МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ:
Директор института
Энергетики и автоматизированных систем
_____ С.И. Лукьянов
«20» сентября 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ
НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем
шифр наименование направления подготовки (специальности)

Направленность (профиль/ специализация) программы
Обеспечение информационной безопасности распределенных информационных систем
наименование направленности (профиля) подготовки (специализации)

Уровень высшего образования
специалитет

Форма обучения
очная

Институт	Энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	3,4
Семестр	6,7

Магнитогорск
2017 г.

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом МОиН РФ от 01.12.2016 № 1509.

Рабочая программа рассмотрена и одобрена на заседании кафедры
Информатики и информационной безопасности
(наименование кафедры - разработчика)

«03» марта 2017 г., протокол № 10.

Зав. кафедрой _____ /И.И. Баранкова/
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией
института Энергетики и автоматизированных систем
(наименование факультета (института) - исполнителя)

«14» марта 2017 г., протокол № 6.

Председатель _____ / С.И. Лукьянов/
(подпись) (И.О. Фамилия)

Рабочая программа составлена: зав.кафедрой ИиИБ, д.т.н., профессор
(должность, ученая степень, ученое звание)

_____ / И.И. Баранкова /
(подпись) (И.О. Фамилия)

Рецензент: зав. кафедрой Бизнес-информатики
и информационных технологий, к.п.н. профессор
(должность, ученая степень, ученое звание)

_____ / Г.Н. Чусавитина/
(подпись) (И.О. Фамилия)

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата, № протокола заседания кафедры	Подпись зав. кафедрой
1.	7	Переработка фонда оценочных средств	№1 от 07.09.2018	
2.	8	Обновление списка основной и дополнительной литературы	№1 от 07.09.2018	
3.	7	Переработка фонда оценочных средств	№ 1 от 07.09.2019	
4.	8	Обновление списка основной и дополнительной литературы	№ 1 от 07.09.2019	
5.	7	Переработка фонда оценочных средств	№1 от 04.09.2020	
6.	8	Обновление списка основной и дополнительной литературы	№1 от 04.09.2020	

1. Цели освоения дисциплины

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 в структуре ООП подготовки специалиста

Дисциплина «Техническая защита информации» входит в цикл дисциплин Б1.Б.29 образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем.

Успешное усвоение материала предполагает знание обучающимися основных положений курсов «Организация ЭВМ и вычислительных систем», «Введение в специальность», «Физика», «Основы радиотехники», «Теория информации», «Основы информационной безопасности», «Электроника и схемотехника».

Дисциплина является предшествующей для изучения дисциплин: «Управление информационной безопасностью», «Разработка и эксплуатация защищенных автоматизированных систем», «Информационная безопасность распределенных информационных систем».

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

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

Структурный элемент компетенции	**Планируемые результаты обучения**
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 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.

Структурный элемент компетенции	Планируемые результаты обучения
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 и содержание дисциплины

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

– контактная работа – 124,95 акад. часов:

– аудиторная – 119 акад. часов;

– внеаудиторная – 5,95 акад. часов;

– самостоятельная работа – 55,35 акад. часов;

– подготовка к экзамену – 35,7 акад. часа.

Форма аттестации: 6 семестр – зачет, 7 семестр – Экзамен и КР.

Раздел дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Вид самостоятельной работы	Формы текущего контроля	Код и структурный элемент
		Лекции	ятияЛабораторные	таСамостоятельная		ной	ции

Раздел 1 **Общие положения защиты информации техническими средствами.**	**Тема 1.1.** Предмет и содержание дисциплины. Физические основы функционирования систем обработки и передачи информации.	**6**	**3**	**4/ 2И**		Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к тестированию.	**КТ-1**	ОПК-1-зв
	Тема 1.2. Задачи защиты информации от утечки по техническим каналам.	**6**	**1**	**2**				
Раздел 2	**Тема 2.1.** Условия и особенности утечки информации.Структура канала утечки. Виды технических каналов утечки информации.	**6**	**3**	**4/ 2И**		Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к ЛР.	**ЛР-1**	ОПК-1-зув, ПК-14, зув, ПК-17-зув
Технические каналы утечки информации.	**Тема 2.2.**Условия образования каналов утечки. Характеристики каналов утечки информации.	**6**	**2**	**4/ 2И**	**2**			
Раздел 3 **Акустический канал утечки информации.**	**Тема 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 ЛР.	**ЛР-2**	ОПК-1-зув, ПК-14, зув, ПК-17-зув
	Тема 3.2.Способы и средства защиты от съема информации по акустическому каналу.Системы защиты от утечки информации по акустическому каналу.	**6**	**2**	**5/ 3И**	**3**			
Раздел 4 **Вибрационный канал утечки информации.**	**Тема 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 ЛР и КТ.	**ЛР-3 КТ-2**	ОПК-1-зув, ПК-14, зув, ПК-17-зув
	Тема 4.2 Способы и средства защиты от съема информации по вибрационному каналу.Системы защиты от утечки информации по вибрационному каналу.	**6**	**2**	**5/ 3И**	**4**			
	Зачет				**6,05**	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного	**Зачет**	ОПК-1-зув, ПК-14,

						портала и ЭБС. Подготовка к зачету.		зув, ПК-17-зув
	Итого по семестру:		**17**	**34 / 18 И**	**20,05**			
Раздел 5 **Электромагнитный канал утечки информации.**	**Тема 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 ЛР и КТ.	**ЛР-4 КТ-3**	ОПК-1-зув, ПК-14, зув, ПК-17-зув
	Тема 5.2. Способы и средства защиты от съема информации по электромагнитному каналу. Системы защиты от утечки информации по электромагнитному каналу.	**7**	**4**	**4/ 2И**	**4**			
Раздел 6 **Оптический канал утечки информации.**	**Тема 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 ЛР и КТ.	**ЛР-5 КТ-4**	ОПК-1-зув, ПК-14, зув, ПК-17-зув
	Тема 6.2.Способы и средства защиты от съема информации по оптическому каналу. Системы защиты от утечки информации по оптическому каналу.	**7**	**4**	**4/ 2И**	**5**			
Раздел 7. **Электросетевой канал утечки информации.**	**Тема 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 ЛР и КТ.	**ЛР-6 КТ-5**	ОПК-1-зув, ПК-14, зув, ПК-17-зув
	Тема 7.2.Способы и средства защиты от съема информации по электросетевому каналу. Системы защиты от утечки информации по электросетевому каналу.	**7**	**4**	**4/ 2И**	**5**	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к ЛР и КТ.		
Раздел 8 **Поиск средств несанкционированного съема информации.**	**Тема 8.1.** Организационные и технические мероприятия по защите информации в	**7**	**4**	**5/ 3И**	**5**	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного	**ЛР-7 КТ-6**	ОПК-1-зув, ПК-14,

	учреждениях и на предприятиях.					портала и ЭБС. Подготовка к ЛР и КТ.		зув, ПК-17-зув
	Тема 8.2.Контроль эффективности мер по защите информации техническими средствами.	**7**	**4**	**5/ 3И**	**4,3**			
	Экзамен				**35,7**	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к экзамену и КР.	Экзамен, КР	ОПК-1-зув, ПК-14, зув, ПК-17-зув
	Итого по семестру		**34**	**34/ 18 И**	**35,3+ 35,7**		Экзамен, КР	**108**
Итого по курсу			**51**	**68/ 36 И**	**55,35 +35,7**		Зачет, Экзамен, КР	**216**

Л – лекции, ПЗ – практические занятия, СР – самостоятельная работа, ЛР – аудиторная лабораторная работа, ИДЗ – индивидуальное задание, КТ – контрольное тестирование.

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:

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.
   c) ***Лекция «обратной связи»*** – лекция–провокация (изложение материала с заранее запланированными ошибками), лекция-беседа, лекция-дискуссия, лекция-прессконференция.
   d) ***Семинар-дискуссия*** – коллективное обсуждение какого-либо спорного вопроса, проблемы, выявление мнений в группе (межгрупповой диалог, дискуссия как спор-диалог).
   e) ***Контекстное обучение*** – для мотивации обучающихся к усвоению знаний путем выявления связей между конкретным знанием и его применение. Овладев в рамках изучения дисциплины навыками обеспечения безопасности информации с помощью типовых программных средств, обучающийся приобретет способность участвовать в разработке защищенных автоматизированных систем по профилю своей профессиональной деятельности;

   f) ***Междисциплинарное обучение*** – для использования знаний из различных областей, их группировки и концентрации в контексте решаемой задачи. Для реализации данного метола обучения обучающимся выдаются задания по решения задач из другой предметной области.

4) **Технологии проблемного обучения** – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности обучающихся. Формы учебных занятий с использованием технологий проблемного обучения:
   a) ***Проблемная лекция*** – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала.
   b) ***Лекция «вдвоем» (бинарная лекция)*** – изложение материала в форме диалогического общения двух преподавателей (например, реконструкция диалога представителей различных научных школ, «ученого» и «практика» и т.п.).

c) ***Практическое занятие в форме практикума*** – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков.
d) ***Практическое занятие на основе кейс-метода*** – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации. разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения учебной проблемы.

5) **Игровые технологии** – организация образовательного процесса, основанная на реконструкции моделей поведения Формы учебных занятий с использованием предложенных сценарных условий. Формы учебных занятий с использованием игровых технологий:
   a) ***Учебная игра*** – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем отношений, которые характерны для этой деятельности как целого.
   b) ***Деловая игра*** – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма», реконструкцией функционального взаимодействия в коллективе и т.п.
   c) ***Ролевая игра*** – имитация или реконструкция моделей ролевого поведения в предложенных сценарных условиях.
6) **Технологии проектного обучения** – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания. Проект предполагает совместную учебно-познавательную деятельность группы обучающихся, направленную на выработку концепции, установление целей и задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлексию. Основные типы проектов:
   a) ***Исследовательский проект*** – структура приближена к формату научного исследования (доказательство актуальности темы, определение научной проблемы, предмета и объекта исследования, целей и задач, методов, источников, выдвижение гипотезы, обобщение результатов, выводы, обозначение новых проблем).
   b) ***Творческий проект***, как правило, не имеет детально проработанной структуры; учебно-познавательная деятельность обучающихся осуществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия и т.п.).
   c) ***Информационный проект*** – учебно-познавательная деятельность с ярко выраженной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).
7) **Информационно-коммуникационные образовательные технологии** – организация образовательного процесса, основанная на применении специализированных программных сред и технических средств работы с информацией. Формы учебных занятий с использованием информационно-коммуникационных технологий:
   a) ***Лекция-визуализация*** – изложение содержания сопровождается презентацией (демонстрацией учебных материалов, представленных в различных знаковых системах, в т.ч. иллюстративных, графических, аудио- и видеоматериалов).
   b) ***Практическое занятие в форме презентации*** – представление результатов проектной или исследовательской деятельности с использованием специализированных программных сред.

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 так же 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 «Касандра».

2. Обнаружение устройств и анализ сети Wi-Fi с использованием комплекса радиомониторинга и цифрового анализа сигналов «Касандра».
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

а) 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 применяемых технических средств 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 безопасности. Самостоятельно настраивать технические средства обеспечения информационной безопасности.	Задания: 1. Замаскировать речевые сигналов акустическими шумами в аудитории 226 с использованием системы виброакустической и акустической защиты Соната-АВ (модель 3М). 2. Обеспечить защиту речевой информации от съема по вибрационному каналу в аудитории 226 с использованием системы виброакустической и

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	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.	акустической защиты Соната-АВ (модель 3М). 3. Вычислить мощность радиосигнала в канале CDMA с использованием анализатора спектра «АКС-1301». 4. Настроить СЗИ Соната-АВ.
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.	Темы курсовых работ: 1. Расчет выполнения норм противодействия акустической речевой разведке выделенного помещения на базе МГТУ. 2. Разработка модели угроз и модели нарушителя с целью создания системы технической защиты информации выделенного помещения на базе МГТУ. 3. Оценка эффективности комплекса защиты акустической информации в выделенном помещении на базе МГТУ. 4. Расчет выполнения норм виброакустической защищенности выделенного помещения на базе МГТУ. 5. Оценка защищенности средств вычислительной техники от утечки информации за счет ПЭМИ в выделенном помещении на базе МГТУ.
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 15. Способы подключения и защита телефонной линии. 16. Конфиденциальное совещание: несанкционированный съём информации и методы защиты от него. 17. Беззаходовые методы прослушивания помещений по ТЛ. 18. Мобильные системы связи и их использование в информационных атаках. 19. Защита информации от атак с помощью сотовых телефонов и диктофонов. 20. Оптические каналы утечки информации (атака и защита). 21. Радиоэлектронные каналы утечки информации. 22. Пассивные и активные методы защиты информации в радиоэлектронном канале. 23. Способы и принципы инженерно технической

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		защиты информации. 24. Способы и средства инженерной защиты и технической охраны объектов. 25. Утечка информации по ПЭМИН и применяемые меры защиты. 26. Зоны электромагнитного поля и возможности утечки информации. 27. 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 Самостоятельно организовывать защиту информации от утечки по техническим каналам на объектах информатизации.	Задания: 1. Изучить устройство и принципы работы комплекса радиомониторинга и цифрового анализа сигналов «Касандра». 2. Обнаружить устройства и проанализировать сети Wi-Fi с использованием комплекса радиомониторинга и цифрового анализа сигналов «Касандра». 3. Обеспечить маскировку информативных ПЭМИН устройств вычислительной техники, размещённой в аудитории 226 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 в аудитории 309а.
Владеть	Средствами технической защиты информации. Методами технической защиты информации. Методами и средствами технической защиты информации.	Темы курсовых работ: 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.
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	**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.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	информации.	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	Контролировать безотказное функционирование технических средств защиты информации. Восстанавливать отказавшие технические средства 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 нормативными правовыми актами в области технической защиты информации. Навыками организации защиты информации от утечки по техническим каналам на объектах информатизации.	1. Разработать модели угроз и нарушителя с целью создания системы технической защиты информации ВП. 2. Разработать модели угроз и нарушителя с целью создания системы технической защиты информации ОИ.

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 ин-формации, 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

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. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с.- Режим доступа: http://znanium.com/bookread.php?book=405000 . - Загл. с экрана. - ISBN 978-5-369-01178-2.

б) Дополнительная литература:

1. Ажмухамедов И.М. Основы организационно-правового обеспечения информационной безопасности: [Электронный ресурс]: учеб. пособие / И.М. Ажмухамедов, О.М. Князева. - СПб.: Издательский центр «Интермедия», 2017. – 264 с. - Режим доступа: https://ibooks.ru/product.php?productid=356930 .- Загл. с экрана. - ISBN: 978-5-4383-0160-8.

2. Унижаев Н.В. Информационно-аналитическое обеспечение безопасности организации: [Электронный ресурс]: учеб. пособие / Н.В. Унижаев - СПб.: Издательский центр «Интермедия», 2018. – 408с. - Режим доступа: https://ibooks.ru/product.php?productid=356934 . - Загл. с экрана. - ISBN: 978-5-4383-0158-5.

3. Царегородцев А.В. Методы и средства защиты информации в государственном управлении: [Электронный ресурс]: учеб. пособие / А.В. Царегородцев, М.М. Тараскин. - Москва: Проспект, 2017. - 208 с. - Режим доступа: https://ibooks.ru/product.php?productid=356008 . - Загл. с экрана. - ISBN: 978-5-392-20353-6.

4. Баркалов С.А. Информационная безопасность при управлении техническими системами: [Электронный ресурс]: учеб. пособие /, О.М. Барсуков, В.Е. Белоусов, К.В. Славнов. – СПб.: ИЦ «Интермедия», 2016. – 528с.: илл. - 208 с. - Режим доступа: https://ibooks.ru/product.php?productid=356935 .- Загл. с экрана. - ISBN: 978-5-4383-0133-2.Комплексная система защиты информации на предприятии [Электронный ресурс]: учеб.пособие / Н.В. Гришина. - М.: Форум, 2009. - 240 с.: ил.; - (Профессиональное образование).- Режим доступа: http://znanium.com/bookread.php?book=175658 .- Загл. с экрана. - ISBN 978-5-91134-369-9.

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:

1. Журнал Information Security. Информационная безопасность [Электронный ресурс]: периодич. интернет-изд. – Режим доступа: http://www.itsec.ru/articles2/allpubliks – Загл. с экрана. Яз. рус.

2. Журнал «Безопасность информационных технологий» [Электронный ресурс]: периодич. интернет-изд. – Режим доступа: http://www.pvti.ru/articles_14.htm . – Загл. с экрана. Яз. рус.

3. Журнал «Вопросы кибербезопасности» [Электронный ресурс]: периодич. интернет-изд. – Режим доступа: http://cyberrus.com/ – Загл. с экрана. Яз. рус.

4. «Журнал сетевых решений LAN»: [Электронный ресурс]: периодич. интернет-изд. URL: http://www.osp.ru/lan/ Издательство "Открытые системы. СУБД". – Режим доступа: http://www.osp.ru/os/ – Загл. с экрана. Яз. рус.

5. Государственная публичная научно-техническая библиотека России [Электронный ресурс] / – Режим доступа: http://www.gpntb.ru , свободный.– Загл. с экрана. Яз. рус.

6. Российская национальная библиотека. [Электронный ресурс] / – Режим доступа: http://www.nlr.ru . Яз. рус.

7. Безопасник [Электронный ресурс]. – Режим доступа: http://www.безопасник.рф .– Загл. с экрана. Яз. рус.

8. Компьтерра: все новости про компьютеры, железо, новые технологии, информационные технологии [Электронный ресурс]. – Периодическое электронное Интернет-издание – Режим доступа: http://www.computerra.ru/ – Загл. с экрана. Яз. рус.

9. ФСТЭК России [Электронный ресурс] – Режим доступа: http://fstec.ru/.– Загл. с экрана. Яз. рус.

9 Материально-техническое обеспечение дисциплины

Материально-техническое обеспечение дисциплины включает:

Тип и название аудитории	Оснащение аудитории
Лекционная аудитория (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.)	Мультимедийные средства хранения, передачи и представления информации
Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.)	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office 2007 (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.
Лаборатория радиомониторинга и	Комплекс радиомониторинга «Касандра К-6»;

Тип и название аудитории	Оснащение аудитории
контроля утечек информации, ауд. 226	Комплекс радиомониторинга «Касандра К-21»; Анализатор спектра «АКС-1301»; Комплект учебного оборудования «Системы мониторинга информационной безопасности»; Генератор радиошума ГШ-1000М; Соната-АВ (модель 3М) система виброакустической и акустической защиты; Устройство защиты Прокруст 2000; Устройства для защиты линий электропитания и заземления от утечки информации «Соната-РС2».
Аудитории для самостоятельной работы (ауд. 132а): компьютерные классы; читальные залы библиотеки.	Персональные компьютеры с ПО: Операционная система MS Windows 7 (Microsoft Imagine Premium D-1227-18 от 08.10.2018 до 08.10.2021); Пакет MS Office 2007 (Microsoft Open License 42649837, бессрочная); Выход в Интернет и доступ в электронную информационно-образовательную среду университета.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций и ПрООП ВО для специальности *10.05.03 Информационная безопасность автоматизированных систем. Специализация «Обеспечение информационной безопасности распределенных информационных систем».*