МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ С.И. Лукьянов

26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки (специальность)
10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Направленность (профиль/специализация) программы
10.05.03 специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем";

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	3, 4
Семестр	6, 7

Магнитогорск
2020 год

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ (приказ Минобрнауки России от 01.12.2016 г. № 1509)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
18.02.2020, протокол № 6

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
зав. кафедрой ИиИБ, д-р техн. наук _____ И.И. Баранкова

Рецензент:
Начальник отдела информационной безопасности "КУБ" (АО) ,
_____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целью дисциплины «Техническая защита информации» является формирование профессиональных навыков обеспечения информационной защиты от съема информации по техническим каналам утечки информации, использования методов и средств инженерно-технической защиты информации и подготовка к деятельности, связанной с эксплуатацией и обслуживанием современных технических средств защиты информации в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Техническая защита информации» рассматривает основные принципы и основные направления технической защиты информации.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Техническая защита информации входит в базовую часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Организация ЭВМ и вычислительных систем

Введение в специальность

Физика

Основы радиотехники

Теория информации

Основы информационной безопасности

Электроника и схемотехника

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Управление информационной безопасностью

Разработка и эксплуатация защищенных автоматизированных систем

Информационная безопасность распределенных информационных систем

Аттестация АИС

Тестирование систем защиты информации автоматизированных систем

Методы мониторинга информационной безопасности АС

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Подготовка к защите и защита выпускной квалификационной работы

Подготовка к сдаче и сдача государственного экзамена

Производственная-преддипломная практика

Научно-исследовательская работа

Обеспечение информационной безопасности критической информационной инфраструктурой

Методы проектирования систем защиты распределенных информационных систем

Защита информационно-технологических ресурсов автоматизированных систем

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Техническая защита информации» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения

ПК-14 способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	
Знать	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по технической защите информации. Способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации. Способы контрольных проверок работоспособности применяемых технических средств защиты информации. Способы контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации.
Уметь	Участвовать в настройке технических средств обеспечения информационной безопасности. Самостоятельно настраивать технические средства обеспечения информационной безопасности. Исследовать эффективность контрольных проверок работоспособности применяемых технических средств защиты информации. Применять технические средства обеспечения информационной безопасности. Исследовать эффективность контрольных проверок работоспособности применяемых технических средств обеспечения информационной безопасности.
Владеть	Техникой настройки технических средств обеспечения информационной безопасности. Навыками использования технических средств обеспечения информационной безопасности автоматизированных систем. Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.
ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	
Знать	Классификацию технических средств перехвата информации Возможности технических средств перехвата информации Организацию защиты информации от утечки по техническим каналам на объектах информатизации.
Уметь	Классифицировать технические средства перехвата информации. Участвовать в организации защиты информации от утечки по техническим каналам на объектах информатизации Самостоятельно организовывать защиту информации от утечки по техническим каналам на объектах информатизации.
Владеть	Средствами технической защиты информации. Методами технической защиты информации. Методами и средствами технической защиты информации.
ОПК-1 способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач	

Знать	Физические основы функционирования систем обработки и передачи информации. Принципы построения средств защиты информации от утечки по техническим каналам. Технические каналы утечки информации. Технические средства контроля эффективности мер защиты информации.
Уметь	Контролировать безотказное функционирование технических средств защиты информации. Восстанавливать отказавшие технические средства защиты информации. Заменять отказавшие технические средства защиты информации.
Владеть	Навыками работы с нормативными правовыми актами в области технической защиты информации. Навыками организации защиты информации от утечки по техническим каналам на объектах информатизации.

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 6 зачетных единиц 216 акад. часов, в том числе:

– контактная работа – 125,45 акад. часов:
– аудиторная – 119 акад. часов;
– внеаудиторная – 6,45 акад. часов
– самостоятельная работа – 54,85 акад. часов;
– подготовка к экзамену – 35,7 акад. часа

Форма аттестации - зачет, курсовой проект, экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Общие положения защиты информации техническими средствами								
1.1 Предмет и содержание дисциплины. Физические основы функционирования систем обработки и передачи информации	6	2	3/2И			Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к тестированию	Контрольное тестирование	ОПК-1
1.2 Задачи защиты информации от утечки по техническим каналам.		1	2			Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к тестированию	Контрольное тестирование	ОПК-1
1.3 Методы и средства инженерной защиты объектов. Системы охранно-тревожной сигнализации. Системы пожарной сигнализации		1	1			Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе	Лабораторная работа	ПК-14

Итого по разделу		4	6/2И					
2. Технические каналы утечки информации								
2.1 Условия и особенности утечки информации. Структура канала утечки. Виды технических каналов утечки информации	6	3	4			Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе	Лабораторная работа	ПК-14, ПК-17, ОПК-1
2.2 Условия образования каналов утечки. Характеристики каналов утечки информации		2	4/2И		2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе	Лабораторная работа	ПК-14, ПК-17, ОПК-1
Итого по разделу		5	8/2И		2			
3. Акустический канал утечки информации								
3.1 Виды акустических каналов утечки информации. Способы перехвата и средства съема информации по акустическому каналу	6	2	5/3И		2	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе	Лабораторная работа	ПК-14, ПК-17, ОПК-1
3.2 Способы и средства защиты от съема информации по акустическому каналу. Системы защиты от утечки информации по акустическому каналу		2	5/1И		3	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе	Лабораторная работа	ПК-14, ПК-17, ОПК-1
Итого по разделу		4	10/4И		5			
4. Вибрационный канал утечки информации								

4.1 Виды вибрационных каналов утечки информации. Способы перехвата и средства съема информации по вибрационному каналу	6	2	5/3И		3	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	ПК-14, ПК-17, ОПК-1
4.2 Способы и средства защиты от съема информации по вибрационному каналу. Системы защиты от утечки информации по вибрационному каналу.		2	5/3И		4	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	ПК-14, ПК-17, ОПК-1
4.3 Подготовка к зачету					6,05	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к зачету	Зачет	ПК-14, ПК-17, ОПК-1
Итого по разделу		4	10/6И		13,05			
Итого за семестр		17	34/14И		20,05		зачёт	
5. Электромагнитный канал утечки информации								
5.1 Виды электромагнитных каналов утечки информации. Способы перехвата и средства съема информации по электромагнитному каналу.	7	6	4/2И		4	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	ПК-14, ПК-17, ОПК-1

5.2 Способы и средства защиты от съема информации по электромагнитному каналу. Системы защиты от утечки информации по электромагнитному каналу		4	4/2И		3,5	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	ПК-14, ПК-17, ОПК-1
Итого по разделу		10	8/4И		7,5			
6. Оптический канал утечки информации								
6.1 Виды оптических каналов утечки информации. Способы перехвата и средства съема информации по оптическому каналу	7	4	4/2И		4	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	ПК-14, ПК-17, ОПК-1
6.2 Способы и средства защиты от съема информации по оптическому каналу. Системы защиты от утечки информации по оптическому каналу		4	4/2И		5	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	ПК-14, ПК-17, ОПК-1
Итого по разделу		8	8/4И		9			
7. Электросетевой канал утечки информации								
7.1 Виды электросетевых каналов утечки информации. Способы перехвата и средства съема информации по электросетевому каналу	7	4	4/2И		4	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	ПК-14, ПК-17, ОПК-1

7.2 Способы и средства защиты от съема информации по электросетевому каналу. Системы защиты от утечки информации по электросетевому каналу		4	4/3И		5	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	ПК-14, ПК-17, ОПК-1
Итого по разделу		8	8/5И		9			
8. Поиск средств несанкционированного съема информации								
8.1 Организационные и технические мероприятия по защите информации в учреждениях и на предприятиях.	7	4	5/1И		5	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	ПК-14, ПК-17, ОПК-1
8.2 Контроль эффективности мер по защите информации техническими средствами		4	5		4,3	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к лабораторной работе и контрольному тестированию	Лабораторная работа Контрольное тестирование	ПК-14, ПК-17, ОПК-1
Итого по разделу		8	10/1И		9,3			
Итого за семестр		34	34/14И		34,8		экзамен, кп	
Итого по дисциплине		51	68/28И		54,85		зачет, курсовой проект, экзамен	ОПК-1,ПК-14,ПК-17

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. Формы учебных занятий с использованием традиционных технологий:

a) Вводная лекция – для целостного представления об учебном предмете и анализа учебно-методической литературы;

b) Обзорные лекции – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;

c) Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя);

d) Семинар – беседа преподавателя и обучающихся, обсуждение заранее подготовленных сообщений по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы;

e) Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму;

f) Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2) Разделно-компетентностная технология, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. Формы учебных занятий с использованием Разделно-компетентностной технологии:

a) Кейс-методы – для овладения системой знаний и умений и творческого их использования в профессиональной деятельности и самообразовании; для квалифицированного и независимого решения профессиональных задач; для ориентации в многообразии учебных программ, пособий, литературы и выбора наиболее эффективных в применении к конкретной ситуации; для осуществления саморефлексии для дальнейшего профессионального, творческого роста и социализации личности.

3) Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды. Формы учебных занятий с использованием интерактивных технологий:

a) Case-study – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения проблемы.

b) Методы IT – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающихся с использованием *методов IT*.

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде чтения литературы по соответствующему разделу с проработкой материала и выполнения домашних заданий с консультациями преподавателя, а также с применением *Кейс-технологий*.

Задания и вопросы по разделам

Раздел 1-4

Вопросы:

1. Виды, источники и носители защищаемой информации.
2. Опасные сигналы и их источники.
3. Классификация технической разведки, основные этапы и процедуры добывания информации технической разведкой.
4. Характеристики технических каналов утечки информации.
5. Комплексное использование каналов утечки информации.
6. Средства обнаружения и локализации закладных устройств.
7. Материально-вещественные каналы утечки информации.
8. Задачи защиты информации от утечки по техническим каналам.
9. Одноканальный канал утечки информации.
10. Носители информации в акустическом канале.

Задания:

1. Маскирование речевых сигналов акустическими шумами с использованием системывиброакустической и акустической защиты Соната-АВ (модель 3М).
2. Защита речевой информации от съема по вибрационному каналу с использованием системывиброакустической и акустической защиты Соната-АВ (модель 3М).
3. Вычислить мощность радиосигнала в канале CDMAс использованием анализатора спектра «АКС-1301».

Раздел 5-8

Вопросы:

1. Случайные опасные сигналы.
2. Диапазоны частот радиоэлектронного канала.
3. Носители информации в оптическом канале.
4. Оптические диапазоны частот.
5. Электрические приборы, создающие случайные опасные сигналы.
6. Пропускная способность канала.
7. Перехват акустических колебаний: через ВТСС, обладающих “микрофонным эффектом”.
8. Стетоскопы, комплексированные с устройствами передачи информации по оптическому каналу в ИК-диапазоне длин волн.
9. Перехват акустических сигналов путем: лазерного зондирования оконных стекол.

Задания:

1. Изучить устройство и принципы работы комплекса радиомониторинга и цифрового анализа сигналов «Кассандра».

2. Обнаружение устройств и анализ сети Wi-Fi с использованием комплекса радиомониторинга и цифрового анализа сигналов «Кассандра».
3. Обеспечить маскировку информативных ПЭМИН устройств вычислительной техники, размещённой в помещении с использованием генератора радиошума ГШ-1000М.
4. Обеспечить подавление нормальной работы телефонных закладок любых типов подключения во время переговоров с использованием устройства защиты Прокруст 2000.
5. Обеспечить защиту линий электропитания и заземления от утечки информации с использованием устройства для защиты линий электропитания и заземления от утечки информации «Соната-РС2».

7 Оценочные средства для проведения промежуточной аттестации

Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-14 - способность проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации**.**		
Знать	Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по технической защите информации. Способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации. Способы контрольных проверок работоспособности и эффективности применяемых технических средств защиты информации.	Вопросы к экзамену 1. Характеристики способов и средств наблюдения в оптическом диапазоне. 2. Характеристики зрительной системы человека. 3. Виды и характеристики объективов. 4. Визуально-оптические приборы (бинокли, трубы. Телескопы) 5. Приборы ночного видения и тепловизоры. 6. Способы и средства наблюдения в радиодиапазоне. 7. Задачи, решаемые при перехвате сигналов и структура типового комплекса для перехвата. 8. Виды и характеристики антенн. 9. Радиоприёмники и их характеристики. 10. Способы и средства прослушивания, слуховая система человека. 11. Стетоскопы и телефонные закладки. 12. Метод ВЧ-навязывания и его применение для добывания информации. 13. Характеристики закладных устройств, затрудняющие их обнаружение. 14. Средства и методы (не меньше двух) обнаружения закладных устройств.
Уметь	Участвовать в настройке технических средств обеспечения информационной	Задания: 1. Замаскировать речевые сигналов акустическими шумами в аудитории с использованием системы виброакустической

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	безопасности. Самостоятельно настраивать технические средства обеспечения информационной безопасности. Исследовать эффективность контрольных проверок работоспособности применяемых технических средств защиты информации. Применять технические средства обеспечения информационной безопасности. Исследовать эффективность контрольных проверок работоспособности применяемых технических средств обеспечения информационной безопасности.	и акустической защиты Соната-АВ (модель 3М). 2. Обеспечить защиту речевой информации от съема по вибрационному каналу в аудитории с использованием системы виброакустической и акустической защиты Соната-АВ (модель 3М). 3. Вычислить мощность радиосигнала в канале CDMA с использованием анализатора спектра «АКС-1301». 4. Настроить СЗИ Соната-АВ. 5. Провести исследование систем активного зашумления и расчет показателей их эффективности с использованием комплекса «Сигурд». 6. Рассчитать отношения «сигнал/шум» в отходящих линиях с использованием комплекса «Сигурд».
Владеть	Техникой настройки технических средств обеспечения информационной безопасности. Навыками использования технических средств обеспечения информационной безопасности автоматизированных систем. Навыками анализа архитектурно-технических и схемотехнических решений компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.	1. С использованием комплекса «Кассандра» определить количество пиковых сигналов в заданном диапазоне частот. Провести полный анализ каждого пикового сигнала. Установить пояснительные метки на все пиковые сигналы. Вывести спектрограмму заданного диапазона частот, графики накопленных максимумов. Найти сигнал максимальной мощности и пометить его. 2. С использованием комплекса «Кассандра» в заданном диапазоне частот регистрировать и заносить в список слабые шумоподобные сигналы. Регистрировать факт наличия излучения на заданной частоте. Провести анализ определения линии порога с использованием критерия «идеального наблюдателя» и критерия Неймана-Пирсона. Обосновать способ создания линии порога. 3. Найти радиозакладку с помощью комплекса радиомониторинга «Кассандра». 4. С использованием комплекса «Кассандра» создать базу данных легальных сигналов и создать на ее основе эталонную панораму частот. Найти разность эталонной и текущей панорам.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-17 - способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации.		
Знать	Классификацию технических средств перехвата информации Возможности технических средств перехвата информации Организацию защиты информации от утечки по техническим каналам на объектах информатизации.	Вопросы к экзамену 1. Способы подключения и защита телефонной линии. 2. Конфиденциальное совещание: несанкционированный съём информации и методы защиты от него. 3. Беззаходовые методы прослушивания помещений по ТЛ. 4. Мобильные системы связи и их использование в информационных атаках. 5. Защита информации от атак с помощью сотовых телефонов и диктофонов. 6. Оптические каналы утечки информации (атака и защита). 7. Радиоэлектронные каналы утечки информации. 8. Пассивные и активные методы защиты информации в радиоэлектронном канале. 9. Способы и принципы инженерно технической защиты информации. 10. Способы и средства инженерной защиты и технической охраны объектов. 11. Утечка информации по ПЭМИН и применяемые меры защиты. 12. Зоны электромагнитного поля и возможности утечки информации. 13. Контролируемая зона и критерий защищённости СВТ.
Уметь	Классифицировать технические средства перехвата информации. Участвовать в организации защиты информации от утечки по техническим каналам на объектах информатизации Выявлять каналы утечки информации Проводить контроль эффективности мер по защите информации техническими средствами	Задания: 1. Изучить устройство и принципы работы комплекса радиомониторинга и цифрового анализа сигналов «Кассандра». 2. Обнаружить устройства и проанализировать сети Wi-Fi с использованием комплекса радиомониторинга и цифрового анализа сигналов «Кассандра». 3. Обеспечить маскировку информативных ПЭМИН устройств вычислительной техники, размещённой в аудитории МГТУ с использованием генератора радиошума ГШ-1000М. 4. Обеспечить подавление нормальной работы телефонных закладок любых типов подключения во время переговоров с использованием устройства защиты

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Прокруст 2000 в аудитории МГТУ.
Владеть	Средствами технической защиты информации. Методами технической защиты информации. Навыками проведения проверки защищенности информации и эффективности мер по защите информации	1. Провести исследование ТС на наличие информативных сигналов ПЭМИН с использованием комплекса «Сигурд». 2. Произвести расчет показателей защищенности технических средств от утечки информации по каналу ПЭМИН в соответствии с действующими нормативными документами с использованием комплекса «Сигурд».
ОПК-1 - способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач.		
Знать	Физические основы функционирования систем обработки и передачи информации. Основные физические явления и законы, используемые при построении средств защиты информации от утечки по техническим каналам. Технические каналы утечки информации.	**Вопросы для зачета** 1. Направленные и лазерные микрофоны. 2. Типы микрофонов и их характеристики. 3. Закладные устройства и их характеристики. 4. Требования защиты информации. 5. Методы и средства защиты речевой информации. 6. Физические АЭП - преобразователи – источники опасных сигналов. 7. Характеристики технических каналов утечки информации. 8. Пассивные и активные методы защиты информации в акустическом канале. 9. Материально-вещественные каналы утечки информации. 10. Акустические каналы утечки информации.
Уметь	Применять соответствующий математический аппарат при проведении расчетов защищенности информации Контролировать безотказное функционирование технических средств защиты информации. Заменять отказавшие технические средства защиты информации.	Задания: 1. Проверить работоспособность генератора шума ГШ-1000М для защиты информации от утечки за счёт побочных электромагнитных излучений. 2. Проверить работоспособность устройства защиты Прокруст 2000. 3. Проверить работоспособность устройства для подавления сигнала сотовой связи.
Владеть	Навыками работы с	1. С использованием графического метода

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	нормативными правовыми актами в области технической защиты информации. Навыками организации защиты информации от утечки по техническим каналам на объектах информатизации.	рассчитать радиус зоны R2 для ЭВТ. 2. Рассчитать показатель защищенности технических средств обработки и передачи цифровой речи по каналу ПЭМИ. 3. Рассчитать показатель защищенности цифровой речи в радиоканале. 4. Для представленной схемы помещения выбрать контрольные точки (КТ) и разработать схемы измерений по акустическому каналу для этих КТ. 5. Проанализировать математическую модель утечки речевой информации по акустическому каналу. 6. Проанализировать математическую модель утечки речевой информации по виброакустическому каналу. 7. Проанализировать математическую модель утечки речевой информации по каналам, использующим перехват электромагнитных и электрических сигналов. 8. Проанализировать математическую модель утечки речевой информации по лазерному каналу.

Темы курсовых работ:

1. Расчет выполнения норм противодействия акустической речевой разведке для выбранного помещения МГТУ.

2. Проектирование эффективного комплекса защиты акустической информации для выбранного помещения МГТУ.

4. Расчет выполнения норм виброакустической защищенности для выбранного помещения МГТУ.

5. Оценка защищенности средств вычислительной техники от утечки информации за счет ПЭМИ для выбранного помещения МГТУ.

7. Аналитическое обоснование необходимости разработки системы технической защиты информации на основе специального исследования выделенного помещения на базе МГТУ.

8. Экспериментальное исследование и расчет основных параметров воздушного канала утечки информации.

9. Экспериментальное исследование и расчет основных параметров акустоэлектрического канала утечки речевой информации.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Показатели и критерии оценивания зачета:

– на «зачтено» – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации**;**

– на «не зачтено» – обучающийся не может показать знания на уровне воспроизведения и объяснения информации**.**

Показатели и критерии оценивания экзамена:

– на оценку **«отлично»** – обучающийся должен показать высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные

навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку **«хорошо»** – обучающийся должен показать средний уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач;

– на оценку **«удовлетворительно»** – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;

– на оценку **«неудовлетворительно»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.

Показатели и критерии оценивания курсовой работы:

– на оценку **«отлично»** (5 баллов) – работа выполнена в соответствии с заданием, обучающийся показывает высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку **«хорошо»** (4 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам;

– на оценку **«удовлетворительно»** (3 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания на уровне воспроизведения и объяснения информации, интеллектуальные навыки решения простых задач;

– на оценку **«неудовлетворительно»** (2 балла) – задание преподавателя выполнено частично, в процессе защиты работы обучающийся допускает существенные ошибки, не может показать интеллектуальные навыки решения поставленной задачи.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Баранкова И.И. Техническая защита информации. Лабораторный практикум [Электронный ресурс]: учебное пособие / И. И. Баранкова, У. В. Михайлова, Г. И. Лукьянов; МГТУ. - Магнитогорск: МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - Режим доступа: https://magtu.informsystema.ru/uploader/fileUpload?name=2935.pdf&show=dcatalogues/1/1134667/2935.pdf&view=true . - Макрообъект*.

2. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901 (дата обращения: 26.02.2019)

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru .
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта.

Примечание: при открытии макрообъектов учитывать особенности настройки антивирусной защиты

б) Дополнительная литература:

1. Румянцев, К. Е. Алгоритмы обнаружения источников оптического излучения : учебник / К. Е. Румянцев ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2019. - 232 с. - ISBN 978-5-9275-3201-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1088145 (дата обращения: 26.02.2019)

А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772 (дата обращения: 24.02.2020).

в) Методические указания:

1. Баранкова И.И. Применение комплекса радиомониторинга для постобработки спектограмм [Текст]: метод. указания к лабораторным и практическим занятиям по дисциплине «Техническая защита информации» для обучающихся по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Обеспечение информационной безопасности распределенных информационных систем» / Михайлова У.В., Лукьянов Г.И. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2016. – 18 с.

2. Баранкова И.И. Защита телефонных линий с использованием прибора «Прокруст-2000» [Текст]: метод. указания к лабораторным и практическим занятиям по дисциплине «Техническая защита информации» для обучающихся по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Обеспечение информационной безопасности распределенных информационных систем» / Михайлова У.В., Калугина О.Б., Лукьянов Г.И. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2016. – 20 с.

3. Баранкова И.И. Поиск радиозакладок с применением комплекса радиомониторинга [Текст]: метод. указания к лабораторным и практическим занятиям по дисциплине «Техническая защита информации» для обучающихся по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Обеспечение информационной безопасности распределенных информационных систем» / Михайлова У.В., Лукьянов Г.И. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2016. – 12 с.

4. Баранкова И.И. Использование комплекса радиомониторинга для построения графиков текущих значений сканируемых частот [Текст]: метод. указания к лабораторным и практическим занятиям по дисциплине «Техническая защита информации» для обучающихся по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Обеспечение информационной безопасности распределенных информационных систем» / Михайлова У.В., Лукьянов Г.И. – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2016. – 18 с.

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно

LibreOffice	свободно распространяемое ПО	бессрочно
MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
MS Windows XP Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2003 Professional	№ 135 от 17.09.2007	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название ресурса	Ссылка
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/

Федеральное государственное бюджетное учреждение «Федеральный институт	URL: http://www1.fips.ru/
Национальная информационно-аналитическая система –	URL: https://elibrary.ru/project_risc.asp
Электронные ресурсы библиотеки МГТУ им. Г.И.	http://magtu.ru:8085/marcweb2/Default.asp
Международная наукометрическая реферативная и	http://webofscience.com
Международная реферативная и полнотекстовая справочная	http://scopus.com
Международная база полнотекстовых журналов	http://link.springer.com/
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii
Информационная система - Банк данных угроз	https://bdu.fstec.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:
Лекционные аудитории:
- Мультимедийные средства хранения, передачи и представления информации.

Лаборатория технической защиты информации:
1. АКС-1301 Анализатор спектра
2. Комплекс радиомониторинга "Касандра К6" с диапазоном рабочих частот 0,009-6000Мгц
3. Комплекс радиомониторинга "Касандра К21" с диапазоном рабочих частот 0,009-21000Мгц
4. Генератор шума стационарный "ГШ-1000-М"
5. Система виброакустической и акустической защиты "Соната-АВ"
6. Устройство защиты телефонных переговоров от прослушивания и записи "Прокруст-200"
7. Осциллограф
8. Комплект учебного оборудовании «Персональный компьютер»

Лаборатория защищенных автоматизированных систем:
1. Стенд пожарной безопасности
2. Стенд климат-контроль

Компьютерные классы:
- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.
Помещения для самостоятельной работы обучающихся:
- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.