственная система защиты информации. Эффективность защиты информации.

4. Основные объекты защиты информации.

5. Дайте определение демаскирующих признаков. Для чего они используются. Приведите примеры.

6. Дайте определение терминам Контролируемая зона, Опасная зона, Опасная зона 1, Опасная зона 2.

7. Состав технического канала утечки информации.

8. Классификация технических каналов утечки информации.

9. Перечислите технические каналы утечки информации, обрабатываемой ОТСС. Приведите примеры.

10. Перечислите технические каналы утечки информации при передаче по каналам связи. Приведите примеры.

11. Перечислите каналы утечки речевой информации. Приведите примеры.

12. Перечислите каналы утечки видовой информации. Приведите примеры.

13. Каково влияние паразитных емкостных, индуктивных и резистивных связей в каналах

14. Перечислите методы противодействия утечке информации по техническим каналам.

15. Способы скрытого видеонаблюдения. Характеристики оборудования для скрытого видеонаблюдения

16. Способы скрытого прослушивания переговоров в помещении. Демаскирующие признаки радиозакладок. Демаскирующие признаки проводных закладок.

17. Способы прослушивания переговоров по телефонным линиям. Демаскирующие признаки акустических закладок типа «телефонное ухо».

18. Направленные микрофоны. Принцип действия.

19. Охранные системы. Назначение. Структура. Приведите примеры охранных систем объектов и помещений.

20. Датчики охранных систем. Принципы действия датчиков.

21. Охранное видеонаблюдение. Назначение. Структура. Основные характеристики.

22. Средства радиотехнической разведки. Состав. Характеристики.

23. Охрана объектов. Особенности охраны объектов различного класса. Задачи средств охраны объектов.

24. Периметровые средства охраны. Датчики периметровых систем охраны.

25. Охрана выделенных (защищаемых) помещений. Технические средства охраны помещений.

26. Экранирование электромагнитных волн.

27. Экранирование акустических сигналов.

28. Фильтрация опасных сигналов. Приведите примеры.

29. Маскировка опасных сигналов зашумлением. Приведите примеры.

30. Металлодетекторы. Сферы применения. Принцип действия.

31. Локаторы нелинейностей. Сферы применения. Принцип действия.

32. Аттестация объектов информатизации по требованиям безопасности. Назначение. Порядок проведения аттестации.

33. Специальная проверка. Специальное обследование. Специальное исследование.

34. Проведение измерений акустических и виброакустических характеристик. Приведите примеры.

35. Проведение измерений побочных электромагнитных излучений. Приведите примеры.

б) критерии оценивания компетенций (результатов):

балльно-рейтинговая система

в) описание шкалы оценивания:

приведено в п 5.3.

5.2.2. Примерные вопросы для устного опроса

а) типовые задания (вопросы) - образец:

1. Какие свойства информации, влияющие на ее безопасность, вы знаете?
2. Определите виды, источники и носители защищаемой информации.
3. Основные направления инженерно-технической защиты информации.
4. Какие основные характеристики технических каналов утечки информации вы знаете?
5. Структура, классификация и основные характеристики технических каналов утечки информации.
6. Перечислите принципы защиты информации техническими средствами.
7. Что такое модель и моделирование?
8. Что такое аналитическая модель системы?
9. Моделирование случайных величин и их законы распределения.
10. Какие числовые характеристики случайных величин вы знаете?
11. Демаскирующие признаки объектов наблюдения, сигналов и веществ.
12. Какие статистические оценки знаете? Как определить их точность?
13. Аппроксимация результатов статистического моделирования.
14. Что такое адекватная модель?
15. Принципы моделирования объектов защиты.
16. Моделирование угроз безопасности информации.
17. Методические рекомендации по выбору рациональных вариантов защиты.
18. Основные понятия теории случайных процессов.
19. Классификация и основные характеристики случайных процессов.
20. Перечислите задачи защиты информации ТКС в условиях конфликта.
21. Понятие конфликта. Способы разрешения конфликта в ТКС.
22. Понятия стратегия, тактика обеспечения защиты информации, воздействия на ТКС.
23. Конфликтная матрица реализации стратегий (тактик) защиты и воздействия.

24. Какие виды контроля эффективности инженерно-технической защиты информации вы знаете?

25. Какие предъявляются требования по защите информации от утечки по техническим каналам?

26. Дайте классификацию методов и средств защиты информации от технических разведок.

27. Математическая модель канала утечки информации применительно к техническим разведкам.

б) критерии оценивания компетенций (результатов):

балльная система

в) описание шкалы оценивания:

правильный ответ – весовой коэффициент оценки в баллах, неправильный ответ – 0 баллов.

5.2.3. Наименование оценочного средства (тест**)**

а) типовые задания (вопросы) - образец:

1. Какой канал утечки информации использует эффект высокочастотного облучения для перехвата информации обрабатываемой в технических средствах?

1) Акустоэлектрический

2) Параметрический

3) Электрический

4) Электромагнитный

2. При передаче информации по каналам связи, какой канал утечки информации возникает в результате возникновения вокруг высокочастотного кабеля электромагнитного поля?

1) Электромагнитный канал

2) Индукционный канал

3) Паразитные связи

4) Электрический канал

3. Каким из каналов утечки речевой информации является окно?

1) Акустическим

2) Виброакустическим

3) Оптическим

4) Все варианты

4. Как называется устройство про помощи которого выполняется измерение ограждающих конструкций при проведении виброакустических измерений разборчивости речи?

1) Акселерометр

2) Микрофон

3) Акустический излучатель

4) Лучевая трубка

5. Какой канал утечки информации возникает за счет преобразований акустических сигналов в электрические различными радиоэлектронными устройствами, обладающими «микрофонным эффектом», а также путем «высокочастотного навязывания»?

1) Акустоэлектрический канал

2) Оптико-электронный канал

3) Гидроакустичекий канал

4) Вибрационный канал

6. Устройство, используемое для проведения измерений ТС на побочные электромагнитные излучения (ПЭМИ)?

1) Анализатор спектра

2) Шумомер

3) Низкочастотный анализатор

4) Все варианты

7. Устройства, подлежащие исследованию на побочные электромагнитные излучения и наводки (ПЭМИН)?

1) Накопители на жестких дисках

2) Принтер

3) Клавиатура

4) Все варианты

8. Каким каналом утечки речевой информации являются системы отопления в помещении?

1) Акустический

2) Видовой

3) Виброакустический

4) Все варианты

9. Каким каналом утечки речевой информации является дверь в выделенное помещение?

1) Параметрический

2) Видовой

3) Акустический

4) Оптико-электронный

10. Что из нижеперечисленного НЕ относится к акустическому каналу утечки речевой информации?

1) Окно

2) Дверь

3) Батареи и трубы отопления

4) Все варианты

б) критерии оценивания компетенций (результатов):

балльная система

в) описание шкалы оценивания:

правильный ответ – весовой коэффициент оценки в баллах, неправильный ответ – 0 баллов.

5.3. Шкалы оценки образовательных достижений

Рейтинговая оценка знаний является интегральным показателем качества теоретических и практических знаний и навыков студентов по дисциплине и складывается из оценок, полученных в ходе текущего контроля и промежуточной аттестации.

Результаты текущего контроля и промежуточной аттестации подводятся по шкале балльно-рейтинговой системы.

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, использует в ответе материал монографической литературы.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется

75-84		C	студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
70-74		D	
65-69	3 – «*удовлетворительно*»		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64		E	
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. Инженерно-техническая защита. информации: Учебное пособие / А. А. Титов - 2010. 195 с.

2. Технические средства охраны: Учебное пособие / А. Н. Дементьев, Г. В. Дементьева - 2012. 119 с.

3. Основы информационной безопасности / В.А. Минаев, С.В. Скрыль, А.П. Фисун, В.Е. Потанин, С.В. Дворянкин. - Воронеж: Воронежский инсти-тут МВД России, 2001. - 464с.

4. Основы системных исследований телекоммуникаций сис-тем в аспекте обеспечения информационной безопасности : учеб. пособие / И. В. Владимиров. - Воронеж : ГОУВПО "Воронежский государственный тех-нический университет", 2006.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

1. Технические средства защиты информации: Учебное пособие / А.А.Титов - 2010. 194с.

2. Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1.

3. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ.

4. Закон Российской Федерации «О персональных данных» от 27 июля 2006 г. №152-ФЗ.

5. Зайцев, Александр Петрович. Технические средства обеспечения информационной безопасности: Учебное пособие для вузов. Ч. 2 : Средства защиты информации по техническим каналам : учебное пособие. - Томск : ТМЦДО , 2004. - 279 с.

6. Зайцев, Александр Петрович. Технические средства обеспечения информационной безопасности: Учебное пособие для вузов. Ч. 1 : Технические каналы утечки информации. – Томск : ТМЦДО , 2004. - 199 с.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. Национальная платформа открытого образования

7 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Освоение дисциплины производится на базе учебных лабораторий кафедры в СарФТИ НИЯУ МИФИ. Лаборатории оснащены современным оборудованием, позволяющим проводить практические и лабораторные занятия. Выполнение лабораторных работ, а также самостоятельной работы студентов осуществляется на рабочих местах, оснащенных макетами.

В качестве материально-технического обеспечения используются также ресурсы и программно-аппаратное обеспечение компьютерного класса.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При чтении лекционного материала используется электронное сопровождение курса: справочно-иллюстративный материал воспроизводится и озвучивается в аудитории с использованием проектора и переносного компьютера в реальном времени.

По дисциплине «Технические каналы утечки информации» в рабочем учебном плане предусмотрены интерактивные часы для проведения практических занятий.

Данный вид деятельности реализуется с помощью видео лекций ведущих специалистов в области информационной безопасности.

9. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ СТУДЕНТАМ ПО ОРГАНИЗАЦИИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Изучение данного курса обеспечивает студента сведениями о современном состоянии в области технической защиты информации. Курс существенно расширяет и углубляет знания, полученные студентами при изучении дисциплины «Технические каналы утечки информации». Материал курса основан на последних достижениях зарубежных и отечественных специалистов как в классических областях применения, так и в новых, связанных с новыми информационными технологиями.

Существенное место в курсе уделено и стандартным методам и рекомендациям технической защиты информации, позволяющим существенно ускорить разработку и внедрение новых систем.

Рекомендации преподавателю

Предлагается:

При изучении теоретического курса работать с обучающими и контролирующими программами, содержащими учебный материал по отдельным вопросам курса.

При проведении практических работ применять расчетные программы, а также контролирующие программы по проверке усвоения студентом знаний, полученных при выполнении практических работ.

Рекомендации студенту

Предлагается:

- Самостоятельно прорабатывать лекционный материал для более полного усвоения материала;
- В учебном процессе при выполнении практикума эффективно использовать методические пособия и методический материал;
- Активно использовать Интернет-ресурсы для получения актуального материала по изучаемой дисциплине;
- Активно использовать Интернет-ресурсы для обновления инструментальной базы (систем программирования, инструментальных сред и т.д.) при выполнении лабораторных работ.

Рабочая программа дисциплины составлена в соответствии с ОС НИЯУ МИФИ (ФГОС) и учебным планом основной образовательной программы (программ).

Автор(ы): старший преподаватель кафедры РФЭ А.А. Евстифеев